Информационные процессы, Том 25, № 3.1, 2025, стр. 559–572.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Исследование безопасности квантовых вычислений классическими алгоритмами шифрования

Р. Р. Абдуллин, Д. А.Егоров, Н. В. Крупенина, В. Ю. Рудь, Ю. Д. Сапожникова

Государственный университет морского и речного флота им. адмирала С. О. Макарова, Санкт-Петербург, Россия

Поступила в редколлегию 10.04.2025 г. Принята 25.11.2025 г.

Аннотация—В статье проводится исследование потенциальных угроз классическим алгоритмам криптографии от квантовых компьютеров и их постоянно растущих мощностей. Рассмотрены существующие методы криптографических алгоритмов и их устойчивость квантовому взлому. Модификация этих алгоритмов в настоящее время способна защитить информацию от атак квантовых компьютеров, но в долгосрочной перспективе необходима разработка новых методов постквантовой криптографии. Особую важность приобретает разработка и совершенствование идентификаторов компрометации данных, для предотвращения копирования данных для их последующего взлома. Для решения этой проблемы предлагается интеллектуальная система защиты компьютерной сети на основе анализа индикаторов компрометации, взятых из журнала безопасности компьютерной сети. Система основана на алгоритмах классификации и позволяет разделить все подозрительные действия в сети на классы опасности (очень опасно, нужно обратить внимание, не стоит внимания).

Ключевые слова: квантовые вычисления, постквантовая криптография, кибербезопасность, алгоритмы шифрования, компрометации данных.

DOI: 10.53921/18195822_2025_25_3.1_559

1. ВВЕДЕНИЕ

В настоящее время происходит бурное развитие квантовых технологий [1]. С их развитием возникает необходимость переосмыслить существующие подходы к обеспечению безопасности данных. Классические алгоритмы шифрования, симметрические и асимметрические, такие как AES и RSA, соответственно, долгое время служили и служат основой для защиты информации. Однако с появлением квантовых компьютеров, способных эффективно и в разы быстрее, чем классические компьютеры, решать задачи, на которых основаны эти алгоритмы, возникает вопрос о их жизнеспособности и устойчивости к новым угрозам [2].

Основными угрозами для стандартных алгоритмов шифрования, происходящими от квантовых вычислителей, считаются атаки алгоритмом Шора, атаки алгоритмом Гровера и компрометация долгосрочных данных [2, 3].

Также на сегодняшний момент самым актуальным является компрометации данных, так называемая проблема «Harvest now decrypt later», что подразумевает под собой получение и накопление зашифрованных данных, для того чтобы в будущем при появлении более подходящих мощностей, таких как достаточно мощный квантовый компьютер, расшифровать и получить секретную информацию.

2. ЦЕЛЬ ИССЛЕДОВАНИЯ

Основная цель исследования заключается в рассмотрении вопросов жизнеспособности классических алгоритмов шифрования в условиях квантовых вычислений и выработке конкретных практических решений по обеспечению безопасности.

3. ПОСТАВЛЕННЫЕ ЗАДАЧИ

Основной задачей исследования является анализ ситуации, в которой на классические криптографические алгоритмы будет производиться атака с помощью квантового компьютера, выявление границ устойчивости ко взломам классических алгоритмов шифрования, а также предложение возможных стратегий защиты, включая оценку постквантовых подходов и рекомендации по их внедрению.

4. МЕТОД ИССЛЕДОВАНИЯ

Метод исследования основан на моделировании атаки. В рамках исследования была разработана программа для моделирования квантовых атак с использованием фреймворка Qiskit от IBM. Для анализа симметричных алгоритмов применялась эмуляция атаки алгоритмом Гровера на ключи AES-128 и AES-256. Для асимметричных алгоритмов — имитация атаки алгоритмом Шора на RSA-1024 и RSA-2048.

5. СИММЕТРИЧНЫЕ АЛГОРИТМЫ ШИФРОВАНИЯ

Симметричные алгоритмы шифрования, такие как DES и AES, используют один и тот же ключ для шифрования и расшифровывания данных. Хотя они эффективны и быстры, их основной недостаток заключается в необходимости безопасной передачи этого общего ключа между отправителем и получателем. Если ключ будет перехвачен злоумышленником, вся система безопасности окажется под угрозой. Атака алгоритмом Гровера, производимая квантовым вычислителем, уменьшает время подбора ключей в два раза, что ослабляет симметричные шифры, такие как AES. Хотя увеличение длины ключа может частично компенсировать эту уязвимость, в долгосрочной перспективе этого недостаточно [3].

Алгоритм Гровера — это квантовый алгоритм для решения задачи перебора, то есть нахождения решения уравнения вида $f(x) = y$, где f — булева функция от n переменных. Алгоритм Гровера основан на физическом эффекте «усиления амплитуды» целевого состояния и достигает квадратичного уменьшения оценки трудоемкости задачи поиска решения, то есть вместо $O(N)$ операций, требующихся для полного перебора в классическом случае, квантовый компьютер способен решить эту задачу за $O(N^{1/2})$ операций [3].

Алгоритм Гровера может быть эффективно применен к задачам криптоанализа. Так, для блочных шифров (AES, Кузнечик и других), квадратичное ускорение взлома методом перебора требует увеличения размера ключа в 2 раза для сохранения того же уровня стойкости.

Моделирование атаки на AES-128 с помощью квантового симулятора (Qiskit) показало, что при идеальных условиях количество шагов для нахождения ключа сокращается с 2^{128} до 2^{64}, что теоретически делает возможным успешную атаку на обычном квантовом процессоре мощностью около 4000 кубит. Но нельзя забывать, что данная атака будет возможна, а точнее эффективна только при мощности квантового компьютера в более чем 4000 кубитов, а на сегодняшний момент (2025 год) существует только компьютер с 105 кубитами. Этого, как мы можем понять, недостаточно, и данная атака хоть является очень опасной в будущем, так как использование симметричного алгоритма используется во многих областях таких как:

1. **Сетевые коммуникации**
   Симметричное шифрование используется для создания защищённого туннеля между клиентом и сервером. После первичной аутентификации (часто с помощью асимметричных методов) устанавливается сеансовый ключ, с помощью которого все данные шифруются, как правило, с использованием AES.
2. **Протоколы TLS/SSL**
   При установлении защищённого соединения между клиентом и сервером (например, при доступе к сайту через HTTPS) используется асимметричное шифрование для обмена симметричным сеансовым ключом. После этого вся передача данных осуществляется при помощи симметричного алгоритма (например, AES), что обеспечивает и безопасность, и производительность.
3. **Защищённые мессенджеры и мобильные приложения**
   Современные мессенджеры, такие как WhatsApp, Telegram используют симметричное шифрование в сочетании с протоколами обмена ключами. После установления защищённого сеанса сообщения между пользователями шифруются симметричным ключом — это даёт высокую скорость и защищённость.
4. **Облачное хранение и резервное копирование**
   Сервисы вроде Google Drive, Dropbox применяют симметричное шифрование для защиты пользовательских данных на серверах. Резервные копии, как локальные, так и удалённые, часто шифруются алгоритмами AES или Triple DES (3DES) для обеспечения конфиденциальности и целостности данных.
5. **Банковская сфера и финансы**
   Банковские терминалы, банкоматы, платёжные шлюзы и карты используют симметричное шифрование для защиты транзакционных данных. Протоколы вроде ISO 8583 опираются на 3DES и AES для шифрования PIN-кодов, токенов и другой конфиденциальной информации. В системах токенизации платёжных данных (например, при оплате через Google Pay или MirPay) также используется симметричное шифрование для защиты сессионных ключей и идентификаторов транзакций.
6. **Встраиваемые системы и IoT-устройства**
   Устройства с ограниченными ресурсами, такие как датчики, медицинские приборы, камеры видеонаблюдения, используют лёгкие симметричные алгоритмы (например, AES-128, Speck, Simon, PRESENT), позволяющие шифровать данные без существенного увеличения энергопотребления или задержек.

Но данные алгоритмы уже модернизируются для постквантового мира с использованием новых алгоритмов таких как решётчатые, гибридные и т.д.

6. АСИММЕТРИЧНЫЕ АЛГОРИТМЫ ШИФРОВАНИЯ

Большинство современных информационных систем использует асимметричный алгоритм шифрования RSA, работающий на основе открытого ключа. Его криптостойкость основывается на сложности разложения на множители больших чисел, что позволило создать систему, в которой public key (публичный ключ) используется для шифрования, а private key (приватный ключ) — для расшифровки. Эта идея позволила обойти проблему передачи секретных ключей и стала революцией в цифровой безопасности.

Наиболее криптостойкие системы в настоящее время используют 1024-битовые и большие числа, но увеличение размерности ключа не может быть бесконечным, поскольку это увеличивает время шифрования и замедляет процесс передачи данных.

Алгоритм Шора — это квантовый алгоритм, который выполняет факторизацию больших чисел за полиномиальное время, а не за экспоненциальное, как обычные методы [5]. Это своего рода криптографический «взломщик». RSA опирается на сложность этой задачи для обеспечения своей безопасности, а потому, если квантовые компьютеры достигнут достаточной мощности, они смогут легко найти приватный ключ по публичному, что сделает весь RSA уязвимым.

С использованием библиотеки Q# было смоделировано применение алгоритма Шора к числу RSA-1024. При этом, несмотря на ограниченность современных квантовых систем, установлено, что для реального взлома потребуется квантовый компьютер с 4000–5000 кубитами и эффективной коррекцией ошибок. IBM и Google прогнозируют возможность появления таких систем в течение 10–15 лет.

Например, при использовании RSA с 2048-битным ключом, квантовый компьютер, способный выполнять 4096 идеальных логических кубитов, сможет взломать систему за считанные часы, что подтверждено моделированием в работах NIST [8].

С данным типом алгоритмов та же ситуация, что и симметричными, алгоритм Шора сможет раскусить данные алгоритмы за считанные часы, но только при использовании компьютера с более чем 5000 кубитов, а как нам известно таких мощностей ныне нет. Но асимметричные алгоритмы используются во многих вещах таких как:

1. **Обеспечение конфиденциальности при передаче данных**
   Наиболее очевидное применение — шифрование сообщений. Например, если пользователь Ваня хочет отправить зашифрованное сообщение пользователю Маша, он использует открытый ключ Маши. Только Маша, обладая соответствующим закрытым ключом, может расшифровать сообщение. К примеру, всем известный протокол HTTPS, обеспечивающий безопасную передачу данных по интернету, использует асимметричное шифрование для установления безопасного канала, по которому далее передаются симметричные ключи.
2. **Цифровая подпись**
   Асимметричные алгоритмы позволяют создавать цифровые подписи, которые подтверждают подлинность отправителя и целостность данных. Рассмотрим ситуацию когда пользователь Андрей подписывает документ своим закрытым ключом, любой другой пользователь может проверить подлинность этой подписи с помощью открытого ключа Андрея.
3. **Аутентификация и контроль доступа**
   Многие системы используют асимметричную криптографию для аутентификации пользователей. Примеры включают SSH-доступ к серверам, VPN-аутентификацию, смарт-карты и системы двухфакторной аутентификации.
4. **Криптовалюты и блокчейн**
   В технологии блокчейн асимметричная криптография используется для создания адресов кошельков (открытые ключи) и подписания транзакций (закрытые ключи). Естественно они используются в 2 самых популярных криптовалютах таких как Bitcoin и Ethereum используются алгоритмы ECDSA (эллиптические кривые) для создания и проверки транзакций.
5. **Защита программного обеспечения**
   Разработчики используют цифровые подписи для подтверждения подлинности и целостности программного обеспечения. Это предотвращает запуск вредоносного или изменённого кода.

7. КОМПРОМЕТАЦИЯ ДОЛГОСРОЧНЫХ ДАННЫХ

Компрометация данных – это ситуация, при которой конфиденциальная информация становится общедоступной в результате утечки, перехвата или неправомерного доступа. В совре-

менном цифровом мире это может касаться как персональных данных (например, пароль от вашей карты или паспортных данных), так и корпоративной, банковской или правительственной информации. Компрометация особенно опасна, когда речь идёт о долгосрочных данных. Это означает, что даже если в момент передачи данные зашифрованы с использованием современных алгоритмов, их копирование и последующее сохранение злоумышленниками может привести к потенциальному раскрытию информации в будущем, когда во всемирной сети будет работать множество квантовых компьютеров, значительно превосходящих по быстродействию компьютеры стандартной архитектуры фон Неймана. Таким образом, даже если в данный момент данные защищены, их долгосрочное хранение без регулярного обновления защитных механизмов может обернуться серьезными проблемами [7]. Согласно отчёту ENISA (2023), срок хранения некоторых данных (в здравоохранении, военном деле и правительственных структурах) превышает 25 лет. Это значит, что информация, зашифрованная сегодня, может быть взломана, когда квантовые компьютеры станут доступными.

Также для того чтобы защитить данные от того чтобы их скопировали и получили к ним доступ с появлением достаточных мощностей разрабатываются индикаторы компрометации данных.

Индикатор компрометации (IOC) является свидетельством того, что кто-то мог создать брешь в сети организации или конечной точке. Эти данные экспертизы не просто указывают на потенциальную угрозу. Они сигнализируют, что уже произошла атака, например, проникновение вредоносных программ, компрометация учетных сведений или кража данных. Специалисты по безопасности ищут индикаторы компрометации в журналах событий, решениях Extended Detection and Response (XDR), а также решениях управления информационной безопасностью и событиями безопасности Security Information and Event Management (SIEM). Во время атаки команда использует IOC для устранения угрозы и снижения ущерба. После восстановления индикаторы компрометации помогают организации лучше понять, что произошло. Это позволяет команде по обеспечению безопасности организации усилить защиту и снизить риск похожего инцидента.

Хочется выделить основные идентификаторы компрометации которые являются звоночком, что на систему совершается, совершилось или были попытки совершить атаку, вот одни из основных идентификаторов:

1. **Аномалии трафика**
   В большинстве организаций существует определённый «профиль» нормального сетевого трафика. Этот профиль отражает ожидаемое поведение пользователей, приложений и сервисов. Например, можно ожидать, что сотрудники передают определённое количество данных в рабочее время. В свою очередь индикатором компрометации может служить резкое увеличение объёма исходящего трафика ночью или подключение к внешним IP-адресам, не входящим в доверенную группу.
   Такие события могут указывать на утечку данных или наличие вредоносного ПО, осуществляющего передачу информации на управляющий сервер.
2. **Необычные попытки входа**
   Рабочие привычки пользователей, как правило, предсказуемы. Они входят в систему из конкретных географических точек, в определённые часы и с одних и тех же устройств, но если начнутся подозрительные действия:
   - Попытка входа в систему ночью, если пользователь обычно работает днём.
   - Вход с IP-адреса, принадлежащего другой стране.
   - Множественные неудачные попытки входа для одной учётной записи, указывающие на возможную атаку перебором паролей (brute force).

То специалист по безопасности сможет принять меры по решению проблемы и защиту данных от атаки.

3. **Аномалии привилегированной учетной записи**
   Учётные записи с повышенными правами (например, администраторские) являются мишенями для злоумышленников, поскольку они дают доступ к конфиденциальным данным и критическим системам. В данном случае показать, что права администраторы находятся под угрозой может послужить данные признаки:
   – Попытки изменения уровня доступа.
   – Входы от имени администратора с необычных устройств.
   – Действия, не соответствующие обычным обязанностям пользователя, например, массовое удаление данных.

   Для защиты привилегированных учётных записей организации внедряют системы PAM (Privileged Access Management), многофакторную аутентификацию и журналы контроля действий.
4. **Изменение конфигураций систем**
   Изменения в системных конфигурациях могут быть признаком действия вредоносного кода, особенно если:
   – были отключены службы безопасности или антивирус;
   – открыт удалённый доступ;
   – изменены настройки межсетевого экрана.

   Такие действия часто совершаются в рамках атаки на ранних этапах для подготовки инфраструктуры злоумышленника.
5. **Неожиданная установка или обновление программного обеспечения**
   Резкое появление нового ПО без одобрения со стороны ИТ-службы может свидетельствовать о попытке компрометации. Данного рода ПО, может появится как от не внимательности и халатности сотрудника, так и от фишинговых атак. Примерами работы вредоносного ПО может быть:
   – Появление новых исполняемых файлов.
   – Изменения в автозагрузке.
   – Установленные службы, имитирующие системные.
6. **Многочисленные запросы для одного файла**
   Если к одному и тому же файлу осуществляется много обращений за короткий промежуток времени, это может быть попыткой обойти ограничения доступа или подготовкой к краже данных.

Для выявления индикаторов компрометации признаки цифровой атаки записываются в файлы журналов. В рамках кибербезопасности с использованием индикаторов компрометации команды регулярно отслеживают цифровые системы на предмет подозрительной активности. Современные решения SIEM и XDR упрощают этот процесс с помощью алгоритмов ИИ и машинного обучения, которые устанавливают базовые показатели нормальной работы в организации, а затем оповещают команду об аномалиях. Кроме того, важно информировать сотрудников, не связанных с системой безопасности, которые могут получить подозрительные сообщения электронной почты или случайно скачать зараженный файл. Хорошие программы обучения безопасности помогают сотрудникам лучше обнаруживать скомпрометированную электронную почту и предоставлять им способы уведомления об аномалиях.

Для демонстрации того, то как будет обучаться нейронная сеть на основе данных полученных из логов windows security, была разработана программа в которой нейронная сеть обучается на основе csv файла полученного из отчёта по безопасности, и далее будет выведена информация по полученной информации.

1. **Исходные данные**
   Данная программа определяет логи по классификациям угроз. У нас имеется CSV таблица с логами, которые содержат данные поля (Рисунок 1).
   – Ключевые слова
   – Дата и время
   – Источник
   – Event ID
   – Категория задачи
   – Описание/доп. информация

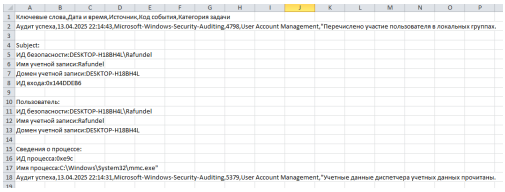

Рис. 1. Часть логов

Далее мы должны преобразовать данные, а именно:
– Удаление строк с пропущенными значениями
– Обработка CSV/текста: учёт ошибок разделения по запятым, слияние столбцов
– Кодирование значений EventID в классы 1, 2 и 3 по степени опасности
Часть кода с кодированием значений по классам, а также поиск их (Рисунок 2).

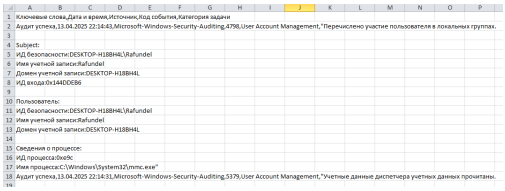

Рис. 2. Часть кода для меток

Нужно построить нейронную сеть для анализа и прогнозировании на основе логов сети или частного ПК, для предубеждений и прогнозировании атаки на устройства или сеть.

2. **Инструменты**
   Для написания работы я выбрал следующие инструменты: Среда разработки:
   – JupyterLab – интегрируемая среда разработка с открытым исходным кодом.
   Язык программирования и библиотеки:
   – Python – удобный язык программирования отлично подходящий для анализа больших данных,
   – Pandas – аналитический инструмент для анализа больших данных,
   – Keras – высокоуровневая библиотека для постороения и обучения нейронных сетей.
   Для постороения и обучения нейронной сети мною был выбран Keras из за его достоинств таких как:
   Простота и удобство использования: Keras предоставляет интуитивно понятный API для быстрого прототипирования нейронных сетей. Это позволяет разработчикам и исследователям легко и быстро экспериментировать с разными архитектурами моделей.

Модульность: Keras организован в виде отдельных модулей (слои, функции активации, потери, оптимизаторы и т.д.), которые можно комбинировать для создания сложных моделей. Это делает код более организованным и удобным для сопровождения.
Широкое сообщество и документация: Благодаря обширному сообществу разработчиков и качественной документации, Keras стал популярным инструментом в академической и промышленной среде. Это облегчает поиск примеров, шаблонов и поддержку при разработке моделей.
Применение: С помощью Keras можно строить как простые модели, так и сложные архитектуры глубокого обучения для задач классификации, регрессии, обработки изображений, текста и многих других.

7.1. Построение нейронной сети

Распределяем данные в соотношении 80% на обучении и 20% тест. Далее создаём слои:

Первый слой:

- Полносвязный (Dense) слой с 64 нейронами и функцией активации ReLU.
- Параметр `input_dim` указывает число признаков во входном векторе.
- Слой Dropout с вероятностью 0.3, который случайным образом обнуляет часть нейронов во время обучения, чтобы предотвратить переобучение.

Второй слой:

- Полносвязный слой с 32 нейронами, также с активацией ReLU.
- Снова применяется Dropout.

Третий слой:

- Дополнительный слой с 16 нейронами, если требуется более глубокая сеть.

Выходной слой:

- Содержит 3 нейрона (соответствующих трём классам угроз).
- Функция активации softmax преобразует выходные значения в вероятности для каждого класса.

Модель компилируется с оптимизатором `adam` и функцией потерь `sparse_categorical_crossentropy`, которая подходит для задач многоклассовой классификации с целочисленными метками.

7.2. Анализ полученных данных

После всех метаморфозов, обучения сети и классификации данных, наша система их распределяет и выводит для удобного анализа специалистом. Наша программа сохраняет отдельными файлами полученные данные, а именно:

- График обучения модели
- Уровень точности по каждому из уровней
- Уровень точности всех модели
- Матрица ошибок
- Сравнение с предыдущим обучением, то как нейронная сеть улучшилась или изменилась

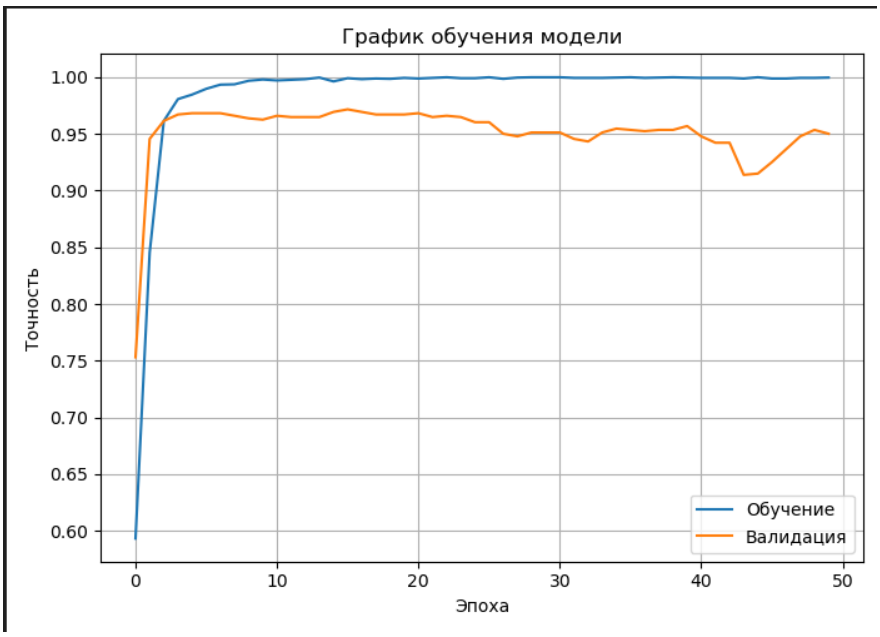

Рис. 3. График обучения

На данном графике мы можем наблюдать график успешных угадок нейронной сети (Рисунок 3).

На ниже представленном скриншоте, мы видим точность на тестовой выборке, а далее видим точность (precision), полноту (recall), f1-меру и количество объектов по классам (Рисунок 4).

Точность на тестовой выборке: 0.9466

	precision	recall	f1-score	support
0	1.00	0.95	0.98	532
1	0.16	0.85	0.27	13
2	1.00	0.94	0.97	559
accuracy			0.95	1104
macro avg	0.72	0.91	0.74	1104
weighted avg	0.99	0.95	0.96	1104

Рис. 4. Таблица точности

Матрица ошибок по классам, по строкам мы можем наблюдать, на примере класса 0, 507 он угадал точно, 25 он перепутал с 1 и 0 он перепутал с 2 (Рисунок 5).

Ниже представлено сравнение с предыдущей моделью, и как мы видим новая итерация не отличается в лучшую сторону в сравнении с прошлой моделью (Рисунок 6).

С учётом угроз, создаваемых квантовыми вычислениями, актуальной задачей является переход от классических криптографических решений к алгоритмам, устойчивым к квантовым атакам. В рамках инициативы NIST по стандартизации постквантовой криптографии было выделено несколько направлений и конкретных алгоритмов, показавших наилучшее соотношение между безопасностью, скоростью и возможностью реализации в реальных системах.

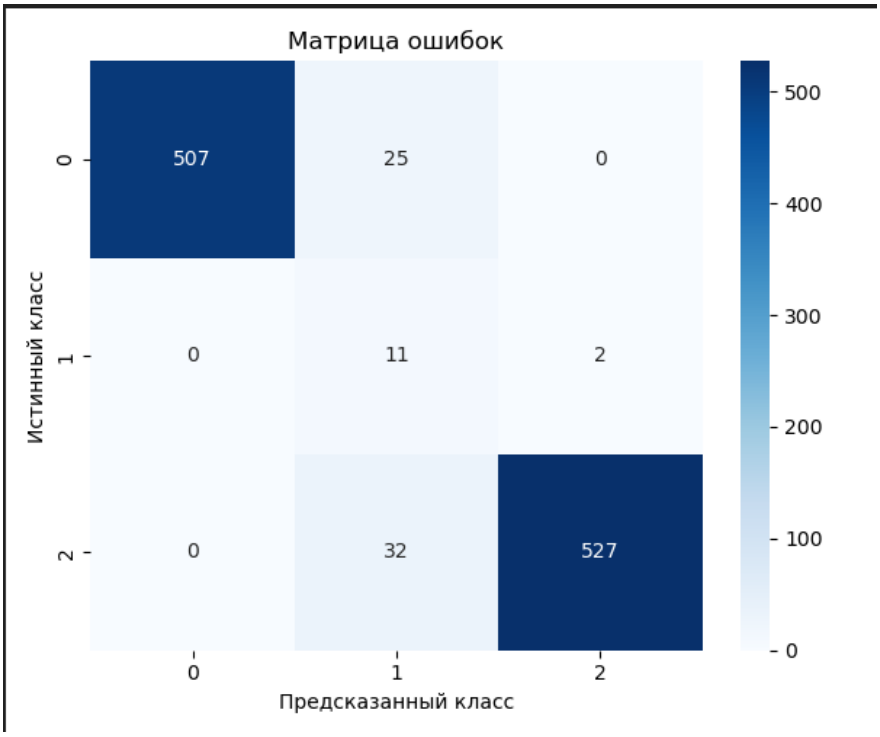

Рис. 5. Матрица ошибок

📊 Сравнение с предыдущей моделью:
точность_на_тесте: 0.4819 ↓ (-0.4647)
потери_на_тесте: 1.1260 ↓ (0.4641)
точность: 0.5317 ↓ (-0.4565)
полнота: 0.4819 ↓ (-0.4647)
f1_мера: 0.4669 ↓ (-0.4971)

Рис. 6. Сравнение с предыдущей

Также идёт развитие и реализация квантово-устойчивых алгоритмов основанных на следующих алгоритмах [8]:

Алгоритмы на решётках (Lattice-based)

Этот класс считается наиболее перспективным с точки зрения практического применения.

- **Kyber** — финалист стандартизации NIST и основной кандидат на внедрение в TLS-протоколах. Он демонстрирует отличное соотношение между скоростью, компактностью и устойчивостью к атакам.
- **NTRU** — один из старейших и проверенных временем алгоритмов. Обеспечивает высокую скорость шифрования и расшифрования, подходит для встраиваемых систем.

Кодовые алгоритмы (Code-based)

- **McEliece** — предлагает очень высокую криптостойкость, устойчив даже к квантовым атакам, однако обладает значительным недостатком — размер публичного ключа может превышать 700 КБ, что затрудняет его использование в мобильных и ограниченных по ресурсам устройствах.

Многочленные алгоритмы (Multivariate polynomial)

- **GeMSS**, **Rainbow** — основаны на сложности решения систем многочленов от многих переменных. Ранее рассматривались как перспективные решения, однако, например, Rainbow был исключён из процесса стандартизации после успешных криптоанализов, что ставит под сомнение их практическую применимость на текущем этапе.

Алгоритмы на основе хэш-функций (Hash-based)

- **SPHINCS+** — один из немногих алгоритмов, подходящих для создания цифровых подписей в постквантовой эпохе. Отличается высокой надёжностью, однако является относительно медленным и требует значительного объёма вычислений при создании и проверке подписей.

7.3. СТРАТЕГИИ ПЕРЕХОДА К ПОСТКВАНТОВОЙ КРИПТОГРАФИИ

Для успешного перехода к устойчивым алгоритмам следует не просто заменить классические схемы на новые, но использовать комплексный и поэтапный подход [12, 13, 14, 15, 16].

Использование гибридных криптографических схем

Для минимизации рисков отказа от устоявшихся решений рекомендуется внедрять *гибридные протоколы*, совмещающие классические и постквантовые алгоритмы. Например, связки `Kyber+RSA` или `Kyber+ECDH` уже применяются в тестовых реализациях протоколов TLS 1.3 и в инфраструктуре VPN. Такие подходы позволяют сохранить обратную совместимость и обеспечить «плавный переход».

Интеграция специализированных библиотек

Для внедрения в существующие программные решения можно использовать открытые библиотеки:

– **liboqs (Open Quantum Safe)** — предоставляет реализацию постквантовых алгоритмов и может быть интегрирована с OpenSSL (начиная с версии 3.0).
– **PQClean** — библиотека с реализациями на чистом языке C, поддерживает большинство алгоритмов, финалистов и кандидатов NIST.
– **BoringSSL (Google)** — модифицированный форк OpenSSL, уже включает поддержку Kyber в рамках экспериментальных сборок.

Актуализация нормативно-правовой базы

На государственном уровне необходимо пересмотреть и дополнить существующие стандарты (например, **ГОСТ Р 34.10**, **ГОСТ Р 34.11**, **ГОСТ 28147-89**) с учётом требований к устойчивости криптографических систем в условиях появления квантовых вычислителей. Это позволит обеспечить как техническую, так и юридическую основу для внедрения постквантовой криптографии в критически важных сферах [4].

8. РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

Результатом проведенных исследований является разработка приложения, показывающая потенциальную уязвимость современных классических алгоритмов шифрования перед мощными квантовыми компьютерами. Были предоставлены варианты развития технологий и интеграции их друг с другом для повышения безопасности, как будущих данных, так и современных. Также была разработана нейросетевая система оценки и классификации инцидентов безопасности на основе логов Windows. Система оценивает потенциальную опасность каждого события и квалифицирует его в один из 3 классов с вероятностью в 90+%, оставшиеся проценты - это потенциально ещё неклассифицированные ошибки и угрозы, обеспечивая автоматизацию анализа и выявления угроз. Это является шагом к построению системы автоматической защиты компьютерной сети и/или персонального компьютера от атак.

Путём создания данной программы, также было, показано удобство анализа и предсказания потенциальной атаки на сеть/компьютер с помощью нейронных технологий.

9. ЗАКЛЮЧЕНИЕ

Хотя квантовые компьютеры угрожают многим существующим криптографическим системам, все время совершенствуются алгоритмы, устойчивые к квантовым атакам. Эти алгоритмы разрабатываются в рамках постквантовой криптографии и основаны на математических задачах, которые не поддаются эффективному решению даже квантовыми компьютерами. Также разрабатываются и уже внедряются решения для превентивного предупреждения атак на данные для их сбора, создаются идентификаторы с использованием искусственного интеллекта и машинного обучения для защиты информационных коммуникаций и передаваемых по ним данных.

СПИСОК ЛИТЕРАТУРЫ

1. Душкин Р. В. Обзор текущего состояния квантовых технологий. *Компьютерные исследования и моделирование*, 2018, том 10, № 2, стр. 165–179.

2. Постквантовая криптография. [Электронный ресурс]. — Режим доступа: `https://infars.ru/blog/post-quantum-cryptography-kak-kvantovye-kompyutery-ugrozhayut-bezopasnosti-dannykh/` (дата обращения: 03.09.2025).

3. Бернхард К. *Квантовые вычисления для настоящих айтишников.* — СПб.: Питер, 2019. — 240 с.

4. Рекомендации по стандартизации использование алгоритмов ГОСТ 28147-89, ГОСТ Р 34.11 и ГОСТ Р 34.10 в криптографических сообщениях формата CMS / ФСТЭК России. — М., 2014. — 30 с.

5. Shor P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM J. Comput.*, 1997, vol. 26, no. 5, pp. 1484–1509.

6. Hidary J.D. *Quantum Computing: An Applied Approach.* — Springer International Publishing, 2019. — 104–107 pp.

7. What is Harvest Now, Decrypt Later (HNDL). [Электронный ресурс]. — URL: `https://www.ssltrust.com.au/blog/what-is-harvest-now-decrypt-later-hndl` (дата обращения: 10.04.2025).

8. Alagic G. et al. Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process. — NISTIR 8309, 2020.

9. Griffiths D.J., Schroeter D.F. *Introduction to Quantum Mechanics.* — 3rd edition. — Cambridge University Press, 2018.

10. Nielsen M.A., Chuang I.L. *Quantum Computation and Quantum Information.* — 10th anniversary edition. — Cambridge University Press, 2010.

11. Shankar R. *Principles of Quantum Mechanics.* — 2nd edition. — Plenum Press, 1994.

12. Ковалев Д.А. Квантовые компьютеры. Что это такое и зачем они нужны? *Международный научный журнал «Символ науки»*, 2021, № 1.

13. Долгочуб Е. А., Поликанин А. Н. Технологии квантовой криптографии. [Электронный ресурс]. — DOI: 10.33764/2618-981X-2021-6-78-83. — URL: `https://cyberleninka.ru/article/n/tehnologii-kvantovoy-kriptografii` (дата обращения: 10.09.2025).

14. Долгочуб Е. А., Поликанин А. Н. Анализ квантовых алгоритмов шифрования BB84 и B92. [Электронный ресурс]. — DOI: 10.33764/2618-981X-2020-6-1-125-130. — URL: `https://cyberleninka.ru/article/n/analiz-kvantovyh-algoritmov-shifrovaniya-bb84-i-b92` (дата обращения: 10.09.2025).

15. Акыев Г.А. Обзор новых методов защиты информации, таких как квантовые криптографические системы и оптические методы обнаружения взлома. *Международный научный журнал «Вестник науки»*, 2025, № 1 (82), том 4, стр. 805–809.

16. Абрамова Е.А., Адамов Е.В., Аксенов В.П., Богач Е.А., Дудоров В.В., Колосов В.В., Левицкий М.Е., Погуца Ч.Е., Павлов И.И. Формирование криптографического ключа в сопряженных приемопередающих атмосферных лазерных системах. [Электронный ресурс]. — DOI: 10.36724/2072-8735-2023-17-2-33-41. — URL: `https://cyberleninka.ru/article/n/formirovanie-kriptograficheskogo-klyuchav-sopryazhennyh-priemo-peredayuschih-atmosfernyh-lazernyh-sistemah` (дата обращения: 10.09.2025).

Research on Security of Quantum Computing by Classical Encryption Algorithms

R. R. Abdullin, D. A. Egorov, N. V. Krupenina, V. Yu. Rud, Yu. D. Sapozhnikova

The article investigates potential threats to classical cryptography algorithms from quantum computers and their ever-growing capabilities. Existing methods of cryptographic algorithms and their resistance to quantum hacking are considered. Modification of these algorithms is currently capable of protecting information from quantum computer attacks, but in the long term, the development of new methods of post-quantum cryptography is necessary. The development and improvement of data compromise identifiers becomes particularly important to prevent data copying for subsequent hacking. To solve this problem, an intelligent computer network protection system based on the analysis of compromise indicators taken from the computer network security log is proposed. The system is based on classification algorithms and allows dividing all suspicious actions in the network into danger classes (very dangerous, needs attention, not worth attention).

KEYWORDS: quantum computing, post-quantum cryptography, cybersecurity, encryption algorithms, data compromise.