Научно-исследовательский
центр «Иннова»

СОВРЕМЕННАЯ НАУКА: ЭКСПЕРИМЕНТ И НАУЧНАЯ ДИСКУССИЯ

Сборник научных трудов по материалам
XXX Международной научно-практической конференции,
27 января 2025 года, г.-к. Анапа

Анапа
2025

УДК 00(082) + 001.18 + 001.89
ББК 94.3 + 72.4: 72.5
С56

С56 **Современная наука: эксперимент и научная дискуссия.** Сборник научных трудов по материалам XXX Международной научно-практической конференции (г.-к. Анапа, 27 января 2025 г.). – Анапа: НИЦ ЭСП в ЮФО, 2025. - 51 с.

ISBN 978-5-95356-643-8

В настоящем издании представлены материалы XXX Международной научно-практической конференции «Современная наука: эксперимент и научная дискуссия», состоявшейся 27 января 2025 года в г.-к. Анапа. Материалы конференции посвящены актуальным проблемам науки, общества и образования. Рассматриваются теоретические и методологические вопросы в социальных, гуманитарных и естественных науках.

Издание предназначено для научных работников, преподавателей, аспирантов, всех, кто интересуется достижениями современной науки.

УДК 00(082) + 001.18 + 001.89
ББК 94.3 + 72.4: 72.5

ISBN 978-5-95356-643-8

СОДЕРЖАНИЕ

ЮРИДИЧЕСКИЕ НАУКИ

ТЕХНИЧЕСКИЕ НАУКИ

УДК 004.05

ПРИМЕНЕНИЕ ОБЛАЧНЫХ ТЕХНОЛОГИЙ ДЛЯ УДАЛЕННОГО УПРАВЛЕНИЯ МОБИЛЬНЫМИ РОБОТАМИ

Аксенов Олег Романович

бакалавр

Куксин Виктор Сергеевич

магистр

Научный руководитель: Михайлова Ольга Владимировна,

к.т.н., доцент

ФГБОУ ВО «Сибирский государственный индустриальный университет»,

город Новокузнецк

Аннотация. *Статья посвящена анализу применения облачных технологий для удаленного управления мобильными роботами. Рассматриваются современные подходы к интеграции облачных вычислений, преимущества и ограничения таких систем, а также их влияние на эффективность работы мобильных роботов. Особое внимание уделено вопросам безопасности, надежности и масштабируемости.*

The article is devoted to the analysis of the use of cloud technologies for remote control of mobile robots. Modern approaches to the integration of cloud computing, the advantages and limitations of such systems, as well as their impact on the efficiency of mobile robots are considered. Special attention is paid to the issues of security, reliability and scalability.

Ключевые слова: *облачные технологии, мобильные роботы, удаленное управление, автоматизация, IoT, безопасность данных*

Keywords: *cloud technologies, mobile robots, remote control, automation, IoT, data security*

С развитием Интернета вещей (IoT) и облачных технологий мобильные роботы получили новые возможности для удаленного управления и взаимодействия. Использование облачных платформ позволяет интегрировать роботов в единую сеть, обеспечивая эффективное распределение ресурсов, доступ к сложным вычислениям и централизованное управление.

Цель статьи — исследовать применение облачных технологий для управления мобильными роботами, оценить их преимущества и определить возможные ограничения.

Применение облачных технологий для управления роботами:

1. Архитектура облачных систем управления.

Облачная система управления мобильными роботами включает три ключевых компонента:

– робот: оборудован сенсорами, приводами и средствами связи;

– облачная платформа: обрабатывает данные, выполняет сложные вычисления и предоставляет интерфейсы для управления;

– пользователь: взаимодействует с системой через удалённое устройство.

2. Преимущества использования облачных технологий

– масштабируемость: возможность подключения большого числа роботов к единой системе;

– снижение затрат: перенос вычислительных операций в облако снижает требования к аппаратным ресурсам роботов.

Сравнение локальных и облачных систем управления перечислены в таблице 1.

Таблица 1 – Сравнение локальных и облачных систем управления

Характеристика	Локальная система	Облачная система
Вычислительные ресурсы	Ограниченные	Практически неограниченные
Стоимость оборудования	Высокая	Низкая
Масштабируемость	Низкая	Высокая
Удобство обновления	Ограниченное	Простое и централизованное

Роботы в здравоохранении. Облачные решения обеспечивают удалённое

управление медицинскими роботами, используемыми для диагностики, хирургии и ухода за пациентами.

Примеры применения:

1. Использование облачных технологий позволяет в режиме реального времени оптимизировать производственные процессы, настраивать алгоритмы работы и проводить диагностику оборудования.

2. Облачные технологии активно применяются в управлении дронами для доставки товаров, а также в автоматизации складов.

3. Облачные решения обеспечивают удалённое управление медицинскими роботами, используемыми для диагностики, хирургии и ухода за пациентами.

Примеры применения облачных технологий в различных отраслях перечислены в таблице 2.

Таблица 2 – Примеры применения облачных технологий в различных отраслях

Отрасль	Пример использования	Облачная платформа
Промышленность	Управление роботами на заводах	AWS RoboMaker
Логистика	Координация дронов и складских систем	Google Cloud
Здравоохранение	Работы для телемедицины и хирургии	Microsoft Azure

Проблемы и ограничения:

– при использовании облачных систем возможно возникновение задержек, что критично для задач реального времени;

– передача данных через облачные платформы требует дополнительных мер защиты, таких как шифрование и мониторинг сетевой активности;

– отсутствие устойчивого подключения может полностью парализовать работу системы.

Основные проблемы облачных технологий и пути их решения перечислены в таблице 3.

Таблица 3 – Основные проблемы облачных технологий и пути их решения

Проблема	Возможное решение
Задержки передачи данных	Оптимизация маршрутизации, использование 5G
Угрозы безопасности	Шифрование данных, использование VPN
Зависимость от сети	Резервные каналы связи

Экономическое обоснование. Применение облачных технологий позволяет снизить капитальные затраты и повысить операционную эффективность.

Экономический анализ внедрения облачных систем перечислены в таблице 4.

Таблица 4 – Экономический анализ внедрения облачных систем

Показатель	Без облачных технологий	С облачными технологиями
Затраты на оборудование	Высокие	Низкие
Эксплуатационные расходы	Средние	Низкие
Производительность системы	Ограниченная	Высокая

Применение облачных технологий для управления мобильными роботами предоставляет значительные преимущества в области автоматизации, эффективности и интеллектуализации систем. Они обеспечивают:

1. Масштабируемость и гибкость: возможность быстрого подключения новых устройств и адаптации к изменяющимся условиям.

2. Экономическую выгоду: снижение затрат на оборудование и операционные расходы за счёт использования облачных вычислений.

3. Улучшение аналитики и прогнозирования: доступ к мощным инструментам анализа данных и машинного обучения для оптимизации процессов.

4. Снижение нагрузки на локальные ресурсы: перенос вычислений в облако минимизирует потребности в аппаратных средствах роботов.

Однако для успешного внедрения необходимо учитывать существующие ограничения, такие как задержки передачи данных, уязвимости в сфере безопасности и зависимость от сети. Преодоление этих барьеров возможно за счёт:

– инвестиций в развитие инфраструктуры связи, включая 5g-сети;

– использования современных методов шифрования данных и защиты от кибератак;

– разработки гибридных систем, сочетающих локальные вычисления с облачными решениями.

В перспективе облачные технологии будут играть ключевую роль в

развитии автономных систем, робототехники и искусственного интеллекта. Их интеграция с 5G, квантовыми вычислениями и распределёнными сетями создаст новые возможности для масштабирования и повышения эффективности работы мобильных роботов.

Список литературы

1. Александров А.В., Калабухов С. А. Облачные технологии в управлении роботами: подходы и решения / Вестник компьютерных и информационных технологий. 2019. № 176. С. 20–27.

2. Балакин В. В., Егошин А.В. Применение облачных вычислений в системах управления роботами / Автоматизация и IT в энергетике. 2018. № 14. С. 36–43.

3. Волгин В. В., Ильинский А. С. Облачная платформа для управления роботами: архитектура и примеры применения / Труды Института проблем управления РАН. 2019. Т. 69, № 1. С. 51–60.

4. Горбунов А. А., Иванов В. А. Облачные сервисы для управления промышленными роботами / Информационно-измерительные и управляющие системы. 2018. Т. 16, № 4. С. 46–53.

5. Дубинин А.В., Никитин А. А. Облачное управление роботами: теория и практика / Научные ведомости Белгородского государственного университета. Серия: Информатика. 2019. Т. 44, № 2. С. 125–132.

6. Ефимов В. А., Миронов А.В. Облачные технологии в робототехнике: возможности и ограничения / Сборник научных трудов Международной конференции «Робототехника и искусственный интеллект». 2018. С. 78–83.

7. Жданов А. А., Сергеев А.В. Управление роботами с использованием облачной инфраструктуры / Вестник МГТУ имени Н.Э. Баумана. Серия: Приборостроение. 2019. № 128. С. 112–121.

УДК 004.05

ПРИМЕНЕНИЕ МОБИЛЬНЫХ РОБОТОВ В ЗДРАВООХРАНЕНИИ И ИХ РОЛЬ В ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЯХ

Аксенов Олег Романович
бакалавр

Куксин Виктор Сергеевич
магистр
Научный руководитель: Михайлова Ольга Владимировна,
к.т.н., доцент
ФГБОУ ВО «Сибирский государственный индустриальный университет»,
город Новокузнецк

Аннотация. *В данной статье рассматриваются современные достижения в области применения мобильных роботов в здравоохранении. Особое внимание уделено их роли в чрезвычайных ситуациях, таких как пандемии, стихийные бедствия и техногенные катастрофы. Приведены примеры успешного применения, а также анализированы потенциальные проблемы и ограничения.*

This article examines modern advances in the field of mobile robots in healthcare. Special attention is paid to their role in emergency situations such as pandemics, natural disasters and man-made disasters. Examples of successful applications are given, as well as potential problems and limitations are analyzed.

Ключевые слова: *мобильные роботы, здравоохранение, чрезвычайные ситуации, телемедицина, автоматизация, экономическое обоснование*

Keywords: *mobile robots, healthcare, emergencies, telemedicine, automation, economic justification*

Мобильные роботы стали важным компонентом в здравоохранении, способствуя автоматизации и повышению эффективности медицинских процессов. В условиях чрезвычайных ситуаций они играют ключевую роль, минимизируя риск для медперсонала и повышая доступность медицинских услуг.

Цель данной статьи — исследовать возможности мобильных роботов в

здравоохранении, их вклад в управление чрезвычайными ситуациями и экономическую целесообразность их применения.

Применение мобильных роботов в здравоохранении:

1. Мобильные роботы используются для автоматической доставки медикаментов, медицинских образцов и оборудования внутри больниц. Это снижает нагрузку на персонал и минимизирует человеческие ошибки.

2. Роботы, оснащенные ультрафиолетовыми лампами или системами распыления, применяются для обеззараживания помещений, что особенно актуально в пандемии COVID-19.

3. Роботы-компаньоны и ассистенты помогают пациентам с ограниченными возможностями передвижения или когнитивными нарушениями. Они могут напоминать о приеме лекарств, помогать в базовых задачах.

4. Роботы с функциями телемедицины обеспечивают удаленный доступ к медицинским услугам, включая диагностику, консультации и мониторинг пациентов.

Примеры применения мобильных роботов в здравоохранении перечислены в таблице 1.

Таблица 1 – Примеры применения мобильных роботов в здравоохранении

Тип робота	Функция	Пример применения
Доставка медикаментов	Транспортировка внутри больницы	Робот TUG (Aethon)
Дезинфекционные	Ультрафиолетовая дезинфекция	Xenex LightStrike
Телемедицинские	Диагностика и консультация удаленно	InTouch Health
Роботы-компаньоны	Социальная поддержка	Робот Pepper

Преимущества использования роботов в здравоохранении перечислены в таблице 2.

Таблица 2 – Преимущества использования роботов в здравоохранении

Преимущество	Описание
Снижение нагрузки на персонал	Освобождение времени медработников
Повышение точности	Исключение человеческих ошибок
Снижение затрат	Оптимизация процессов
Повышение безопасности	Уменьшение контакта с инфекциями

Роль мобильных роботов в чрезвычайных ситуациях:

1. В чрезвычайных ситуациях, таких как пандемии, использование роботов минимизирует контакт персонала с инфекционными пациентами.

2. Мобильные роботы могут использоваться для эвакуации пациентов из зон бедствия, обеспечивая их безопасность.

3. В условиях кризиса мобильные роботы помогают сортировать пациентов, обеспечивая приоритетное обслуживание тяжелых случаев.

Примеры применения роботов в чрезвычайных ситуациях перечислены в таблице 3.

Таблица 3 – Примеры применения роботов в чрезвычайных ситуациях

Ситуация	Функция робота	Пример использования
Пандемия	Дезинфекция больниц	UV-C роботы в клиниках
Землетрясение	Поиск пострадавших	Роботы-дроны для сканирования местности
Техногенные катастрофы	Устранение загрязнений	Роботы для контроля утечек

Технологические и социальные аспекты применения, имеют преимущества и проблемы.

Преимущества:

– повышение скорости выполнения задач;

– снижение нагрузки на медперсонал;

– минимизация рисков для здоровья.

Проблемы и ограничения:

– высокая стоимость внедрения;

– необходимость регулярного технического обслуживания;

– возможное сопротивление со стороны персонала;

– требование к адаптации инфраструктуры под использование роботов.

Экономическое обоснование внедрения. Для оценки экономической целесообразности применения мобильных роботов был выполнен анализ затрат и выгод.

Сравнение затрат и выгод при использовании роботов перечислены в таблице 4.

Таблица 4 – Сравнение затрат и выгод при использовании роботов

Показатель	Без роботов (в год)	С роботами (в год)
Затраты на персонал	10 000 000	7 000 000
Стоимость оборудования	0	2 000 000
Общая стоимость	10 000 000	9 000 000
Ожидаемая экономия	-	1 000 000

Прямые и косвенные выгоды от использования роботов перечислены в таблице 5.

Таблица 5 – Прямые и косвенные выгоды от использования роботов

Тип выгоды	Пример
Прямые	Снижение затрат на персонал
Косвенные	Повышение скорости обслуживания пациентов

Результаты демонстрируют, что внедрение мобильных роботов обеспечивает значительную экономию при повышении производительности.

Мобильные роботы играют важную роль в трансформации здравоохранения, особенно в условиях чрезвычайных ситуаций. Несмотря на существующие барьеры, их использование способствует повышению эффективности, безопасности и качества медицинских услуг.

Список литературы

1. Артюшкин О. Л., Карпов А.В. Применение мобильных роботов в медицине: современные тенденции и перспективы / Вестник Южно-Уральского государственного университета. Серия: Компьютерные технологии, управление, радиоэлектроника. 2019. Т. 19, № 3. С. 15–24.

2. Васильев В. Н., Семенов Н. В. Роботы в медицине: от теории к практике / Медицинская техника. 2018. № 4. С. 21–25.

3. Гаврилюк В. Л., Назаров В. Е. Роботы-спасатели: история, современное состояние и перспективы развития / Проблемы безопасности и чрезвычайных ситуаций. 2017. № 2. С. 23–31.

4. Губанков А. С., Ивановский Р. В. Автономные мобильные роботы в здравоохранении: обзор современных разработок / Инновации в науке и

образовании. 2019. № 13. С. 37–45.

5. Давыдов А.В., Сидоренко В. Ф. Применение робототехники в медицине: опыт и перспективы / Вопросы современной науки и практики. Университет им. В. И. Вернадского. 2018. № 66. С. 16–22.

6. Дмитриев А. К., Соколов В. В. Интеллектуальные системы управления мобильными роботами / Известия Тульского государственного университета. Технические науки. 2017. Вып. 12. С. 33–40.

7. Колесниченко А.В., Михайлов В. А. Роботы в медицинских учреждениях: опыт применения и проблемы внедрения / Научные ведомости Белгородского государственного университета. Серия: Медицина. Фармация. 2019. Т. 42, № 2. С. 123–130.

8. Осипов Г. С., Смирнов И. В. Искусственный интеллект в медицине: достижения и вызовы / Информационные технологии и вычислительные системы. 2018. № 3. С. 48–57.

9. Полякова М. Ю., Соловьев В. В. Медицинские роботы: настоящее и будущее / Наука и инновации. 2019. № 194. С. 28–32.

10. Ромашевский В. В., Кузнецов А.В. Чрезвычайные ситуации и роботы: взаимодействие и перспективы / Безопасность жизнедеятельности. 2018. № 6. С. 41–47.

УДК 004.9

АНАЛИЗ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ВОССТАНОВЛЕНИЯ ДАННЫХ

Куртинова Айжан Абаевна
Николаева Александра Евгеньевна
Сенчик Василий Иванович
Пасынков Максим Александрович
студенты
Научный руководитель: Куприянов Дмитрий Олегович,
ассистент
ФГБОУ ВО «Санкт-Петербургский государственный
морской технический университет»,
город Санкт-Петербург

Аннотация. *Рассмотрены различные программные средства для восстановления удалённых данных. Проведён сравнительный квалиметрический анализ их эффективности, преимуществ и недостатков путем практического тестирования для выявления наиболее конкурентоспособных решений.*

Various software tools for recovering deleted data are considered. Comparative qualimetric analysis of their efficiency, advantages and disadvantages by means of practical testing to identify the most competitive solutions is carried out.

Ключевые слова: *удалённые данные, восстановление файлов, QSWOT*

Keywords: *deleted data, file recovery, QSWOT*

В связи с увеличением объемов обрабатываемой информации и глобальной цифровизацией общества потеря, нарушение целостности или искажение данных становятся все более серьезной проблемой как для частных

пользователей, так и для организаций. Удаление данных происходит по разным причинам, включая ошибки пользователей, системные сбои и вирусные атаки. Поэтому возникает необходимость в различных программных средствах, способных восстанавливать удаленные данные, когда по тем или иным причинам отсутствует их резервная копия. В настоящее время достигнутый уровень развития в области восстановления информации позволяет выбрать оптимальный вариант, который поможет свести возможные убытки к минимуму.

Постановка задачи. Исходя из вышеизложенного, возникает потребность в исследовании различных программных решений для восстановления удаленных данных. Это включает в себя анализ их конкурентной способности, преимуществ и недостатков использования, а также изучение того, с какими операционными системами работают эти программные обеспечения. Целью исследования является выявление наиболее качественных решений, способствующих восстановлению данных после их удаления.

Результаты исследования. При удалении файлов данные не исчезают, они становятся недоступными для пользователя и путь к ним теряется, но удалённый необходимый информационный материал остаётся на жёстком диске компьютера до тех пор, пока эти данные не будут перезаписаны новыми. Поэтому при установке различных инструментов для восстановления данных необходимо быть осторожными, ведь в памяти они могут занять место нужных пользователю файлов, что сделает невозможным восстановление. Одним из наилучших вариантов является скачивание программного обеспечения для восстановления данных на сменный носитель.

В рамках исследования для изучения и последующего тестирования лучших решений было выбрано следующее ПО для восстановления удаленных данных: TestDisk, Photo Rec, Foremost, EaseUS Data Recovery Wizard PRO, R-Linux. Для получения наиболее качественной оценки был выбран метод квалиметрического SWOT-анализа [1] с последующим ранжированием результатов (Таблицы 1.1 и 1.2).

Таблица 1.1 - QSWOT-анализ ПО для восстановления данных ч. 1

Название ПО	*Назначение средства. Лицензия.*	*Экспертная оценка рейтинга R*	S.Сильные (внутренние) стороны	S	W.Слабые (внутренние) стороны	W
TestDisk	Программное обеспечение, которое предназначено для восстановления потерянных разделов на носителях информации, а также для восстановления загрузочного сектора после программных или человеческих ошибок. Open Source	1	Работает на Windows, Linux и macOS. Поддерживает множество различных файловых систем. Имеет сообщество пользователей и разработчиков, которые вносят свой вклад в его развитие и могут предложить поддержку через форумы и рассылки. Может восстановить потерянные разделы, сделать незагружаемые диски снова загрузочными и исправить таблицы разделов.Есть возможность собирать информацию о повреждённом диске.	9,2	Нет графического интерфейса. Может быть сложной в использовании для непрофессионального пользователя. Нет официальной поддержки клиентов, пользователи полагаются на поддержку сообщества.	2,0
Photo Rec	Программа для восстановления утерянных данных в памяти цифровых камер, на жёстких дисках и компакт-дисках. Open Source	2	ПО является бесплатным с открытым кодом. Программа поддерживает Windows, macOS и Linux. Работает с разными типами файловых систем. Восстанавливает данные с различных видов хранителей памяти. Безопасный доступ к данным. PhotoRec не пытается записать поврежденные данные туда, откуда вы их пытаетесь восстановить.	8,7	Большое время сканирования. Случайные имена восстановленных файлов.Отсутствие возможности просмотреть файлы перед восстановлением. Зависит от сигнатур файлов.	3,5
Foremost	Программа для восстановления файлов, разработанная для операционной системы Linux. Главной целью инструмента является восстановление удалённых файлов с помощью метода основанного на анализе заголовков и структур данных файлов. Open Source	3	Поддерживает Linux. Открытый исходный код. Поддерживает восстановление многих типов данных. Не зависит от вида файловой системы. Программа может восстанавливать файлы даже в случае повреждения файловой системы или удаления метаданных. Поддержка множества форматов.	8,5	Не имеет графического интерфейса. Отсутствие подходящего канала коммуникации для постоянного улучшения продуктов. Пропуск файлов при быстром режиме работы. Отсутствие поддержки некоторых типов файлов. Программа не работает с линуксовыми архивами типа bzip2 и p7zip.	4
EaseUS Data Recovery Wizard Pro	Программа способна восстанавливать файлы, потерянные при удалении, форматировании раздела, повреждении логического диска, сбое питания, внезапном выключении системы и даже в результате хакерской атаки.	4	Удобный и интуитивно понятный интерфейс. Глубокое сканирование системы. Есть фильтрация восстанавливаемых файлов. Можно просмотреть удалённые данные до их восстановления. Сохранение результатов сканирования. Отсутствие ограничения на объём восстановленных данных.	9,3	Высокая стоимость коммерческой лицензии. Не поддерживает Linux. Медленное глубокое сканирование. Нет поддержки восстановления данных с мобильных устройств. Большое потребление ресурсов.	5
R-Linux	программа для восстановления файловых систем Ext2/Ext3/Ext4 FS, используемых в Linux и некоторых Unix-системах. Open Sourse.	5	Возвращение данных с существующих логических дисков, даже если записи файлов утрачены. Может восстановить файлы даже в раздел с другой файловой системой. Позволяет скопировать информацию и создать образ целого диска или его части, а уже затем работать с файлом образа, сохранённым на другом носителе, как с оригинальным диском. Может отсканировать жесткий диск, найти ранее удаленный или поврежденный раздел, а уже затем восстановить данные с найденного раздела.	7,5	Отсутствие возможности восстановления данных по сети. Нельзя реконструировать дисковые массивы и восстановления с них данных.	5

Таблица 1.2 - QSWOT-анализ ПО для восстановления данных ч.1

Название ПО	*Назначение средства. Лицензия.*	*Экспертная оценка рейтинга R*	O.Возможности развития с учетом внешних факторов	O	T.Угрозы развития с учетом внешних факторов	T	Q	BQ
TestDisk	Программное обеспечение, которое предназначено для восстановления потерянных разделов на носителях информации, а также для восстановления загрузочного сектора после программных или человеческих ошибок. Open Source	1	Создание поддержки клиентов. Оптимизация решения.	9,0	Возможны кибератаки.	2,0	8,5	1
Photo Rec	Программа для восстановления утерянных данных в памяти цифровых камер, на жёстких дисках и компакт-дисках. Open Source	2	Повышение уровня оптимизации решения. Адаптация под непрофессионального пользователя. Добавление выбора восстанавливаемых данных. Увеличение базы данных сигнатур.	8,0	Возможность появления санкций. Вероятность совершения кибератак.	3,5	7,4	2
Foremost	Программа для восстановления файлов, разработанная для операционной системы Linux. Главной целью инструмента является восстановление удалённых файлов с помощью метода основанного на анализе заголовков и структур данных файлов. Open Source	3	Создание канала для обсуждения по оптимизации решения. Устранение сбоев при быстром редиме работы. Создание инструментов для работы с большим количеством архивов.	8,0	Возможность появления санкций. Риск атак.	3	7,3	3
EaseUS Data Recovery Wizard Pro	Программа способна восстанавливать файлы, потерянные при удалении, форматировании раздела, повреждении логического диска, сбое питания, внезапном выключении системы и даже в результате хакерской атаки.	4	Адаптация решения под Linux. Усовершенствование сканирования. Оптимизация затрат ресурсов.	6,0	Повышение коммерческой лицензии.	4	6,4	4
R-Linux	программа для восстановления файловых систем Ext2/Ext3/Ext4 FS, используемых в Linux и некоторых Unix-системах. Open Sourse.	5	Оптимизация работы программы с дисковыми массивами. Создание функционала для восстановления файлов по сети.	7	Возможность появления санкций (Разработчик Канада). Вероятны кибератаки.	4	6,3	5

На основе результатов QSWOT-анализа можно сделать вывод, что лучшими программными решениями для восстановления данных являются TestDisk,

Foremost и Photo Rec. У всех этих средств открытый исходный код, поэтому удобны в использовании и бесплатны, также у них оказались наилучшие характеристики и перспективы.

Одна из самых удобных утилит — это Foremost (рейтинг 3). У неё нет графического интерфейса, но это не затрудняет работу. Далее представлены результаты тестирования эффективности этого средства в операционной системе Xubuntu Linux. Установить Foremost достаточно легко, так как он присутствует в официальных репозиториях и устанавливается с помощью пакетного менеджере *APT*.

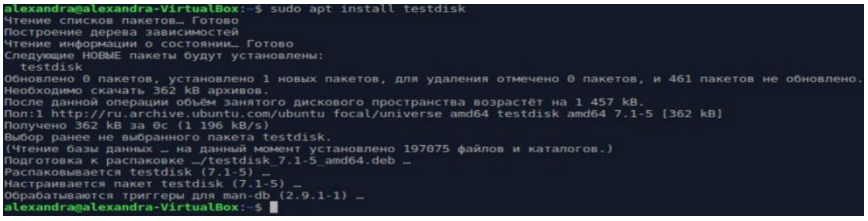

Рис. 1 – Установка Foremost

Последующие действия зависят от того, что и откуда необходимо восстановить. Допустим, нужно восстановить с жёсткого диска */dev/sda* удалённую фотографию, для этого мы используем команду (рис. 2) с определёнными ключами (рис. 3).

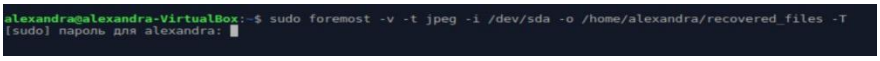

Рис. 2 – Команда восстановления данных

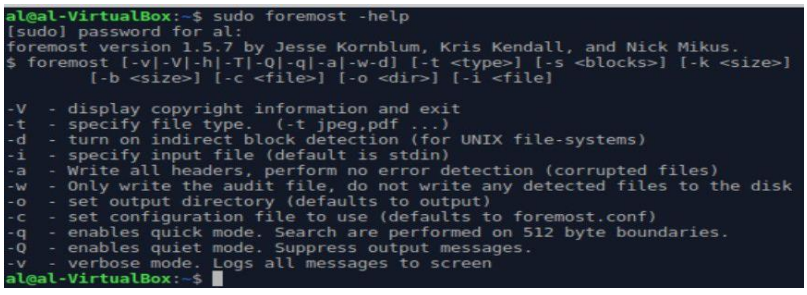

Рис. 3 – Ключи команды для восстановления данных

В результате работы программы в выбранном месте создаётся папка (Рис. 4) с восстановленными файлами (Рис. 5).

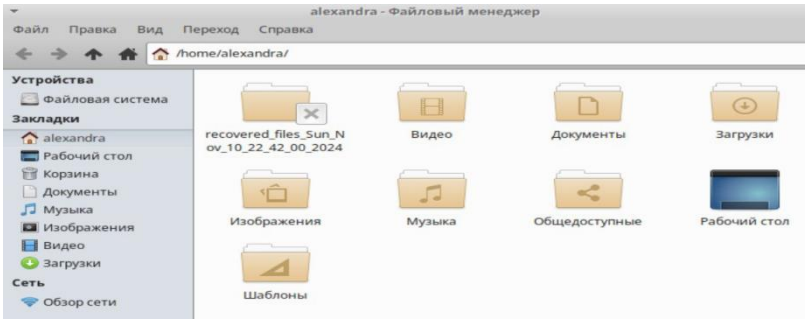

Рис. 4 – Местоположение восстановленных данных

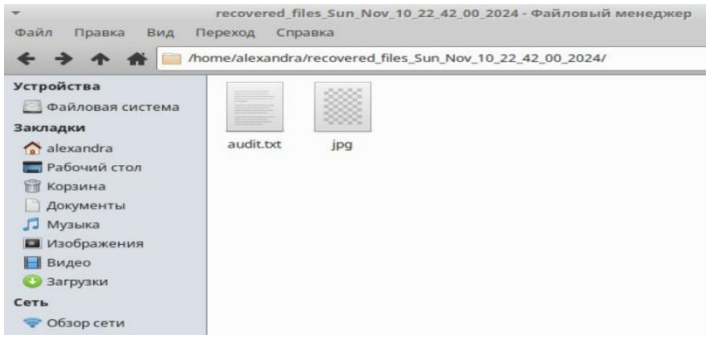

Рис. 5 – Результат работы Foremost

Заключение. Таким образом, по результатам квалиметрического SWOT-анализа были выявлены лучшие конкурентоспособные решения для восстановления удаленных данных, а также рассмотрена работа одного из лучших средств в этой сфере.

Список литературы

1. Алексеев А.В., Удодова Е. Н. Квалиметрический SWOT-анализ и его применение в задачах управления развитием критических морских объектов / Морские интеллектуальные технологии. Научный журнал №1 (31) Т. 1 – 2016 – С. 38-48.

2. Возможности мобильной криминалистики: сайт – URL: https://www.facct.ru/media-library/whitepaper/facct-mobile-forensics-white-paper-2020.pdf.

3. Образование во имя правосудия. Модуль 4. Введение в цифровую криминалистику – Управление ООН по наркотикам и преступности – URL: https://www.unodc.org/documents/e4j/Cybercrime_Module_4_Introduction_to_Digital_Forensics_RU.pdf. (Доступно на www.unodc.org).

4. Что такое восстановление даных и как этой работает: сайт – URL:

https://recoverit.wondershare.com.ru/memorycard-recovery/how-does-data-recovery-works.html.

5. Все о реезервном копировании: основные принципы, правила и лайфхаки: сайт – URL: https://goo.su/BBJVH3A.

УДК 622.276

МОДЕЛИРОВАНИЕ ПОЛИМЕРНОГО ЗАВОДНЕНИЯ ПРИ ЭКСПЛУАТАЦИИ ВЫСОКООБВОДНЕННЫХ СКВАЖИН

Мегахед Юсеф Арафа

магистрант

Научный руководитель: Рябикова Ксения Олеговна,

к.т.н., доцент

ФГБОУ ВО «Тюменский индустриальный университет»,

город Тюмень

Аннотация. *Большое количество мировых нефтяных месторождений эксплуатируется на 4 стадии разработки, перед рядом компаний стоит вызов в продлении рентабельности разработки таких месторождений. Один из методов – применение третичных методов увеличения нефтеотдачи. Для месторождений большой площади актуально будет применение полимерного заводнения. По объекту исследования, на котором средняя обводненности скважинной продукции около 90%, была оценена эффективность технологии полимерного заводнения за 20 лет.*

A large number of the world's oil fields are being exploited at 4 stages of development, and a number of companies face a challenge in extending the development of such fields. One of the methods is the use of tertiary methods to increase oil recovery. For large-area deposits, the use of polymer flooding will be relevant. According to the research object, where the average water content of borehole products is about 90%, the effectiveness of polymer flooding technology over 20 years has been assessed.

Ключевые слова: *гидродинамическое моделирование, полимерное заводнение, нефтяной пласт, прирост накопленной добычи нефти, увеличение коэффициента охвата заводнением*

Keywords: *hydrodynamic modeling, polymer flooding, oil reservoir, increase in accumulated oil production, increase in flood coverage coefficient*

Большое количество нефтяных месторождений в мире находится на заключительной стадии разработки, для которой характерна высокая обводненность продукции скважин. Себестоимость нефти, добытой из таких скважин, значительно выше ввиду высоких затрат на электроэнергию.

Полимерное заводнение – третичный метод увеличения нефтеотдачи (МУН), направленный на увеличение коэффициента охвата [1]. При традиционном заводнении холодной воды возможны прорывы по высокопроницаемым пропласткам от нагнетательных скважин к добывающим. При полимерном заводнении образуется равномерный фронт вытеснения нефти.

По пласту была построена синтетическая гидродинамическая модель (ГДМ), представляющей пласт в целом с позиции геолого-промысловых параметров. В синтетической ГДМ задана геологическая неоднородность (рисунок 1).

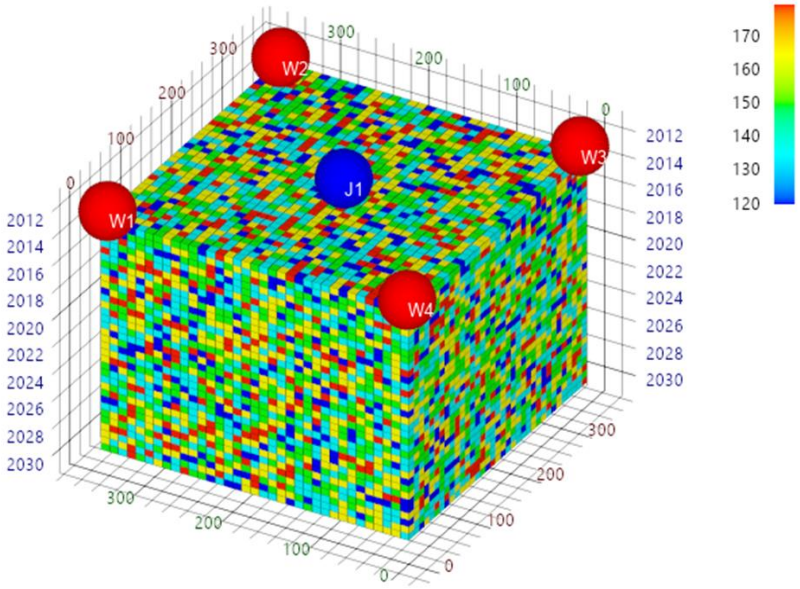

Рисунок 1 – Синтетическая ГДМ по объекту исследования. Куб проницаемости

Средняя пористость по объекту исследования – 23%, проницаемость – 149 мД, мощность пласта – 17 м, песчанистость – 55%, глубина залегания – 2013 м, вязкость нефти – 1.21 сПз.

В модели задана пятиточечная обращенная система скважин, в центре нагнетательная скважина J1, в углах добывающие скважины W1, W2, W3, W4, на которые были заданы множители на продуктивность с целью масштабирования участка на весь объект в целом. Расстояние между добывающими скважинами составляет 340 м, от нагнетательной до добывающих – 240 м.

Расчеты проводились на 40 лет. Контроль добывающих и нагнетательной скважин – по забойному давлению. Расчеты были проведены для следующих вариантов: базовый без закачки полимеров, три варианта с закачкой полимеров с концентрациями 0.1, 0.3, 0.5 кг/м^3 в период с 01.01.2025 до 01.01.2045 г.

Накопленная добыча нефти за 20 лет (включая историческую работу) по вариантам: базовый – 157.29 тыс. м^3, вариант с концентрацией полимеров 0.1 кг/м^3 – 157.40 тыс. м^3 (прирост 111.18 м^3), вариант с концентрацией полимеров 0.3 кг/м^3 – 157.68 тыс. м^3 (прирост 384.32 м^3), вариант с концентрацией полимеров 0.5 кг/м^3 – 158.17 тыс. м^3 (прирост 879.34 м^3) (рисунок 2 и 3).

Накопленная добыча жидкости за 20 лет по вариантам: базовый – 3655.80 м^3, вариант с концентрацией полимеров 0.1 кг/м^3 – 2528.72 тыс. м^3 (уменьшение на 1127.08 тыс. м^3), вариант с концентрацией полимеров 0.3 кг/м^3 – 1495.14 тыс. м^3 (уменьшение на 2160.66 тыс. м^3), вариант с концентрацией полимеров 0.5 кг/м^3 – 904.04 тыс. м^3 (уменьшение на 2751.77 тыс. м^3) (рисунок 4 и 5).

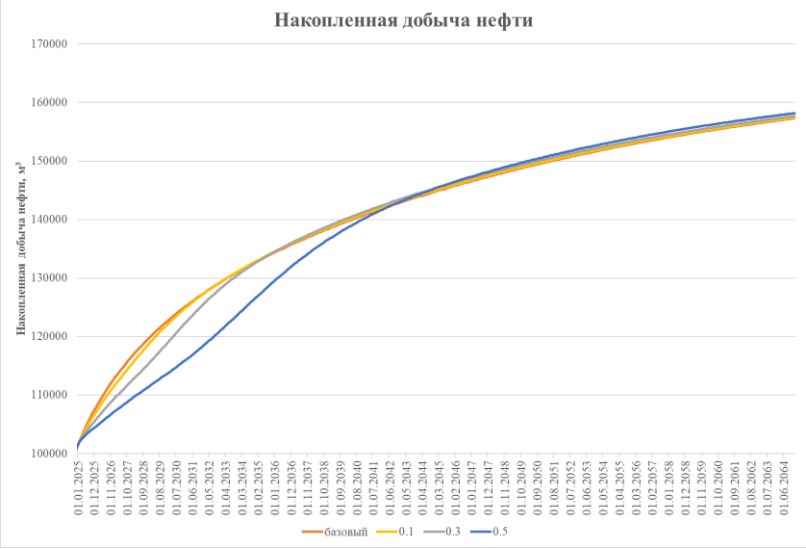

Рисунок 2 - Накопленная добыча нефти по вариантам расчетов

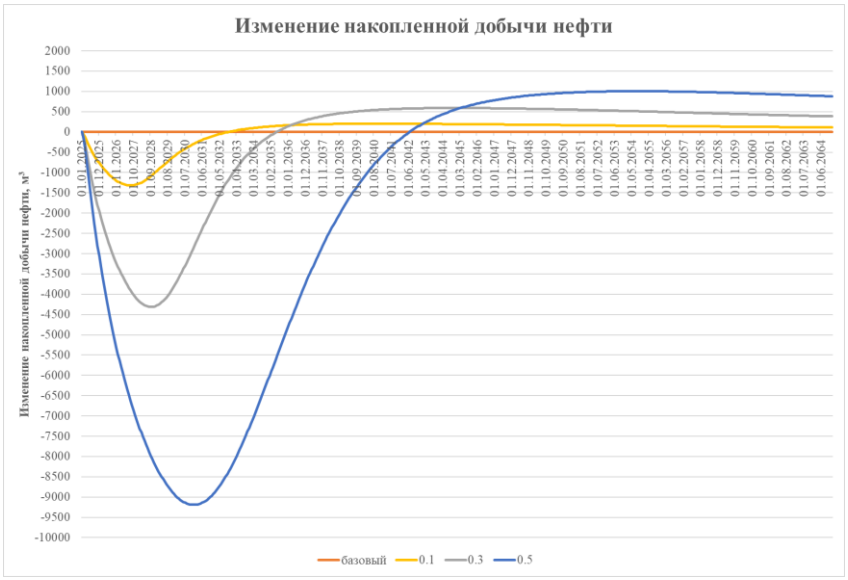

Рисунок 3 - Изменение накопленной добычи нефти по вариантам расчетов

Рисунок 4 - Накопленная добыча жидкости по вариантам расчетов

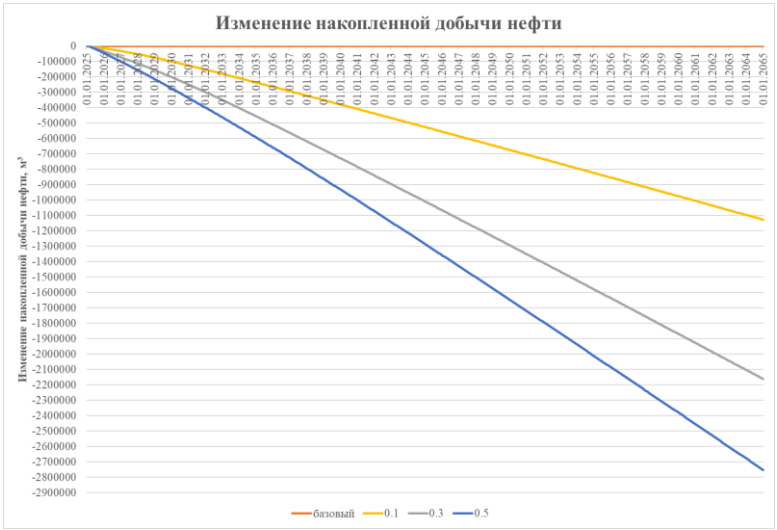

Рисунок 5 - Изменение накопленной добычи жидкости по вариантам расчетов

Приросты добычи нефти оказались незначительными. Например, для высокой обводненности, как на объекте исследования, был получен прирост коэффициента извлечения нефти 1,85 % [3]. При анализе мирового опыта, что приросты в работе вполне реалистичны [4]. В ходе работы не были заданы современные растворы полимеров, от которых происходит снижение остаточной нефтенасыщенности [5]. Снижение приемистости по нагнетательной скважины снижает пластовое давление по модели, из-за чего происходит снижение дебитов жидкости по добывающим скважинам. Однако происходит снижение обводненности продукции, соответственно снижается электроэнергия на добычу нефти.

Список литературы

1. Полимеры. – Текст: электронный / Studfiles: официальный сайт. – URL : https://studfile.net/preview/6145156 (дата обращения: 12.01.2025).

2. Мессояханефтегаз получил результаты испытаний технологии повышения нефтеотдачи с помощью полимерного заводнения / Д. Савосин – URL: http://neftegaz.ru (дата обращения: 12.01.2025). – Текст: электронный.

3. Зольников Д. Н., Оценка потенциала применения полимерного заводнения на нефтяном месторождении Западной Сибири / Д. Н. Зольников. – Текст: непосредственный / Известия высших учебных заведений. Нефть и газ. – 2024. – № 3 (165). – С. 73-82.

4. Прибылев Е. М., Анализ мирового опыта реализации технологии полимерного заводнения / Е. М. Прибылев. – Текст: непосредственный / Проблемы разработки месторождений углеводородных и рудных полезных ископаемых. – 2020. – Т. 2. – С. 332-336.

5. Оценка технологической эффективности полимерного заводнения на примере пласта Ю2 Усть-Тегусской площади месторождения им. Малыка / А.В. Кобяшев, А. А. Пятков, В. А. Захаренко [и др.]. – Текст: непосредственный / Известия высших учебных заведений. Нефть и газ. – 2023. – № 2 (158). – С. 41-61.

УДК 004.89

ПРЕИМУЩЕСТВА И НЕДОСТАТКИ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ

Пасынков Максим Александрович
Сенчик Василий Иванович
Куртинова Айжан Абаевна
Николаева Александра Евгеньевна
студенты
Научный руководитель: Куприянов Дмитрий Олегович,
ассистент
ФГБОУ ВО «Санкт-Петербургский государственный морской технический университет»,
город Санкт-Петербург

Аннотация. *Целью данной работы является изучения важности квантового распределения ключей в работе квантовых компьютеров. Описаны принципы работы квантового распределения ключей, возможности их дальнейшего развития, их преимущества, такие как: адаптивность протоколов, долговечность ключей, принцип «проверки подслушивания» и т.д. Также рассмотрены и недостатки - сложность реализации, уязвимости, проблемы совместимости и т.д.*

The aim of this work is to study the importance of quantum key distribution in the operation of quantum computers. The principles of quantum key distribution are described, along with the possibilities for their further development and their advantages, such as: adaptability of protocols, durability of keys, the principle of "eavesdropping detection", etc. The disadvantages are also discussed, including implementation complexity, vulnerabilities, compatibility issues, etc.

Ключевые слова: *квантовый компьютер, распределение ключей, уязвимости, преимущества, недостатки*

Keywords: *quantum computer, key distribution, vulnerabilities, advantages, disadvantages*

В развитие вопросов, рассмотренных в статье «Исследование необходимости применения квантовых компьютеров в криптографии» предлагается рассмотреть тему квантового распределения ключей. Квантовое распределение ключей (англ.: Quantum Key Distribution, QKD) — метод передачи ключа, который использует квантовые явления для гарантии безопасной связи. Эта технология позволяет двум сторонам, соединенным по открытому классическому каналу связи, создать общий случайный ключ, который известен только им, и использовать его для шифрования и расшифровки сообщений, передаваемых по классическому каналу. Алгоритм QKD обеспечивает безопасность передачи криптографических ключей на основе принципов квантовой механики, что делает его устойчивым к перехвату. Он защищает от атак квантовых компьютеров, которые могут угрожать традиционным криптографическим методам. С увеличением интереса к квантовым технологиям QKD становится важным инструментом для обеспечения безопасности данных в различных сферах. Постоянные исследования улучшают алгоритмы QKD, увеличивая их скорость и снижая стоимость оборудования**.** Алгоритм квантового распределения ключей является неотъемлемой программной частью квантового компьютера.

Квантовое распределение ключа. Это метод передачи ключа, который использует квантовые явления для обеспечения безопасности передачи данных. Данный метод позволяет двум сторонам передавать данные с помощью общего ключа, который будет использоваться для шифровки и дешифровки. Данный метод похож на AES, но обладает преимуществом, при попытке третьей стороны как-то завладеть или изменить информацию это приведет к аномалии, так как при квантовом распределении ключа используется фундаментальный аспект квантовой механики: процесс измерения квантовой системы нарушает её. Третья сторона, пытающаяся получить ключ, должна измерить передаваемые по

каналу связи квантовые состояния, что ведет к их изменению и появлению аномалии. С помощью квантовой суперпозиции (способность квантовых систем находиться в нескольких состояниях одновременно), квантовой запутанности (связь между квантовыми частицами, при которой изменение состояния одной мгновенно влияет на другую.) и передачи данных в квантовых состояниях можно осуществить канал связи, который обнаруживает аномалии. Если количество аномалий ниже определённого порога, то ключ будет создан, что гарантирует безопасность, третья сторона не имеет информации об этом, иначе секретный ключ не будет создан и связь прекратится.

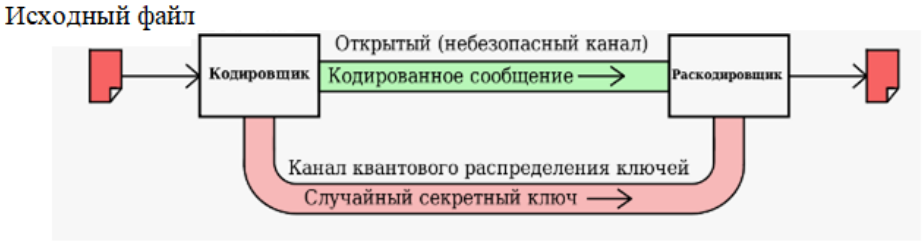

Рис. 1 Схема работы квантового распределения ключей

Протоколы квантового распределения ключей (QKD) — это методы, которые используют принципы квантовой механики для безопасной передачи криптографических ключей между двумя сторонами. Эти протоколы обеспечивают защиту от подслушивания и других атак, используя уникальные свойства квантовых систем, такие как суперпозиция и запутанность.

Протокол BB84. Протокол использует четыре квантовых состояния фотона, направление вектора поляризации, одно из которых выбирается в зависимости от передаваемого бита: $90°$ или $135°$ для 1, $45°$ или $0°$ для . Одна пара соответствует и и принадлежит базису. Другая пара соответственно $|0(\times)\rangle$ и $|1(\times)\rangle$ и принадлежит базису $\times$.

Этапы протокола BB84:

1. Подготовка кубитов:

– Отправитель (А.) подготавливает кубиты в одном из четырех возможных состояний:

– $|0\rangle$ (горизонтальное)

– |1⟩ (вертикальное)

– |+⟩ (диагональное)

– |-⟩ (антидиагональное)

– Состояния |0⟩ и |1⟩ измеряются в одной базе (базис Z), а состояния |+⟩ и |-⟩ — в другой базе (базис X).

2. Отправка кубитов:

– А. отправляет подготовленные кубиты получателю (Б.) через квантовый канал.

3. Измерение кубитов:

– Б. получает кубиты и измеряет их, выбирая случайные базисы (либо Z, либо X) для измерения каждого кубита.

4. Обмен базисами:

– После завершения измерений А. и Б. обмениваются информацией о выбранных базисах по классическому каналу, но не сообщают результаты измерений.

5. Формирование общего ключа:

– А. и Б. сохраняют только те результаты, где они использовали одинаковые базисы. Эти результаты формируют общий секретный ключ.

6. Проверка на подслушивание:

– А. и Б. могут провести проверку на наличие подслушивателей, сравнив часть своих измерений. Если результаты совпадают, это подтверждает безопасность ключа. Если обнаруживаются несоответствия, это может указывать на присутствие подслушивателя.

Преимущества:

– Гарантированная секретность ключа на расстоянии до 50 км

– Сложность перехвата данных

– Возможность определить попытки несанкционированного доступа к информации

Недостатки:

– Сложная реализация

– Сравнительно небольшое расстояние передачи (100-150 км)

– Необходимость двух каналов связи: квантового и классического

– Дорогостоящее оборудование

– Возможная потеря данных

Протокол B92.В протоколе используются фотоны, поляризованные в двух различных направлениях для представления нулей и единиц ($|\phi_0\rangle$и$|\phi_1\rangle, \langle\phi_0|\phi_1\rangle \neq 0$). Фотоны, поляризованные вдоль направления $45°$, несут информацию о единичном бите, фотоны, поляризованные вдоль направления — о нулевом бите.

Основные элементы протокола BB92:

1. **Кубиты**:

– А. использует два состояния кубитов: $|0\rangle$ и $|1\rangle$. Эти состояния могут быть представлены в виде векторов в двумерном гильбертовом пространстве:

– $|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$

– $|1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$

2. **Подготовка и отправка кубитов**:

– А. случайным образом выбирает одно из двух состояний ($|0\rangle$ или $|1\rangle$) и отправляет его Б.

3. **Измерение кубитов**:

– Б. измеряет полученные кубиты, используя базис Z ($|0\rangle$ и $|1\rangle$). Результат измерения определяется вероятностями:

– Если Б. измеряет $|0\rangle$, он получает результат 0 с вероятностью 1.

– Если Б. измеряет $|1\rangle$, он получает результат 1 с вероятностью 1.

4. **Обмен результатами**:

– После завершения измерений А. и Б. обмениваются информацией о том, какие кубиты были отправлены и какие были измерены, но не сообщают результаты измерений.

5. **Формирование общего ключа**:

– Б. сохраняет только те результаты, где он использовал базис Z. Эти

результаты формируют общий секретный ключ.

6. **Проверка на подслушивание**:

– Для проверки на подслушивание А. и Б. могут сравнить часть своих измерений. Если результаты совпадают, это подтверждает безопасность ключа. Если обнаруживаются несоответствия, это может указывать на присутствие подслушивателя.

Преимущества:

– Использование фотонов с двумя типами поляризации (вместо четырёх)

– Простота схемы реализации

Недостатки:

– Меньшая эффективность

– Гарантированная секретность ключа на расстоянии до 20 км

– Нет гарантий полной передачи данных

Протокол E91. В 1991 Артур Экерт предположил, что квантовое распределение ключей можно осуществить с помощью квантовой запутанности. Кроме участников Васи и Саши, есть источник создания запутанных частиц, который присылает частицы Васе и Саше. Протокол Экерта точнее определяет реальную ситуацию, так как из-за ограничения передачи на большие расстояния, передача будет включать в себя центральный источник, такой как спутник, который будет пересылать нескольким приемникам. Для объяснения могут использоваться многие физические величины, но Экерт использует синглетные состояния. Вместо того, чтобы доверять источнику, который может быть в руках Евы, Экерт настроил протокол, таким образом, что источник испускает пары частиц со спином $\frac{1}{2}$ в синглетых состояниях $\phi = \frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle)$. Вася и Саша должны выбрать одну из трех осей, в которых будут проводиться измерения входных частиц.

Основные этапы:

1. **Создание запутанных пар**: В. создает запутанные пары кубитов и отправляет один кубит каждой пары С.

2. **Измерение**: B. измеряет полученные кубиты, выбирая случайные базисы.

3. **Обмен базисами**: B. и C. обмениваются информацией о выбранных базисах.

4. **Формирование ключа**: сохраняются только результаты с одинаковыми базисами, формируя общий секретный ключ.

5. **Проверка на подслушивание**: сравниваются части измерений для обнаружения подслушивания.

Преимущества:

– Использует квантовую запутанность, что обеспечивает высокий уровень безопасности.

– Позволяет обнаруживать попытки подслушивания благодаря свойствам запутанных состояний.

Недостатки:

– Сложность в реализации, так как требуется создание и передача запутанных пар кубитов.

– Зависимость от качества квантового канала и измерительных устройств.

Преимущества QKD

Сопротивляемость к вычислительным атакам. Сопротивляемость квантового распределения ключа (QKD) к вычислительным атакам заключается в нескольких ключевых аспектах:

Принцип неопределенности: Невозможность точности измерения и видимость любого вмешательства

Квантовая запутанность: QKD использует явление квантовой запутанности, при котором два или более квантовых объекта становятся взаимосвязанными, что означает что изменение дргого объекта повлечет за собой изменение второго. Она так же, как и принцип неопределенности помогает увидеть любое вмешательство.

Отказ от вычислительных предположений: QKD не полагается на вычислительные трудности. Это делает его более устойчивым к будущим угрозам,

связанным с развитием квантовых вычислений, которые могут угрожать традиционным криптографическим методам.

Физическая реализация: Устойчивость QKD также зависит от физической реализации системы. Современные протоколы учитывают потенциальные атаки на физическом уровне, такие как атаки на источники фотонов или детекторы. Разработка новых технологий и методов защиты помогает минимизировать риски, связанные с такими атаками.

Принцип «проверки на наличие подслушивания». Он основан на использовании квантовых свойств для обнаружения вмешательства в процесс передачи информации. Этот принцип включает несколько ключевых аспектов:

Сравнение результатов: после передачи ключа отправитель и получатель могут сравнить часть своих измерений. Например, они могут заранее согласовать, какие из переданных кубитов будут проверены. Если результаты совпадают, это указывает на то, что не было вмешательства. Если результаты различаются, это сигнализирует о возможном прослушивании.

Проверка ошибок: В процессе проверки на наличие подслушивания стороны могут использовать специальные протоколы для оценки целостности ключа. Если обнаруживаются ошибки, это может указывать на то, что злоумышленник пытался вмешаться в передачу.

Секретные битовые строки: В некоторых протоколах QKD отправитель передает кубиты, которые могут быть в разных состояниях и в разных базах. Получатель измеряет эти кубиты в своих собственных базах. После этого стороны могут обменяться информацией о том, в каких базах они проводили измерения, и отсеивать те кубиты, для которых они использовали разные базы. Это позволяет им сохранить только те кубиты, которые были измерены в одинаковых базах, тем самым минимизируя риск утечки информации.

Недостатки QKD

Техническая сложность: Реализация QKD требует сложного и дорогостоящего оборудования, включая квантовые источники и детекторы. Все оборудование должно штатно работать, что требует слаженной работы технических

специалистов – с этим также могут возникнуть проблемы.

Ограниченная дальность: на текущий момент QKD имеет ограничения по расстоянию, на котором можно безопасно передавать ключи. На больших расстояниях из-за особенностей оптических волокон могут быть проблемы с качественной передачей данных, что может привести к полной потери информации.

Скорость передачи: Скорость передачи данных с использованием QKD может быть ниже, чем у традиционных методов, что ограничивает его применение в некоторых областях.

Уязвимости к физическим атакам: хотя QKD защищает от вычислительных атак, она может быть уязвима к физическим атакам, таким как атаки на оборудование или каналы передачи.

Необходимость в доверенной среде: для некоторых протоколов QKD требуется наличие доверенной среды, что может ограничивать их применение в реальных условиях. Не всегда и не везде можно обеспечить безопасную среду для выполнения процессов.

Сложности интеграции с существующими системами: Интеграция QKD в существующие криптографические системы и инфраструктуры может быть сложной задачей. Различные протоколы и принципы работы – главная проблема гибридных схем.

Интеграция QKD на сегодняшний день. Оптоволоконные сети: QKD может быть интегрировано в существующие оптоволоконные сети. Например, квантовые ключевые распределительные устройства могут быть установлены на узловых точках сети, позволяя пользователям генерировать и обмениваться ключами в режиме реального времени.

Спутниковая связь: QKD может быть использовано для обеспечения безопасной связи между спутниками и наземными станциями. Это особенно актуально для военных и правительственных приложений, где безопасность данных критически важна.

Облачные сервисы: QKD может быть использовано для генерации ключей, которые затем используются для шифрования данных, хранящихся в

облачных сервисах.

Финансовые системы: банковские транзакции: QKD может быть использовано для безопасного обмена ключами при проведении финансовых транзакций, обеспечивая защиту от мошенничества и утечек данных.

Электронная коммерция: интеграция QKD в платформы электронной коммерции может улучшить безопасность платежей и защитить личные данные клиентов.

Вывод. Таким образом, алгоритм квантового распределения ключей является важным программным элементом квантового компьютера. QKD на сегодняшний день - лучший способ шифрования данных для квантового компьютера, который сочетает в себе сопротивляемость к вычислительным атакам и способность определять проникновение в систему. Названные выше недостатки в будущем будут решены с помощью оптимизации алгоритмов, более современных технологий и новых материалов для комплектующих квантовых компьютеров, способных повысить скорость и качество передачи информации.

Список литературы

1. Голубчиков Д. М., Румянцев К. Е. Квантовая криптография: принципы, протоколы, системы. — С. 37. Архивировано 30 ноября 2016 года.

2. Голубчиков Д. М. Методика исследования и оценивания систем квантового распределения ключей / Известия ЮФУ. Технические науки. — 2009. — С. 154-159. Архивировано 20 декабря 2016 года.

3. Кронберг Д. А., Ожигов Ю. И., Чернявский А. Ю. Квантовая криптография. Учебное пособие. — МГУ имени М. В. Ломоносова. — С. 112. Архивировано 30 ноября 2016 года.

УДК 004.89

ИССЛЕДОВАНИЕ НЕОБХОДИМОСТИ ПРИМЕНЕНИЯ КВАНТОВЫХ КОМПЬЮТЕРОВ В КРИПТОГРАФИИ

Сенчик Василий Иванович
Пасынков Максим Александрович
Куртинова Айжан Абаевна
Николаева Александра Евгеньевна
студенты
Научный руководитель: Куприянов Дмитрий Олегович,
Ассистент
ФГБОУ ВО «Санкт-Петербургский государственный морской технический университет»

Аннотация. *Нынешние криптографические алгоритмы могут лишь отсрочить на небольшой период времени дешифровку критически важных данных. Появление квантовых компьютеров, принципы работы, строение, потенциал и отличительные особенности основные алгоритмы которых, такие как Алгоритм Шора и Гровера, приведут к резкому росту вычислительных мощностей и зарождению постквантовой криптографии. Поэтому важен вопрос о практическом применении квантовых компьютеров в криптографической среде. Целью работы является анализ дальнейшего развития криптографии и криптографических алгоритмов при внедрении квантовых компьютеров, анализ появления постквантовой криптографии и оценка влияния квантовых алгоритмов на современные.*

Current cryptographic algorithms can only delay for a short period of time the decryption of critical data. The emergence of quantum computers, the principles of operation, structure, potential and distinctive features of the main algorithms of which,

such as Shor and Grover Algorithm, will lead to a sharp increase in computing power and the birth of post-quantum cryptography. Therefore, the question of practical application of quantum computers in cryptographic environment is important. The aim of the paper is to analyse the further development of cryptography and cryptographic algorithms with the introduction of quantum computers, to analyse the emergence of post-quantum cryptography and to assess the impact of quantum algorithms on modern ones.

Ключевые слова: *квантовый компьютер, квантовые алгоритмы, алгоритмы шифрования, криптография*

Keywords: *quantum computer, quantum algorithms, encryption algorithms, cryptography*

В современном мире все чаще встает вопрос о безопасности того или иного ресурса. Компании обеспокоены отсутствием должного уровня безопасности в информационной среде. Все нынешние криптографические алгоритмы могут лишь отсрочить на небольшой период времени дешифровку критически важных данных. На смену устаревшим компьютерам придут квантовые компьютеры, в основе работы которых будет лежать квантовая механика. Появление таких компьютеров приведёт к зарождению постквантовой криптографии. Алгоритмы, основанные на такой криптографии, будут отличаться большим уровнем безопасности и вычислительной скорости. В данной работе будет рассматриваться процесс развития таких алгоритмов.

Постановка задачи. Исходя из вышеизложенного, появляется необходимость исследования принципов постквантовой криптографии. Это включает в себя анализ квантовых алгоритмов и сравнение их с существующими, исследования квантового компьютера, принципов его работы и возможностей в криптографии.

Понятие квантового компьютера. Квантовый компьютер — вычислительное устройство, которое использует явления квантовой механики для передачи и обработки данных. Главное отличие обычного компьютера от квантового заключается в том, что первый оперирует битами (Обычные компьютеры

используют биты как основную единицу информации. Бит может находиться в одном из двух состояний: 0 или 1), в то время как второй имеет кубиты (Кубит может находиться не только в состоянии 0 или 1, но и в состоянии суперпозиции, что означает, что он может одновременно представлять и 0, и 1 с определёнными вероятностями.) находящиеся в суперпозиции. Кубиты могут быть взаимосвязаны через квантовую запутанность. Это означает, что состояние одного кубита может зависеть от состояния другого, даже если они находятся на большом расстоянии друг от друга. Так же благодаря вышеперечисленным преимуществам квантовый компьютер обладает параллелизмом, что означает, что он может выполнять несколько задач одновременно. Но главным плюсом является вычислительная мощность, ведь задачи, с которыми обычный компьютер или даже суперкомпьютер будут справляться десятки, а то и сотни лет, квантовый компьютер будет способен решить за пару секунд. Но также у квантового компьютера имеются и недостатки, такие как ограниченность определенными алгоритмами, т.е. в данных реалиях квантовый компьютер способен выполнять исключительно определенные задачи, в то время как обычный компьютер имеет огромный функционал.

Алгоритм Шора. Американский математик Питер Шор в 1994 году разработал квантовый алгоритм для целочисленной факторизации. Алгоритм использует математический метод определения периода функции и может быть настроен для решения задач вычисления дискретного логарифма в конечной группе или группе точек эллиптических. Работоспособность алгоритма Шора была наглядно продемонстрирована в 2001 году на примере факторизации числа 15 на квантовом компьютере состоящим всего лишь из 7 кубитов. В момент создания квантового компьютера достаточной мощности алгоритм Шора позволит эффективно (за время, лишь ненамного превосходящее требующееся для зашифрования) взламывать большинство используемых сейчас асимметричных криптографических алгоритмов (RSA, DSA, EdDSA, ГОСТ Р 34.10-2012 и других).

В таблице ниже приведены актуальные на начало 2021 года рекорды по факторизации чисел, используемых в качестве открытого ключа в наиболее

распространенной криптосистеме с открытым ключом RSA. Для сравнения также даны рекорды факторизации, достигнутые на классических компьютерах.

Таблица 1 - Сравнение факторизации чисел двух типов компьютеров

Год	Число (квантовый компьютер)	Число (обычный компьютер)
2012	143 (8 битов)	RSA-768 (768 битов)
2014	56135 (16 битов)	-
2016	200 099 (18 битов)	-
2019	291 311 (18 битов)	RSA-240 (795 битов)
2020	1 099 551 473 989 (41 бит)	RSA-250 (829 битов)

Ниже приведен график построенной по второй колонке данной таблицы экстраполирующей функции (по оси X — год, по оси Y — количество битов в числах RSA, факторизуемых квантовым вычислителем).

Если учитывать, что современные международные рекомендации по защите информации предполагают использование в криптосистеме RSA чисел размера не менее 2048 битов (рекомендовано 3072), можно сделать вывод о том, что квантовые компьютеры, способные эффективно решать задачи криптоанализа используемых сейчас криптосистем, будут доступны в диапазоне 2028-2033 годов.

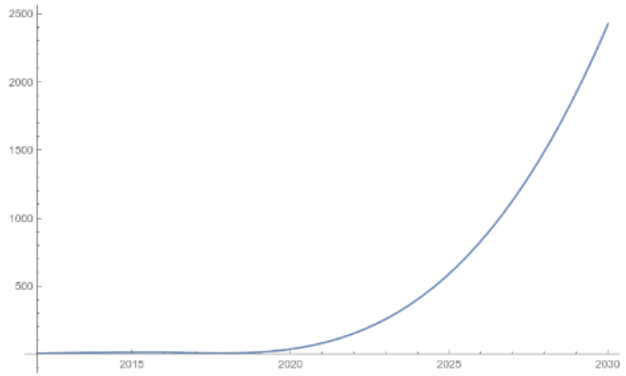

Рис. 1- График роста мощности квантовых компьютеров

Отметим также, что часть указанных в таблице рекордов по факторизации чисел получены при помощи прототипов квантовых компьютеров, реализующих модели, которые ранее считались не вполне подходящими для решения задач криптоанализа, таких как модель «квантового отжига», реализованного в квантовых вычислителях производства компании D-Wave. На стойкость симметричных шифров (AES, Кузнечик и других) и хэш-функций (SHA, Стрибог и других) алгоритм Шора не оказывает влияния, поскольку для их анализа применяются другие, не столь эффективные алгоритмы (метод Гровера, Саймона, BHT и другие), для успешной защиты от которых достаточно увеличить размер параметров в 2-3 раза.

Алгоритм Гровера. Американским математиком Ловом Гровером в 1996 году был предложен квантовый алгоритм решения задачи перебора, то есть нахождения решения уравнения $f(x) = 1$, где f есть булева функция от n переменных. В последствии был назван в честь математика — Алгоритм Гровера (также GSA от англ. Grover search algorithm).

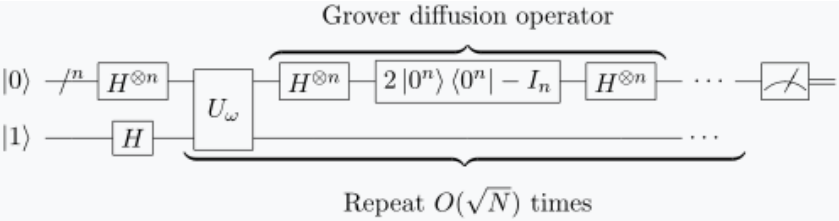

Рис. 2. - Схема работы алгоритма Гровера

Предполагается, что функция f задана в виде чёрного ящика, или оракула, то есть в ходе решения можно задавать оракулу только вопрос типа: «чему равна f на данном x?», и использовать ответ в дальнейших вычислениях. То есть, задача решения уравнения (1) является общей формой задачи перебора: здесь требуется отыскать «пароль к устройству f», что классически требует полного перебора всех $N = 2^n$ вариантов.

Алгоритм Гровера находит какой-нибудь корень уравнения, используя $\frac{\pi}{4}\sqrt{N}$ обращений к функции f, с использованием $O(n)$ кубитов.

Смысл алгоритма Гровера состоит в так называемой «усилении

амплитуды» целевого состояния за счёт убывания амплитуды всех других состояний. Геометрически алгоритм Гровера заключается во вращении текущего вектора состояния квантового компьютера по направлению точно к целевому состоянию (движение по наикратчайшему пути обеспечивает оптимальность алгоритма Гровера). Каждый шаг дает вращение на угол $2a$, где угол между I_0 и $I_{x_{tar}}$ составляет $\frac{\pi}{2} - a$. Дальнейшее продолжение итераций оператора G даст продолжение обхода окружности в вещественной плоскости, порождённой данными векторами.

Гроверовское «усиление амплитуды» является, по-видимому, фундаментальным физическим феноменом в квантовой теории многих тел, например, его учёт необходим для оценки вероятностей событий, которые кажутся «редкими». Процесс, реализующий схему алгоритма Гровера, приводит к взрывному росту первоначально пренебрежимо малой амплитуды, что способно быстро довести её до реально наблюдаемых величин.

Алгоритм Гровера также может быть использован для нахождения медианы и среднего арифметического числового ряда. Кроме того, он может применяться для решения NP-полных задач путём исчерпывающего поиска среди множества возможных решений. Это может повлечь значительный прирост скорости по сравнению с классическими алгоритмами, хотя, и не предоставляя «полиномиального решения» в общем виде.

Сравнение производительности обычного и квантового компьютера. *Классические компьютеры:* Пиковая производительность измеряется в FLOPS (операциях с плавающей запятой в секунду) или инструкциях в секунду (IPS). Топовые суперкомпьютеры достигают примерно 200 петаFLOPS (200 миллионов миллиардов операций в секунду).

Квантовые компьютеры: Производительность измеряется в квантовых операциях в секунду (QOPS) или квантовом объеме (мере числа кубитов и коррекции ошибок). Современные квантовые компьютеры достигают примерно 10^6 QOPS.

Проблемы и ограничения квантового компьютера.

– **Коррекция ошибок:** Квантовые компьютеры требуют сложных методов коррекции ошибок для поддержания хрупких квантовых состояний кубитов.

– **Шум и декогеренция:** Квантовые компьютеры подвержены шуму и декогеренции, что может разрушать квантовые состояния и снижать производительность.

– **Масштабируемость:** в настоящее время большинство квантовых компьютеров имеют малый масштаб и нуждаются в увеличении, чтобы справляться с комплексными задачами.

Понятие Конфайнмента. Конфайнмент - (от англ. confinement — удержание, заточение) — явление в физике элементарных частиц, состоящее в невозможности получения кварков в свободном состоянии.

Ученые из центра CCQ при Институте Флэтайрона с помощью такого эффекта, как конфайнмент смогли выполнить задачи, ранее доступные лишь в одномерных квантовых системах, на классическом компьютере, что привело к разрушению монополии квантовых компьютеров.

В ходе исследования ученые изучили двумерную квантовую систему переворачивающихся магнитов и обнаружили, что наличие конфайнмента сдерживало рост запутанности в системе, что и сделало задачу решаемой на классическом компьютере. Это открытие помогает четче определить границу между возможностями классических и квантовых компьютеров, которая до сих пор оставалась размытой. В квантовых масштабах отдельный магнит может быть ориентирован вверх или вниз, или он может находиться в суперпозиции — квантовом состоянии, в котором он одновременно указывает вверх и вниз. То, насколько вверх или вниз направлен магнит, влияет на то, сколько энергии он имеет, когда находится в магнитном поле. В первоначальной настройке системы все магниты были направлены в одном направлении. Затем система была возмущена небольшим магнитным полем, заставив некоторые магниты перевернуться, что также побудило соседние магниты перевернуться. Такое поведение — когда магниты влияют на переворачивание друг друга — может привести к запутыванию, то

есть связыванию суперпозиций магнитов. Со временем возросшая запутанность системы затрудняет моделирование на классическом компьютере. Но в закрытой системе имеется ограниченное количество энергии, что ограничивает масштаб запутанности. Было показано, что энергии достаточно для того, чтобы перевернуть небольшие, изолированные кластеры магнитов, что ограничивало запутанность. Это явление, названное конфайнментом, объясняет, почему классический компьютер смог выполнить задачу. Исследование продемонстрировало, что в двумерных квантовых системах с замкнутой геометрией возможен конфайнмент, аналогичный явлению, наблюдаемому в одномерных системах. Это значительно упрощает математическое описание системы и делает ее доступной для классических вычислений.

Таким образом, математическая модель конфайнмента может быть применима к ряду других двумерных квантовых систем. Она не только помогает глубже понять квантовые процессы в таких системах, но и предоставляет ученым полезный инструмент для анализа и разработки новых симуляций, которые позволят исследовать границы возможностей квантовых и классических компьютеров.

Прототипы квантовых компьютеров на сегодняшний день. На данный момент существует множество прототипов квантовых компьютеров, которые применяются в различных сферах жизни общества.

1. IBM Quantum Condor. Самый мощный квантовый компьютер, представленный в 2023 году, с 433 кубитами. Однако он не доступен для широкого использования и работает только в лабораторных условиях.

2. Intel Tunnel Falls. В середине 2023 года компания выпустила свой первый 12-кубитный квантовый кремниевый чип.

3. MosaiQ от Quandela. В октябре 2023 года французский стартап поставил свой первый квантовый компьютер MosaiQ в один из дата-центров ведущего облачного провайдера Европы OVHcloud. На данный момент у него шесть кубитов, но для большинства сложных коммерческих задач этого более чем хватит.

4. D-Wave 2000Q. В 2022 году D-Wave совместно с Volkswagen

использовал свой 2000-кубитный адиабатический квантовый компьютер D-Wave 2000Q для планирования оптимальных маршрутов для такси в Пекине.

Заключение. Таким образом, основываясь на всем вышесказанном, можно сделать вывод, что внедрение квантовых компьютеров является важным этапом развития криптографии. В современном мире ни одна сфера не остается без внедрения новых технологий. Постоянная эволюция и совершенствование процессов, алгоритмов и методов – именно это требуется для современной безопасности данных. Исследование квантовых компьютеров является одной из ведущих тем информационных технологий. Квантовый компьютер дает начало новой эре развития шифрующих алгоритмов и технологий, развитие таких компьютеров является большим шагом для всей криптографии как науки в целом. Данное исследование ориентировано на то, чтобы предложить полезные сведения как для профессионалов в области криптографии, так и для рядовых пользователей, выявить сильные и слабые стороны новых технологий. В данной работе продемонстрирована важность внедрения квантовых технологий в современные системы безопасности.

Список литературы

1. Валиев К. А., Кокин А. А. Квантовые компьютеры: надежды и реальность. — Ижевск: РХД, 2004. — 320 с.

2. Квантовый компьютер и квантовые вычисления Архивная копия от 16 марта 2021 на Wayback Machine / Под ред. Садовничего В. А.

3. Прескилл Дж. Квантовая информация и квантовые вычисления. — Ижевск: РХД, 2008—2011. — 464+312 с.

4. Кайе Ф., Лафламм Р., Моска М. Введение в квантовые вычисления. — Ижевск: РХД, 2009. — 360 с.

5. Нильсен М., Чанг И. Квантовые вычисления и квантовая информация. — М.: Мир, 2006. — 824 с

ЮРИДИЧЕСКИЕ НАУКИ

УДК 340

НЕЗАВИСИМАЯ ГАРАНТИЯ КАК СПОСОБ ОБЕСПЕЧЕНИЯ ИСПОЛНЕНИЯ ОБЯЗАТЕЛЬСТВ

Полухина Ирина Игоревна

магистрант

Научный руководитель: Кубиевич Светлана Владимировна,

к.э.н., доцент

НОЧУ ВО «Московский финансово-промышленный университет «СИНЕРГИЯ», г. Волгоград

Аннотация. *В статье рассмотрены вопросы применения банковской гарантии, особенности ее использования в гражданском праве. Проанализирована сущность банковской гарантии как способа обеспечения исполнения обязательств в гражданском праве.*

Ключевые слова: *обеспечение исполнения обязательств, независимая гарантия, обеспечительный договор, гражданское право*

Проблема обеспечения исполнения обязательств является одной из наиболее актуальных в современном гражданском праве, и в особенности в коммерческих правоотношениях.

Одним из путей обеспечения исполнения обязательств является независимая гарантия, предусмотренная ст. Гражданского кодекса Российской Федерации от 30.11.1994 № 51-ФЗ (далее – ГК РФ) [1]. По независимой гарантии гарант принимает на себя по просьбе другого лица (принципала) обязательство уплатить указанному им третьему лицу (бенефициару) определенную денежную сумму в соответствии с условиями данного гарантом обязательства независимо от действительности обеспечиваемого такой гарантией обязательства.

Кауза договора в широком смысле представляет собой тот юридический

фат, который лежит в основе возникновения правоотношений. Независимая гарантия является одним из видов обеспечительных договоров. При рассмотрении каузы обеспечительного договора в правовой литературе фиксируется ряд противоречий. Это обусловлено тем, что любой договор порождает, так или иначе, обязанность одного лица по отношению к другому или взаимные обязанности. В рамках этого существует точка зрения, в соответствии с которой обеспечительный договор не следует выделять в отдельный вид договора, так как его кауза – возникшее обязательство присутствует во всех видах договоров.

Ряд других авторов, напротив, указывают на то, что обеспечительный договор имеет собственную, отличную от иных видов договоров каузу, и она состоит не столько в возникновении обязательства, сколько в установлении конкретного вида обеспечения исполнения данного обязательства.

Условно, если любой иной договор (купли-продажи, подряда и др.), диктует только какое именно, в каком объеме обязательство должно быть исполнено и при наступлении каких условий, то обеспечительный договор расширяет эти условия до того момента, что указывает, каким именно способом исполняется обязательство, называет в материалом эквиваленте размер обязательства и подразумевает, что «стоимость» обязательства уже заведомо передана потенциальным должником, но может быть возвращена ему, если он исполнит обязательство иным способом.

Ряд авторов указывают на то, что независимая гарантия всегда подчинена какому-то иному договору, и на основании этого, ее кауза несамостоятельна. То есть юридический факт независимой гарантии не может возникнуть сам по себе, без некоего – первичного, основного договора.

Данная точка зрения в практике находит подтверждение, что наиболее наглядно можно продемонстрировать на примере договора залога. Например, если кредитор и должник заключают договор займа, то в обеспечение исполнения этого договора займа стороны также заключают дополнительный договор залога имущества. В данном случае договор займа – это основное обязательство, а договор залога как способ обеспечения его исполнения будет вторичным. При

неисполнении условий основного договора кредитор сможет удовлетворить интересы за счет и на основании условий «дополнительного» договора залога – путем обращения взыскания на заложенное имущество должника.

Если целью договора выступает создание (оформление) правоотношения – обладатель некоего блага получает обязанность удовлетворить потребность другого – заинтересованного в получении этого блага лица, то и основанием договора будут конкретные юридические значимые обстоятельства и факты – то есть, собственно, кауза договора [2]. Аналогично это предположение можно распространить и на обеспечительные договоры, цель которых – установление конкретного способа обеспечения обязательств, защиты сторон в договорных отношениях.

В рамках такого подхода кауза обеспечительного договора, и в том числе, независимой гарантии – это уже имеющееся обязательство одной стороны в отношении другой или взаимное их обязательство. В связи с этим, на основании такого подхода обеспечительный договор можно выделить в отдельный вид договора. Это обусловлено тем, что для того, чтобы обеспечительный договор и соответствующие правоотношения возникли, обязательство уже должно существовать.

Для признания цели договора и каузысинонимами в теории и судебной практикенеобходимо, чтобы кауза (causa) являлась законной и осуществимой. Если у сторон цель при заключении договора не соответствует императивным требованиям, то говорить о безупречности и каузе в конкретном договоре нельзя. Это распространяется и на обеспечительные договоры, так, например, если обеспечительный договор подразумевает несопоставимые условия с основным обязательством, то он не может быть признан правомерно заключенным.

В этом смысле – на первый план выходит именно специфическая кауза обеспечительного договора – наличие обязательства и необходимость (либо желание одной из сторон) защиты в рамках этого обязательства сторон договора.

Интересно, что заключение обеспечительного договора представляет собой по смыслу, достаточно интересный юридический факт, указывающий на то,

что одна из сторон либо обе, сомневаются в полноценном исполнении обязательств.

Стороны при заключении любого договора осознают, какое основание лежит в договоре, какие устанавливаются текстом договора права и обязанности для каждой из сторон. Следовательно, заключая договор обе стороны осознают необходимость исполнения «своего» обязательства. При таком подходе обеспечительный договор, как «дополнительный» необходим при условии, если один из участников сделки сомневается в своих возможностях исполнения обязательств. К примеру, если должник, заключив договор займа, опасается, что не сможет по независящим от него причинам полностью исполнить обязательство (к примеру, если его доход снизится), то в качестве гаранта он может предложить кредитору независимую гарантию.

Сложность независимой гарантии и ее особенность состоит в том, что как юридический факт она реализуется (то есть договор исполняется) только в том случае если наступит первичный юридический факт – неисполнение обязательства должником (должниками) по договору. По сути, обеспечительный договор может быть не реализован, он не предполагает обязательного исполнения, в отличие, к примеру, от договора купли продажи, когда исполнение договора ставится в прямую зависимость от того факта, что предмет купли продажи передан и за него получены установленные условиями и соглашением сторон финансовые средства [2].

В отличие от такого договора, независимая гарантия не подлежит обязательному исполнению, а его исполнение ставится в зависимость от наступления иного юридического факта – неисполнения обязательств одной из сторон или сторонами договора.

В силу банковской гарантии банк, иное кредитное учреждение или страховая организация (гарант) дают по просьбе другого лица (принципала) письменное обязательство уплатить кредитору принципала (бенефициару) в соответствии с условиями даваемого гарантом обязательства денежную сумму по представлении бенефициаром письменного требования о ее уплате. Банковская

гарантия обеспечивает надлежащее исполнение принципалом его обязательства перед бенефициаром (основного обязательства).

По договору поручительства поручитель обязывается перед кредитором другого лица отвечать за исполнение последним его обязательства полностью или в части. Договор поручительства может быть заключен также для обеспечения обязательства, которое возникнет в будущем. Договор поручительства должен быть совершен в письменной форме. Несоблюдение письменной формы влечет недействительность договора поручительства [3].

Залог, банковская гарантия и поручительство также являются действенными мерами обеспечения договора. Они являются хорошими стимулами для должника по неукоснительному исполнению договорных обязательств, так как повышают для кредитора вероятность удовлетворения его требования за счет соответствующего обеспечения.

Ряд авторов рассматривает независимую гарантию, как представление об обязательствах другой стороны или сторон. С этой точки зрения независимая гарантия также имеет некоторые отличия, поскольку именно независимая гарантия позволяет наиболее полно охарактеризовать и выразить в финансовом эквиваленте обязательства второй стороны или сторон договора.

Представления об обязательствах другой стороны существует для любого типа договора, так как любой договор заключается с целью взаимного исполнения обязательств, и стороны, соответственно, ожидают друг от друга их исполнения [4].

При этом независимая гарантия позволяет сторонам не только точно представить материальное выражение обязательств, но и устанавливает возможность их исполнения, средства исполнения и условия.

Таким образом, независимая гарантия имеет ряд характерных особенностей:

1. Она вторична по отношению к «основному» договору – тому, на основании которого возникли обязательства [2].

2. Независимая гарантия подразумевает, что условием ее реализации будет

«первичный» юридический факт – неисполнение обязательства. По сути, договор может быть и не реализован, то есть сделка, оформленная им, не состоится, если исполнятся условия «основного договора» [3].

3. Независимая гарантия играет «защитную» роль – она призвана изначально защитить интересы участников договорных отношений и выразить в материальном эквиваленте объем обязательств, а также средства их исполнения.

Перечисленные особенности независимой гарантии обуславливают сложность его правового регулирования и некоторые проблемы правоприменения в рамках судебной практики.

Список литературы

1. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ (ред. от 08.08.2024, с изм. от 31.10.2024) / СПС Консультант Плюс URL: https://www.consultant.ru/document/cons_doc_LAW_5142/03edc46b2ef855fddfaaa3d77dac1d071ef3dba1/

2. Белобородов М. В. Правовое содержание независимой гарантии как способа обеспечения обязательств на рынке публичных торгов / Азиатско-Тихоокеанский регион: экономика, политика, право. – 2021. – №1. – URL: https://cyberleninka.ru/article/n/pravovoe-soderzhanie-nezavisimoy-garantii-kak-sposoba-obespecheniya-obyazatelstv-na-rynke-publichnyh-torgov (дата обращения: 23.01.2025).

3. Васильев В. В. Сущность метода гражданско-правового регулирования в современных реалиях / Юридическая наука. – 2012. - № 2. – С. 61 – 65.

4. Пестикова Т. А. Банковская гарантия как способ обеспечения исполнения государственного контракта / Ученые записки Тамбовского отделения РоСМУ. – 2018. №10. – URL: https://cyberleninka.ru/article/n/bankovskaya-garantiya-kak-sposob-obespecheniya-ispolneniya-gosudarstvennogo-kontrakta (дата обращения: 23.01.2025).

«СОВРЕМЕННАЯ НАУКА: ЭКСПЕРИМЕНТ И НАУЧНАЯ ДИСКУССИЯ»

XXX Международная научно-практическая конференция

Научное издание

ООО «НИЦ ЭСП» в ЮФО
(Подразделение НИЦ «Иннова»)
353445, Россия, Краснодарский край, г.-к. Анапа,
ул. Весенняя, 8, оф. 1
Тел.: 8-800-201-62-45; 8 (861) 333-44-82

Подписано в печать 27.01.2025 г. Формат 60x84/16. Усл. печ. л. 2,96
Бумага офсетная. Печать: цифровая. Гарнитура шрифта: Times New Roman
Тираж 50 экз. Заказ 975