Информационные процессы, Том 25, № 3.1, 2025, стр. 573–585.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Квантовое распознавание инцидентов среди событий информационной безопасности

Д. А. Городиский*, С. В. Зуев**

**Белгородский государственный технологический университет им. В. Г. Шухова, Белгород, Россия*
***Крымский федеральный университет им. В. И. Вернадского, Симферополь, Россия*
Поступила в редколлегию 15.10.2025 г. Принята 25.11.2025 г.

Аннотация—В качестве модели машинного обучения используется квантовая нейронная сеть прямого распространения. Подготовка данных делается общепринятыми методами, но вместо нормализации используется приведение данных к целочисленным векторам, чтобы далее привести размерность данных к подходящим для квантовой нейронной сети значениям. Данные для анализа представляют собой обезличенные данные одного из центров обеспечения информационной безопасности, собранные в течение года. Средствами для исследования выбраны язык программирования Python и библиотеки с открытым кодом. В работе реализуется метод статистического машинного обучения, который позволяет производить обучение в реальном времени. В результате исследования построена интеллектуальная система, которая на основании значений признаков событий безопасности строит предположение о принадлежности события к классу инцидентов. Тем самым, система позволяет распознать событие, которое с повышенной вероятностью приведет к ущербу, и по которому оправдано незамедлительное реагирование. Работа системы верифицирована на реальных данных, которые характеризуются той же несбалансированностью, что и обучающие выборки событий информационной безопасности, то есть имеет очень низкую долю инцидентов (менее одного процента). Было установлено, что квантовая модель с тремя кубитами достигла полноты (recall) 100% при точности (precision) 5.5%, что на 37% выше, чем у классической нейросети. Эффективность квантовой интеллектуальной системы заключается в том, что она может обучаться онлайн и позволяет производить до-обучение, всегда стремясь к улучшению качества классификации. Системы такой архитектуры можно применять и в других случаях, где несбалансированность данных затрудняет использование классического машинного обучения и известные алгоритмы оверсемплинга не помогают справиться с задачей.

КЛЮЧЕВЫЕ СЛОВА: квантовое машинное обучение, квантовая нейронная сеть, инцидент информационной безопасности, несбалансированные обучающие выборки, несбалансированные данные.

DOI: 10.53921/18195822_2025_25_3.1_573

1. ВВЕДЕНИЕ

По мере того, как общество мигрирует в цифровой мир, угроза киберпреступности становится все более ощутимой. Человечество все больше полагается на технологии для управления всеми аспектами жизни — от коммунальных услуг до бизнес-процессов и даже покупок продуктов. Применение цифровых технологий для реализации товаров и услуг, оказания государственных услуг, образования граждан позволяет всему миру приобрести так называемые цифровые дивиденды. Однако любые информационные и технические новшества значительно расширяют сферу киберпреступности и создают условия для повышения эффективности криминальных действий. Всеобщее использование облачных технологий и хранилищ данных

привело к распространению киберпреступности как в финансовой среде, так и в производственной и торговой сферах.

Согласно данным одного из ведущих исследовательских центров мировой киберэкономики Cybersecurity Ventures, глобальные расходы на киберпреступность будут расти на 15 процентов в год, достигнув 10,5 трлн долларов США в год к 2025 году, в сравнении с 3 трлн долларов США в 2015 году [1]. Но потери не ограничиваются только экономическими — ключевая инфраструктура общества, доверие к цифровым трансформациям и общее доверие к технологиям также под угрозой. Усугубляют риски низкие входные барьеры для субъектов киберугроз, более циничные методы атак, нехватка профессионалов в области кибербезопасности.

По данным Всемирного обзора экономических преступлений от PricewaterhouseCoopers (PWC) за 2022 год, киберпреступность представляет наибольшую угрозу для организаций любого размера, за которой следуют мошенничество с клиентами и незаконное присвоение активов [2]. При этом наибольшую долю среди экономических преступлений киберпреступность занимает в секторе информационных технологий и телекоммуникациий (50%) и отрасли здравоохранения (40%), что обусловлено ценностью медицинских данных, сравнительной легкостью проникновения и недостаточной грамотностью сотрудников в области кибербезопасности.

Компания IBM Security изучила 550 организаций, пострадавших от утечек данных, произошедших в период с марта 2021 по март 2022 года. 83% из них имели более одной утечки данных, и 60% нарушений, допущенных организациями, привели к повышению цен, что легло на плечи клиентов. Утечки данных произошли в 17 странах и регионах и в 17 различных отраслях промышленности [3]. Был выявлен наиболее распространенный вектор атаки: кража учетных данных (19%), фишинг (16%), неправильно настроенное облако (15%), и уязвимости в стороннем программном обеспечении (13%). Однако этот отчет охватывает только обнаруженные и зарегистрированные инциденты, а количество незарегистрированных инцидентов, вероятно, намного выше.

Общая годовая стоимость кибератак любого типа также растет устойчивыми темпами [4]. Самая высокая средняя стоимость утечки данных наблюдается в отрасли здравоохранения. С 2021 по 2022 г. она выросла на 9,4%. Финансовые организации являются вторыми по величине расходов, за ними следуют фармацевтическая, технологическая и энергетическая отрасли. Самой распространенной атакой, связанной с утечками данных, в 2022 году была кража учетных данных [5]. Деструктивное вредоносное программное обеспечение связано с 17% атак. Еще 19% утечек были вызваны атаками на цепочки поставок. Человеческие ошибки, то есть нарушения, происшедшие непреднамеренно из-за ошибок и небрежностей сотрудников дают еще 21%.

С каждым годом сфера кибербезопасности становится всё более сложной и динамичной. За последние два десятилетия появилась классификация кибератак на типы: отказ в обслуживании (DOS), распределенный отказ в обслуживании (DDOS), SQL-инъекцию (SQLi), фишинг, криптоджекинг, межсайтовой скриптинг (XSS), кибервандализм, шпионаж, атаки перехвата веб-сессии и т.д. [6]-[8]. Отдельно следует назвать программы-вымогатели [9] и социальный инжиниринг. По данным [10], в 2020 году злоумышленники получили 412 миллионов долларов США в виде выплат. Для защиты от таких угроз по всему миру развернуты различные системы безопасности, такие как межсетевые экраны, IDS, IPS и другие системы. Для повышения производительности этих систем безопасности сейчас все чаще рассматривается использование методов машинного обучения [11]. Но до сих пор множество атак остаются незамеченными ни одним устройством защиты информации.

Центры управления безопасностью (SOC) играют ключевую роль в обеспечении безопасности организаций. Они предназначены для того, чтобы потенциальные инциденты безопасности (*события*) были правильно идентифицированы, проанализированы, коммуницированы, обработаны защитой, а в случае ущерба - расследованы [12]. Обычно SOC непрерывно мони-

торит сетевую активность и анализирует потоки данных, происходящие в информационной среде организации. Это включает в себя сбор информации из различных источников, таких как системы журналирования, сетевые устройства, система управления доступом и другие. С момента создания Центров управления безопасностью (SOC) около 19 лет назад их значение значительно выросло, особенно за последние пять лет. В основном это связано с острой необходимостью предотвращения крупных киберинцидентов и, как следствие, с внедрением централизованных операций по обеспечению безопасности на предприятиях.

В SOC полученная информация подвергается анализу с использование специализированных алгоритмов и методов обнаружения угроз. При обнаружении потенциальной угрозы или инцидента, SOC принимает меры для нейтрализации угрозы и минимизации ущерба для организации. Этот процесс включает в себя блокировку атаки, изоляцию скомпрометированных систем, а также восстановление после инцидента. Однако, с увеличением объема информации, поступающей в SOC, существует проблема эффективной классификации данных, то есть распознавания потенциально опасных инцидентов среди большого числа обычных событий. Для эффективного функционирования системы SOC необходимо постоянно отслеживать и анализировать новые угрозы, включая различные виды вредоносных программ, социальную инженерию, атаки на приложения и инфраструктуру. Важным аспектом обнаружения угроз является способность не только реагировать на события в реальном времени, но и прогнозировать потенциальные угрозы и принимать меры для их предотвращения заранее. Это может включать в себя анализ текущих трендов, угроз и уязвимостей, использование прогностических алгоритмов для выявления возможных угроз в будущем.

Для эффективного реагирования на угрозы информационной безопасности и предотвращения возможных инцидентов необходимы инновационные подходы и технологии. Одним из таких подходов является применение рекомендательных систем в системах SOC. Использование рекомендательной системы в работе SOC может дать преимущества в виде автоматизации процесса обнаружения угроз, повышения точности выявления аномалий (инцидентов), сокращение времени реагирования на угрозы и улучшение общей эффективности работы SOC. Принцип работы этой рекомендательной системы базируется на анализе данных, полученных из различных источников, таких как журналы аудита, сетевые пакеты и журналы входа в систему. Важным этапом работы системы является предварительная обработка данных. Основной целью рекомендательной системы в SOC является обнаружение аномальной или подозрительной активности, которая может свидетельствовать о наличии угроз безопасности.

Существуют ограничения, с которыми может столкнуться применение рекомендательных систем в SOC. Данные в разных SOC разнообразны и неоднородны по своей природе. Это создает сложности при разработке рекомендательных систем и вызывает необходимость использования методов анализа больших данных и моделей машинного обучения. Стратегии атак постоянно эволюционируют, что требует непрерывной адаптации рекомендательных систем. Это вызывает необходимость использования онлайн обучения моделей — с подкреплением, статистического обучения. Отсюда появляются требования не только к функциям, но и к архитектуре рекомендательной системы, то есть, к используемым моделям и алгоритмам обучения.

На сегодняшний день в России имеется программно-аппаратный комплекс ViPNet TIAS для автоматического выявления инцидентов на основе анализа событий информационной безопасности [13]. Выявление инцидентов в этой системе делается по двум группам сценариев: сигнатурном методе анализа, основанном на использовании метаправил выявления инцидентов, и модели машинного обучения, работающей на основе статистического анализа угроз. ViPNet TIAS в виде графиков и числовых показателей показывает статистическую информацию о событиях, отражая динамику вредоносной активности. Таким образом, благодаря

автоматическим рекомендациям и сбору данных, связанных с событиями, комплекс упрощает реагирование на угрозы информационной безопасности, что сокращает затраты на персонал, сокращает время обнаружение инцидента по сравнению с ручным анализом с 30 до 2 минут [14].

Одно из ведущих средств для анализа данных о событиях информационной безопасности в мире — это решение Splunk Enterprise Security от компании Splunk. Оно предназначено для автоматического выявления инцидентов на основе анализа событий информационной безопасности. Выявление инцидентов основано на алгоритмах анализа данных и обнаружения аномалий, а также интегрированных средствах мониторинга [15]. Система Splunk Enterprise Security обеспечивает автоматизированное реагирование на угрозы информационной безопасности, значительно сокращая время обнаружения инцидентов.

Рассмотрим перспективы применения квантовой нейронной сети в контексте обнаружения угроз информационной безопасности. Квантовые нейронные сети обладают потенциалом для решения сложных задач, включая обнаружение аномалий в информационных системах. Традиционно считается, что они могут обрабатывать информацию более эффективно благодаря возможности параллельной обработки (квантовый параллелизм). В то же время, использование квантовой запутанности непосредственно для поиска взаимосвязей в данных есть еще одно направление, в котором квантовые интеллектуальные системы могут демонстрировать большую эффективность. Квантовые вычисления продемонстрировали своё превосходство в решении проблем, неразрешимых на классических компьютерах [16]: в экспериментах с 40 сверхпроводящими кубитами и 1300 квантовыми вентилями было выявлено существенное квантовое преимущество [17]. Также с преимуществами квантовых вычислений и квантовых компьютеров в решении задач в области искусственного интеллекта можно ознакомиться в обзоре [18], в котором обоснована актуальность работ в этой области. В обзоре 2023 г. [19] имеются ссылки на все современные продвижения в этой области.

Существует множество задач анализа данных, которые можно решать на квантовых компьютерах. Например, классификация [20]-[21], в том числе в приложениях [22]. Для кластеризации разработано несколько методов квантового машинного обучения (см., например, [23]). Квантовая версия алгоритма k-средних представлена в работе [24]. В [25] разработан квантовый аналог метода главных компонент. Имеются результаты в области квантовой оптимизации [26] и в одной из современных работ [27] можно увидеть экспериментальное доказательство превосходства над классическими алгоритмами.

Главным преимуществом квантового машинного обучения считается достижимое экспоненциальное снижение сложности вычислений. Применение квантовых версий позволяет значительно ускорить выполнение алгоритмов обучения и классификации [28]. Представление данных в виде состояния квантовой системы требует умения работать с размерностями данных без потери информации. В работах [29]-[31] предложены прототипы квантовых нейронных сетей на основе квантовых схем с настраиваемыми параметрами. В настоящей работе показана реализация этого подхода с архитектурой квантовой нейронной сети прямого распространения, существенно использующей запутанные квантовые состояния. Прототипы таких сетей исследованы в [31], [32].

Таким образом, перспективы применения квантовых нейронных сетей в контексте безопасности выглядит многообещающим. Однако требуются дальнейшие исследования в области адаптации квантовых алгоритмов к специфике задач обнаружения угроз, а также реализация соответствующих практических решений для интеграции в системы SOC.

2. МАТЕРИАЛЫ И МЕТОДЫ

Цель анализа данных SOC заключается не только в классификации событий на инциденты и не инциденты, но и распознавание контекста, сопровождающего события: выявление особенностей, отличающих атаку от случайных действий. В результате требуется предоставить аналитикам кибербезопасности инструменты для оперативного реагирования на угрозы. Рассмотрим теперь методы, которые позволяют эффективно анализировать SOC-датасет, с учетом динамичности и сложности современной среды угроз.

Находящийся в нашем распоряжении датасет, построенный из данных, полученных Центром управления безопасностью (далее — просто датасет), содержит следующие признаки:

1. 'Id',
2. 'Дата',
3. 'Время',
4. 'Часовой пояс',
5. 'Статус',
6. '**Вердикт**',
7. 'Приоритет инцидента ',
8. '**Приоритет подозрения на инцидент**',
9. 'KUMA-Тип',
10. '**ID корреляции**',
11. '**Категория**',
12. '**Источник**',
13. '**Наименование**',
14. 'Наименование2',
15. '**Technique**',
16. 'Примененные контрмеры',
17. 'Комментарий',
18. 'Рекомендации',
19. 'SLA взятия в работу',
20. 'SLA выполнения',
21. '**SV-Тип**'

Перед тем, как приступить к препроцессингу, необходимо устранить те признаки, которые своим присутствием будут давать некорректный ответ. Данные были проанализированы на пропуски, зависимости, а также значимости для классификации. Использовались библиотеки pandas, seaborn и matplotlib.

Такие признаки, как "Id", "дата", "время", "часовой пояс" исключены, так как не несут никакой значимости для ответа: считаем, что ландшафт угроз в моменты обучения и тестирования одинаков. Те поля, которые появились уже после объявления вердикта, а также те, которые разделены на несколько других полей, тоже были исключены, как не имеющие отношения к классификации – "рекомендации", "комментарий", "SLA взятие в работу" и так далее. В результате остались признаки, не подлежавшие исключению (выделены в списке): 'Приоритет подозрения на инцидент', 'ID корреляции', 'Категория', 'Источник', Наименование', 'Technique', 'SV-Тип'. Они пошли на обучение модели со всеми своими значениями. Признак 'Вердикт', изначально имевший 5 возможных значений, только одно из которых было связано с инцидентом, преобразован в бинарную целевую метку: 1 – инцидент, 0 – не инцидент.

Признак 'Приоритет подозрения на инцидент' указывает на степень важности подозрительной активности, которая может свидетельствовать о возможном инциденте безопасности. 'ID корреляции' является идентификатором, связанным с определенной категорией правила корреляции, используемого для анализа безопасности в системе SIEM. 'Категория' указывает на

категорию контрольного механизма безопасности и мер по защите информационных систем. Признак 'Источник' указывает, собственно, на источник событий, связанных с мониторингом информационной безопасности в системе SOC. 'Наименование' есть наименование инцидента информационной безопасности, которые могут быть обнаружены и обработаны в системе SOC. 'Technique' это вид техники по матрице mitre attack, на которую сработало правило в SIEM. 'SV-Тип' указывает на типы операционных систем и инструментов, используемых в сети. В данных, характеризуемых отобранными признаками, остаются пропуски, которые нужно убрать, то есть, устранить неполный экземпляр данных или заменить значение отсутствующего признака на наиболее распространенное. И то, и другое можно сделать с помощью метода fillna в библиотеке pandas.

Надо сказать, что этот этап анализа данных SOC существенно зависит от используемых SIEM механизмов и должен рассматриваться отдельно для каждой архитектуры SOC + SIEM.

В нашем случае, как и во всех случаях выявления аномалий, данные содержат очень небольшой процент положительных результатов (инцидентов), то есть, не сбалансированы. Классические модели машинного обучения, имеющие реализации в библиотеках sklearn, keras и других, для классификации на таких обучающих данных не подойдут. Они будут иметь малую точность, сравнимую с наивной моделью (например, объявляющей любое событие инцидентом). Поэтому для решения этой проблемы была использована квантовая нейронная сеть на запутанных состояниях, предложенная в работе [31]. Чтобы передать экземпляр данных в эту квантовую нейронную сеть, нужно закодировать данные в векторы определенной размерности с комплексными значениями, а сами векторы должны быть нормированы на единицу. Все значения признаков переведены в числовые с помощью методов класса LabelEncoder из библиотеки sklearn. В результате, в частном случае рассматриваемого датасета, получилось, что все признаки принимают только целые значения.

Процедура кодирования данных в квантовые состояния заключается в том, чтобы:

1. Привести все значения признаков к целочисленным, лежащим в диапазоне от 0 до известного для каждого признака максимального значения.
2. Преобразовать размерность датасета к ближайшему значению вида $2^{n+1} - 2$, где $n > 1$ — натуральное число, совпадающее с количеством кубитов на входе в квантовую нейронную сеть.
3. Закодировать данные в векторы пространства состояний n-кубитовой квантовой системы.

Первый пункт у нас уже выполнен. Второй пункт может быть легко сделан с помощью библиотеки genser, которая трансформирует весь датасет к заданной размерности, сохраняя при этом словарь перехода, чтобы при необходимости вернуть размерность обратно. Но для этого нужно знать какую размерность выбрать. Для обычных данных (не графических, текстовых или видео) чаще всего достаточно рассмотреть одно из значений 6, 14, 30, 62, 126 в качестве размерности данных. Эти размерности подразумевают число кубитов от 2 до 6, соответственно. Эмпирически выяснилось, что максимальное количество значений на одно вещественное измерение (координату) не должно превышать 20. Поэтому для оценки необходимого числа кубитов для анализа наших данных воспользуемся соотношением

$$\left[\log_2\left(\sum_j \log_{20} M_j\right)\right] \le n \le \left[\log_2\left(\sum_j \log_2 M_j\right)\right],$$

где M_j есть число возможных значений признака j, а минимальное количество значений на одну координату, очевидно, равно 2. В случае рассматриваемого датасета, допустимое число кубитов для кодирования данных равно 2,3 и 4.

Представляя квантовое состояние в виде

$$|q^j\rangle = \sum_{j=0}^{2^n-1} z_k^j |k\rangle, \tag{1}$$

где z_k^j — комплексные амплитуды, встречаем необходимость связать значения компонент x_l^j j-го экземпляра $2^{n+1}-2$-мерных данных с комплексными амплитудами z_k^j. Как показано в [31], эта связь для каждого j может быть следующей:

$$\begin{aligned} z_0^j &= \cos\delta_0^j \dots \cos\delta_{2^n-1}^j, \\ z_1^j &= \sin\delta_0^j \cos\delta_1^j \dots \cos\delta_{2^n-1}^j e^{i\gamma_0^j}, \\ &\dots. \\ z_{2^n-2}^j &= \sin\delta_{2^n-2}^j \cos\delta_{2^n-1}^j e^{i\gamma_{2^n-2}^j}, \\ z_{2^n-1}^j &= \sin\delta_{2^n-1}^j e^{i\gamma_{2^n-1}^j}, \end{aligned} \tag{2}$$

$$\delta_l^j = \frac{\pi x_l^j}{2M_l}, \quad \gamma_l^j = \frac{2\pi x_{l+2^n-1}^j}{M_l}, \quad l = 0, \dots, 2^n-1, \tag{3}$$

где M_j, как и раньше, есть число возможных значений признака j, а значения находятся в диапазоне $0, \dots, M_j - 1$. Таким образом, после проведенных (обратимых) преобразований исходных данных, они имеют вид квантовых состояний (1).

Квантовые состояния, несущие экземпляры данных, уже содержат некоторые взаимосвязи в признаках и каждому состоянию сопоставляется метка (0 или 1). То есть, обучение должно заключаться в том, чтобы выяснить какие взаимосвязи характерны для инцидентов (метки 1). Детально вскрывать эти взаимосвязи не требуется, но нужно построить такую квантовую схему, которая проявит их в измерении. Эта квантовая схема хорошо известна — она представляет собой многокубитовое обобщение квантовой схемы, переводящей запутанные состояния Белла в состояния вычислительного базиса (рис. 1). Далее, для обучения, мы будем собирать статистику измерений на обучающей выборке. Если в данных имеются взаимосвязи, то они неизбежно проявятся в статистике измерений, и для дальнейшей классификации пробного экземпляра потребуется лишь установить к какой из статистик он ближе — к инцидентам (с меткой 1) или не-инцидентам (с меткой 0). Когда вычисления производятся на эмуляторе, в качестве результата обучения можно просто выдавать дискретное распределение вероятностей результатов измерений. В программном коде эксперимента было сделано именно так, то есть, выдавалось не количество экземпляров, давших определенный результат измерения, а именно распределение вероятностей результатов измерений для конкретного экземпляра данных обучающей выборки.

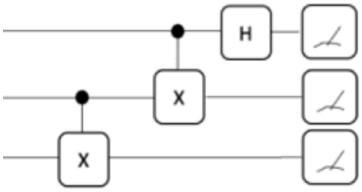

Рис. 1. Квантовая схема для преобразования запутанных состояний в векторы вычислительного базиса.

В соответствии с тем, как закодированы данные, схема на рис. 1 может классифицировать данные, содержащие 14 признаков. Схема для 6 признаков будет содержать на один кубит меньше, а для 30 признаков — на один кубит больше. Наш SOC-датасет содержит 6 признаков и 1 метку, то есть, схему с двумя кубитами к нему можно применить сразу. Но прежде, чем это делать, проведем еще небольшой дополнительный анализ.

Наш датасет, как и все датасеты Центров информационной безопасности, содержит довольно много тождественных экземпляров данных. Бывает так, что один или более таких экземпляров соответствуют инциденту, а остальные — нет. Поскольку в этом исследовании мы предполагаем, что ландшафт угроз не зависит от времени (именно поэтому временная метка не сохранена в пространстве признаков), то если среди группы тождественных экземпляров данных хотя бы один помечен как инцидент, то для обучения системы мы должны считать этот экземпляр соответствующим инциденту. Конечно, в большой выборке с многими идентичными событиями, это приведет к росту числа ложных срабатываний, то есть, увеличится показатель false positive и, следовательно, уменьшится точность (precision). В то же время, такой подход резко снижает вероятность пропустить инцидент и в целом снижает количество шумов в данных. Компании, работающие на рынке информационной безопасности, считают, что этот подход оправдан. Таким образом, нам необходимо оставить в датасете для обучения только уникальные экземпляры данных, причем если данный экземпляр когда-нибудь имел метку 1, то он будет иметь эту метку в обучающем датасете. После такой обработки был сформирован датасет из 1005 экземпляров данных, из которых 40 — инциденты. Как видим, дисбаланс в данных остался, но стал слабее: теперь инциденты составляют чуть меньше 4% экземпляров.

Проведем следующий эксперимент. Разделим отфильтрованную выборку на обучающую и тестовую в пропорции 65/35, сохраняя долю инцидентов в каждой из них. Проведем классификацию 4 способами: три раза используем квантовый нейрон с 2,3 и 4 кубитами, соответственно, а один раз - полносвязную искусственную нейронную сеть (ИНС). Проверять качество классификации будем на тестовой выборке, измеряя две метрики: точность (precision) и полноту (recall). Как известно, первая дает информацию о том, насколько хорошо работает система с точки зрения ложных срабатываний, а вторая — насколько она ставит заслон инцидентам. С практической точки зрения важна именно вторая метрика, но в то же время, наивный классификатор, назначающий инцидент каждому событию, будет давать полноту 100%, но заставит обрабатывать все события как инциденты. Ясно, что для нормального функционирования SOC эта ситуация неприемлема. Поэтому лучшим классификатором будем считать тот, который покажет наибольшую точность при равном или большем значении полноты. Ну и, разумеется, он должен быть лучше наивного классификатора: значение точности должно превышать 4% при полноте равной 100%.

3. РЕЗУЛЬТАТЫ

Квантовые нейроны. Для опыта с 2-частичной системой трансформация размерности данных не нужна и каждый экземпляр непосредственно отображается в двухчастичное квантовое состояние. Для большего числа кубитов потребуется соответствующая трансформация размерности, что может быть выполнено методом обобщенной сериализации, реализованным в модуле genser. Затем все состояния пропускаются через квантовую схему и для каждого получается распределение вероятностей результатов измерения:

$$\{x_i^j\} \to \{z_k^j\} \to \{p_k^j\}, \quad i = 0, \ldots, 2^{n+1} - 3, \quad k = 0, \ldots, 2^n - 1.$$

В данном случае для каждого j имеем 4, 8 или 16 вещественных неотрицательных чисел p_k^j, дающих в сумме 1 (для 2,3 и 4 кубитов, соответственно). Кроме этого распределения, для это-

го экземпляра данных имеется еще метка l^j, принимающая значение 0 или 1. Таким образом, для инцидентов (метка 1) и для не-инцидентов (метка 0) имеются наборы дискретных вероятностных распределений, характеризующие их. Этих наборов столько же, сколько экземпляров данных в обучающей выборке и они представляют собой результат обучения.

Для валидации нашей квантовой модели, пропустим теперь через квантовую схему по очереди все экземпляры тестовой выборки. Для каждого из них получим дискретное распределение вероятностей и будем находить косинусное расстояние между этим распределением и распределениями инцидентов из обучающей выборки. Если встретится такое инцидентное распределение, к которому распределение пробного экземпляра окажется ближе, чем заданное пороговое расстояние, присваиваем пробному экземпляру метку 1 (инцидент). Если такого не нашлось, то присваиваем 0.

Нейронная сеть прямого распространения. Для эксперимента была выбрана нейронная сеть прямого распространения, поскольку в модели предполагается стационарность ландшафта угроз. В противном случае рассмотрение было бы иным и использовались бы рекуррентные нейронные сети. В нейронной сети было взято всего два слоя — этого достаточно чтобы понять обучается ли сеть в принципе. В итоге, как и следовало ожидать, классическая нейронная сеть не обучилась вовсе, поскольку метрики обучения соответствовали наивной модели. Добавление слоев или усложнение архитектуры не приведет ни к какому эффекту, поскольку несбалансированность данных заставляет сеть учитывать паттерны, в основном, не-инцидентов. Попытка использовать оверсемплинг (алгоритм SMOTE) также не дала эффекта: метрики на тестовой выборке остались на том же уровне. Так произошло потому, что методы оверсемплинга (в частности, SMOTE) явно или неявно используют расстояние в пространстве признаков, предполагая, что ближайшие экземпляры с большей вероятностью принадлежат одному классу. В случае событий информационной безопасности расстояние в пространстве признаков никак не коррелирует с классом — расположенный рядом с инцидентом экземпляр не имеет повышенной вероятности быть инцидентом. Но расстояние в пространстве распределений вероятности результатов квантовых измерений коррелирует с классом, так как учитывает зависимости в данных, присущие инцидентам. Поэтому квантовый нейрон воспринимает обучение в рассматриваемом случае, в отличие от классической нейронной сети.

Результат работы всех моделей представлен в таблице 1 Классическая двухслойная нейро-

Таблица 1. Качество классификации квантовыми нейронами и классической нейронной сетью

Модель	Precision	Recall
2-частичный q-нейрон	6,3%	85%
3-частичный q-нейрон	5,5%	100%
4-частичный q-нейрон	3,7%	93%
2-слойная ИНС	4,0%	100%

сетевая модель с архитектурой, представленной на рис. 2, достигает 100% полноты (recall), но точность (precision) довольно низкая 4% (продемонстрировано на рис. 3). В то время, как квантовая модель с 3 частицами обеспечивает полноту в 100% при более высокой точности 5.5% (рис. 4). Как видим, с точки зрения практического применения, имеет смысл использовать 3-частичный квантовый нейрон (он изображен на рис. 1). Эта система не пропускает инциденты и, так как точность ее на 37% выше, чем у классической нейросети, рекомендации мер против инцидентов она будет давать не каждому событию, а примерно 2/3 из них. Кроме того, раз q-нейрон обучается, то с приходом в SOC информации о новых инцидентах, качество классификации будет увеличиваться. Но для этого нужно или больше данных, или более продолжительное наблюдение. Еще одна возможность состоит в увеличении количества значимых признаков в описании события.

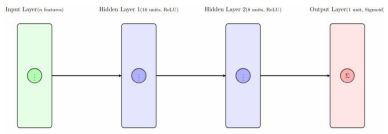

Рис. 2. Архитектура классической двухслойной нейронной сети.

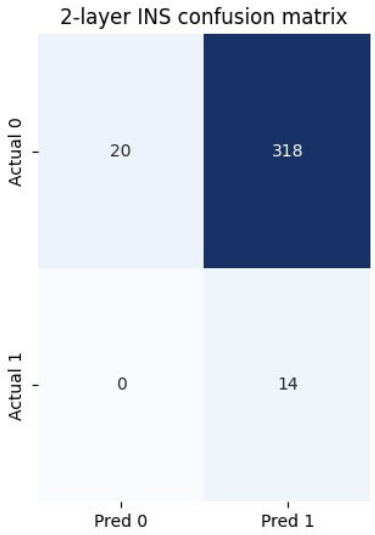

Рис. 3. Матрица ошибок для классической двухслойной нейронной сети.

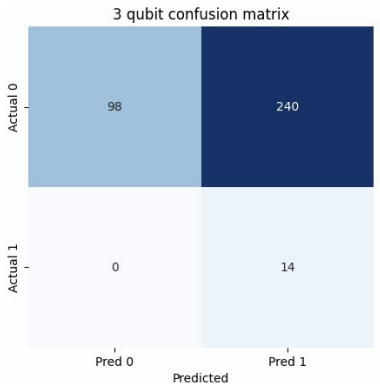

Рис. 4. Матрица ошибок для 3-частичной квантовой модели.

Такие процедуры классификации могут работать практически на любом устройстве. Указанный выше эксперимент проводился на машине с процессором Intel Core I5 и ОЗУ 16Гб в одном потоке.

4. ЗАКЛЮЧЕНИЕ

В результате проведенного исследования была разработана интеллектуальная система на основе квантового нейрона, предназначенная для классификации событий информационной

безопасности и выявления инцидентов. В проведенном эксперименте квантовая модель с тремя кубитами обеспечила полноту выявления инцидентов 100% и точность 5.5% против 4% у классической нейросети. Таким образом, система не пропускает инциденты и снижает количество ложных срабатываний по сравнению с традиционными методами.

5. БЛАГОДАРНОСТИ

Авторы выражают благодарность ООО Инфосекьюрити за любезную подготовку (обезличивание) и предоставление данных Центра информационной безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. *Cybercrime To Cost The World $10.5 Trillion Annually By 2025* [Electronic resource]. – Mode of access: https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/ - Date of access: 18.08.2024.

2. *Global Cybersecurity Outlook 2022* [Electronic resource]. – Mode of access: https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf – Date of access: 18.08.2024.

3. *Cost of a Data Breach Report 2022* [Electronic resource]. - Mode of access: https://www.key4biz.it/wp-content/uploads/2022/07/Cost-of-a-Data-Breach-Full-Report-2022.pdf - Date of access: 18.08.2024.

4. *Global Cybercrime Damages Predicted To Reach $6 Trillion Annually By 2021* [Electronic resource]. - Mode of access: https://cybersecurityventures.com/annual-cybercrime-report-2020 – Date of access: 18.08.2024.

5. *The biggest cyberattacks of 2022* [Electronic resource]. - Mode of access: https://www.bcs.org/articles-opinion-and-research/the-biggest-cyber-attacks-of-2022/ – Date of access: 18.08.2024.

6. *Saleem S., Sheeraz M., Hanif M. and Farooq U.* Web server attack detection using machine learning // in Proceedings of 2020 International Conference on Cyber Warfare and Security (IC-CWS), Islamabad, Pakistan, 2020. 1-7.

7. *Hwang W.S., Shon J.G. and Park J.S.* Web session hijacking defense technique using user information // Human-centric Computing and Information Sciences. 2022. Vol. 12. art. 16. https://doi.org/10.22967/HCIS.2022.12.016

8. *Tang D., Dai R., Tang L. and Li X.* Low-rate DoS attack detection based on two-step cluster analysis and UTR analysis. // Human-centric Computing and Information Sciences. 2020. Vol. 10. art. 6. http://dx.doi.org/10.1186/s13673-020-0210-9

9. *Alqahtani A.and Sheldon F.T.* A survey of crypto ransomware attack detection methodologies: an evolving outlook. // Sensors. 2022. Vol. 22. N. 5, art.1837. https://doi.org/10.3390/s22051837

10. *Kshetri N. and Voas J.*. Ransomware: pay to play? // Computer. 2022. Vol. 55. N. 3. 11-13. https://doi.org/10.1109/MC.2021.3126529

11. *Tcydenova E., Kim T. W., Lee C., Park J. H.* Detection of adversarial attacks in AI-based intrusion detection systems using explainable AI. // Human-centric Computing and Information Sciences. 2021. Vol. 11, art. 35. https://doi.org/10.22967/HCIS.2021.11.035

12. *Baldassarre M.T., Barletta V.S., Caivano D., Raguseo D. and Scalera M.* Teaching Cyber Security: The HACK-SPACE Integrated Model. // In Proceedings of the ITASEC, Pisa, Italy, 13–15 February 2019. https://ceur-ws.org/Vol-2315/paper06.pdf

13. *Infotecs ViPNet TIAS* [Electronic resource]. Mode of access: https://infotecs.ru/downloads/documents/vipnet-tias/ - Date of access: 18.08.2024.

14. *ИТ Энигма* [Electronic resource]. Mode of access: https://it-enigma.ru/produktyi/zashhita-ot-czelevyix-atak - Date of access: 18.08.2024.

15. *Splunk, a CISCO company* [Electronic resource].
Mode of access: https://www.splunk.com/en_us/products/splunk-enterprise-security-features.html - Date of access: 18.08.2024.

16. *Biamonte J., Wittek P., Pancotti N. et al.* Quantum machine learning. // Nature. 2017. 549. 195–202. https://doi.org/10.1038/nature23474

17. *Huang H. et al.* Quantum advantage in learning from experiments. //Science. 2022. 376. 1182-1186. https://doi.org/10.1126/science.abn7293

18. *Сигов А.С., Андрианова Е.Г., Жуков Д.О., Зыков С.В., Тарасов И.Е.* Квантовая информатика: обзор основных достижений. // Russian Technological Journal. 2019. Т. 7. №1. 5–37. https://doi.org/10.32362/2500-316X-2019-7-1-5-37

19. *Zeguendry A., Jarir Z., Quafafou M.* Quantum Machine Learning: A Review and Case Studies. // Entropy. 2023. V.25. N.2. 287. https://doi.org/10.3390/e25020287

20. *Hu W.* Empirical Analysis of a Quantum Classifier Implemented on IBM's 5Q Quantum Computer. // Journal of Quantum Information Science. 2018. V.8. 1-11. https://doi.org/10.4236/jqis.2018.81001

21. *Irfan M., Jiangbin Z., Iqbal M., Masood Z., Arif M.* Knowledge Extraction and Retention Based Continual Learning by Using Convolutional Autoencoder-based Learning Classifier System. // Information Sciences. 2022. V. 591. http://dx.doi.org/10.1016/j.ins.2022.01.043

22. *Maheshwari D., Garcia-Zapirain B. and Sierra-Sosa D.* Quantum Machine Learning Applications in the Biomedical Domain: A Systematic Review // in IEEE Access 2022. V. 10. 80463-80484. https://doi.org/10.1109/ACCESS.2022.3195044

23. *Lloyd S., Mohseni M., Rebentrost P.* Quantum algorithms for supervised and unsupervised machine learning. // arXiv:1307.0411. https://doi.org/10.48550/arXiv.1307.0411

24. *Lloyd S.* Least squares quantization in PCM. // IEEE Trans. Inf. Theory 1982. V. 28. N. 2. 129–137. https://doi.org/10.1109/TIT.1982.1056489

25. *Lloyd S., Mohseni M., Rebentrost P.* Quantum principal component analysis. // Nat. Phys. 2014. V. 10. N. 9. 631–633. https://doi.org/10.1038/nphys3029

26. *Jiang Z., Rieffel E.G., Wang Z.* Near-optimal quantum circuit for Grover's unstructured search using a transverse field. // Phys. Rev. A. 2017. V. 95. N. 6. 062317. https://doi.org/10.1103/PhysRevA.95.062317

27. *Simões R.D.M., Huber P., Meier N., Smailov N., Füchslin R.M., Stockinger K.* Experimental Evaluation of Quantum Machine Learning Algorithms. // IEEE Access. 2023. V.11. 6197–6208. https://doi.org/10.1109/ACCESS.2023.3236409

28. *Menneer T., Narayanan A.* Quantum-inspired neural networks. // In: Proceedings of the Neural Information Processing Systems 95. Denver, CO, USA, 27–30 November 1995. URL: https://www.researchgate.net/publication/2267350_Quantum-inspired_Neural_Networks

29. *Cong I., Choi S., Lukin M.D.* Quantum convolutional neural networks. // Nat. Phys. 2019. V.15. N.12. 1273–1278. https://doi.org/10.1038/s41567-019-0648-8

30. *Гушанский С.М., Буглов В.Е.* Квантовое глубокое обучение сверточной нейронной сети с использованием вариационной квантовой схемы. // Известия ЮФУ. Технические науки. 2021. Т.7. №224. 167–174.

31. *Зуев С.В.* Геометрические свойства квантовой запутанности и машинное обучение. // Russian Technological Journal. 2023. Т.11. №5. 19–33. https://doi.org/10.32362/2500-316X-2023-11-5-19-33

32. *Зуев С.В.* Статистическое онлайн-обучение в рекуррентных и прямого распространения квантовых нейронных сетях. // Докл. РАН. Математика, информатика, процессы управления. 2023. Т. 514. № 2. 177–186. https://doi.org/10.31857/S268695432360129X

Quantum intelligence system to recognise incidents among the information security events

D. A. Gorodisky, S. V. Zuev

The purpose of the work is to build a good binary classifier that recognizes an information security incident among events by the values of the features. A direct propagation quantum neural network is used as a machine learning model. Data preparation is done by conventional methods, but instead of normalization, data reduction to integer vectors is used to further bring the data dimension to values suitable for a quantum neural network. The data for analysis are anonimiized data from one of the information security centers of the city of Moscow, collected for the year. The Python programming language and open source libraries were chosen as the tools for research. The work implements a statistical machine learning method that allows real-time learning. As a result of the research, an intelligent system has been built, which builds a very plausible assumption that the event belongs to the class of incidents based on the values of the known values of features of security events. Thus, the system allows anybody to recognize an event that is highly likely to lead to damage, and for which an immediate response is justified. The system is tested on real data, which is characterized by the same imbalance as the training samples of information security events. That is, it has a very low proportion of incidents (less than a percent). It was found that incidents are detected with high quality, with a minimum of false positives and a high percentage of correctly recognized incidents. This confirms the reliability and effectiveness of the proposed quantum intelligent system, and also suggests that systems of such an architecture can be used in other cases where data imbalance makes it difficult to use classical machine learning.

KEYWORDS: quantum machine learning, quantum neural network, information security incident, unbalanced training samples, unbalanced data.