REDS:

Телекоммуникационные устройства и системы

№1

2023

СОДЕРЖАНИЕ

ТЕХНОЛОГИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ЗАДАЧАХ КИБЕРБЕЗОПАСНОСТИ НА ПРИМЕРЕ АНТИФРОДА

Амиров Данис Фанисович,
Московский технический университет связи и информатики,
старший преподаватель кафедры «Цифровое телерадиовещание и информационная безопасность»;
ГК «АЙТИКОМ», руководитель направления «Информационная безопасность», преподаватель,
к.п.н., доцент, Москва, Россия
d.amirov@itcomgk.ru

Аннотация

В этой статье рассматривается связь систем искусственного интеллекта и кибербезопасности. В современной трактовке, системы искусственного интеллекта – это системы машинного обучения, иногда это еще более сужается до искусственных нейронных сетей. Если мы говорим о все более широком проникновении машинного обучения в разные сферы применения информационных технологий, то, естественно, что должны возникать пересечения с кибербезопасностью. Но проблема в том, что такое пересечение не может быть описано какой-то одной моделью. Сочетания искусственный интеллект и кибербезопасность имеют множество разных аспектов применения. Общим является, естественно, использование методов машинного обучения, но задачи, а также достигнутые на сегодняшний день результаты, являются совершенно разными. Например, если применение машинного обучения для обнаружения атак и вторжений показывает реальные достижения по сравнению с применявшимися ранее подходами, то атаки на сами системы машинного обучения пока полностью побеждают возможные защиты. Классификации моделей применения машинного обучения в кибербезопасности и посвящена данная статья.

Ключевые слова: *искусственный интеллект, машинное обучение, кибербезопасность, информационная безопасность, информационные технологии.*

Введение

Искусственный интеллект (ИИ) помогает решать задачи машинного обучения (ML).Основная задача машинного обучения – разработка алгоритма, который работает с данными для принятия каких-либо решений.

ИИ – свойство интеллектуальных систем – выполнять творческие функции, которые традиционно считаются прерогативой человека. ML – класс методов ИИ, характерной чертой которых является не прямое решение задач, а обучение за счет применения решений множества сходных задач.

Ключевое отличие разработки моделей машинного обучения и систем принятия решений от традиционной разработки программного обеспечения в том, что человек не закладывает определенную логику и не реализует ее в программе принятия решений. Вместо этого используются алгоритмы, которые на основании данных строят деревья решений и решающие поверхности многомерных пространств. То есть после подачи на вход в систему новых данных ужесами алгоритмы выносят вердикты на основании виденных ими ранее данных, использованных дляобучения. Человек не влияет на принятие решения. Он влияет только на подбор примеров, на которых алгоритм обучается, а также алгоритмов, которые должны будут решать задачи [1].

Машинное обучение находится на вершине пирамиды эволюции обработки данных. Но для качественного решения задач модели необходимо обеспечить релевантными и регулярно поступающими данными. Четыре класса задач машинного обучения:

- ✓ Обучение с учителем:
  - o классификация нового объекта: есть массив данных, описания для отнесения к тому или иному классу и сами классы. В модель подаются новые объекты с их описаниями, модель определяет, к какому классу относится объект;
  - o регрессия: предсказание числового значения, числовая оценка чего-либо в зависимости от различных условий.
- ✓ Обучение без учителя:
  - o кластеризация: разделение объектов массива данных на кластеры с выявлениемособенностей

каждого, чтобы вести более точечную работу с ними;

- поиск аномалий в данных: сначала строится модель нормальности данных,затем выявляются отклонения и проводится дополнительный анализ.

✓ Обучение с частичным привлечением учителя: под имеющийся большой массив данных есть правила разметки только для части данных. В этом случае применяются специальные алгоритмы, которые пытаются разметить остальные данные.

✓ Обучение с подкреплением: машина с ИИ автоматически учится в среде взаимодействия, соблюдая определенные правила.

В кибербезопасности чаще всего возникают задачи обучения с учителем и в меньшей степени задачи кластеризации и поиска аномалий. Если применение ИИ изобразить на координатной плоскости, то на одной оси будет класс задачи и используемый алгоритм, на другой - характеристики массива данных. Выделяют две категории данных:

✓ структурированные: можно естественным образом представить в виде таблицыв базе данных, каждый элемент данных обладает общей структурой (например,транзакции клиентов, сетевой трафик);

✓ неструктурированные: каждый элемент данных уникален (например,видеоизображение, картинки, текст, запись голоса).

В вопросах кибербезопасности чаще всего работают с неструктурированными данными(документы в форматах .pdf, .doc, почтовая переписка, изображения). Таким образом, при решении задач в машинном обучении необходимо определить класс задачи и категорию данных. Исходя из этого выбираются алгоритмы и подходы.

Ключевые области применения ИИ в кибербезопасности:

✓ противодействие мошенничеству, антифрод: оценка риска транзакций (насколько операция может быть мошеннической, а клиент - мошенником);

✓ расследования: по уже известным или предотвращенным случаям мошенничества выявляются дополнительные связи мошенников;

✓ киберзащита: выявление аномалий, заражений хостов, DDos-атак, их предотвращение, выявление фишинговых доменов;

✓ контроль конфиденциальной информации: нельзя допустить, чтобы информация, содержащая банковскую или коммерческую тайну, переместилась за периметр обработки либо попала в домены, где ее не должно быть.

Для противодействия социальной инженерии используются схожие модели ИИ, что и для противодействия мошенничеству в целом, но они изучают другие признаки операций.

Зрелость open source ML-библиотек/инструментов позволяет использовать готовый продукт для решения сложных практических задач. Текущие data science-технологии построены на open source-решения. Они эффективны для разработки моделей машинного обучения. Рынок open source-решений активно развивается благодаря тому, что промышленные корпорации публикуют внутренние инструменты, а сообщество разработчиков совершенствует их [2],[3].

Структурированные данные и деревья решений

Алгоритм дерева решений построен на том, что каждому классу объектов присваивается область определенных признаков. Например, обычный клиент получает денежные переводы, 70% из них тратит на покупки, 20% - переводит, 10% - копит. Мошенник постоянно получает деньги из неизвестных источников и тут же переводит их другим.

Дерево решений:

✓ делит область признаков на площади;

✓ относит экземпляры данных объекта к тому или иному классу на основании построенной области;

✓ определяет, сколько признаков представляют тот или иной класс;

✓ перебирает доступные атрибуты,

✓ ищет сплиты (точки разделения по данным) с использованием математических функций оптимизации.

Путь в дереве – соответствие правилам: если признак меньше какого-то значения, идем по одной ветке, если больше – по другой. Таким образом, приходим в «листы деревьев», где есть представители классов.

Деревья решений – простой и интерпретируемый алгоритм, поскольку всегда есть правило,почему дерево отнесло экземпляр данных к одному или другому классу. Главный недостаток алгоритма – невозможность описать сложные зависимости данных только с помощью запоминания примеров, что вытекает в «переобучение» алгоритма. Сталкиваясь с новыми данными, он дает плохой результат.

Следующий этап развития обработки структурированных данных предусматривает построение не одного дерева, а ансамбля деревьев – «леса» решений – алгоритм **Random forest** (случайный лес). Его принцип работы - обучающая выборка с помощью сэмплирований с возвращением делится на подмножества известных кейсов и доступных признаков. На каждом из подмножеств строится дерево решений. Деревья строятся не глубокими, а по принципу «weak learns» - слабыми с точки зрения принятия решения. Так как они неглубокие, не подвергаются переобучению, а строится их много, то итоговый алгоритм усредняет их предсказания о принадлежности к классу. На основании этого принимает решение.

Алгоритм Random forest достаточно устойчив к переобучению и позволяет описывать сложные закономерности, так как процессы проходят параллельно (рис. 1).

Рис. 1. Алгоритм Random forest

Более современный алгоритм – **Gradient boosting**. Он также строит множество деревьев решений, но по другому принципу - деревья строятся поэтапно. Сначала алгоритм делит пространство данных по одному признаку, выделяет максимально чистые выборки данных, остальное считает «ошибками». Затем он то же самое делает с оставшимся пространством «ошибок», делит его по следующему признаку. Таким образом, на каждой итерации алгоритм классифицирует часть объектов по определенному признаку, поэтапно охватывая все изначальноепространство (рис. 2).

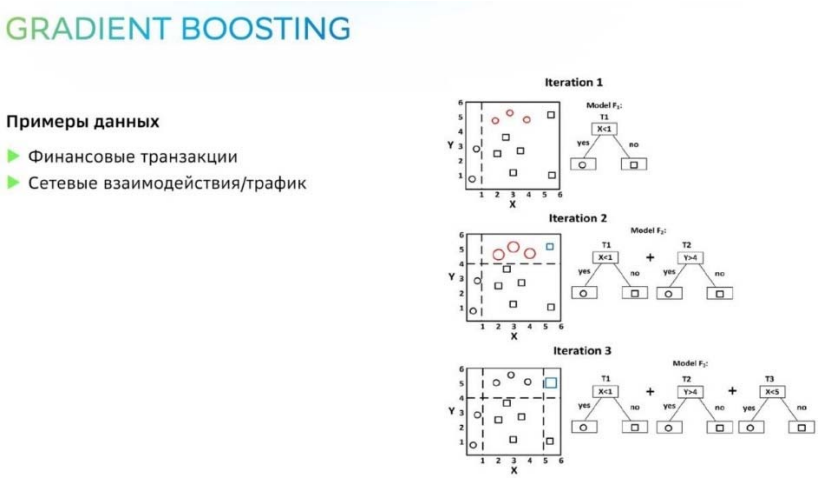

Рис. 2. Алгоритм Gradient boosting

Главное преимущество алгоритма Gradient boosting в том, что он показывает более стабильные и лучшие результаты при правильном обучении и подборе параметров. Однако он чувствителен к «шумам» и пропускам в данных и подвержен переобучению. При наличии большого числа пропусков данных лучше использовать алгоритм Random forest.

Для выявления глобальных аномалий (data outliers) используется алгоритм **Isolation forest**. Он строит множество деревьев, деля пространство данных на блоки, и схож с Random forest - использует подмножество выборки. По итогам данный алгоритм дает скоринг того, что элемент данных является аномальным. Аномальным он считается потому, что в пространстве признаков егоможно быстро выделить, т.е. изолировать как вершину. Гипотеза данного алгоритма заключается втом, что обычные данные располагаются скученно, образуют кластер, а аномалии лежат на границах либо за границами классов (рис. 3).

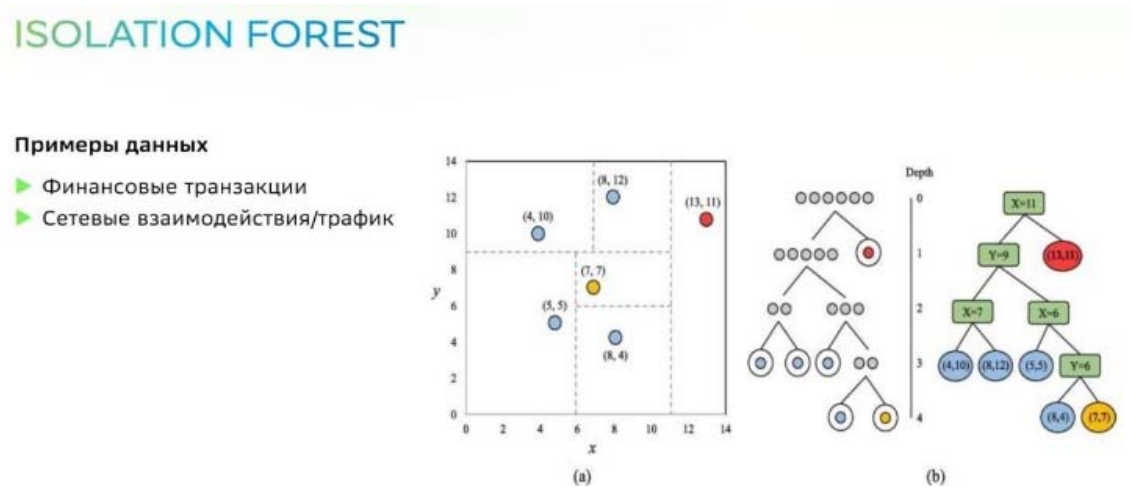

Рис. 3. Алгоритм Isolation forest

В антифрод-системах в большей степени используются модели, построенные на алгоритме Gradient boosting. Он хорошо решает задачи с учетом сильного дисбаланса классов: количественное отношение мошеннических транзакций к легитимным составляет десятитысячныеи стотысячные. Например, алгоритм Gradient boosting применяется для выявления дроп-счетов, через которые выводятся похищенные средства, классификации обращений по жалобам клиентов инразные типы.

Алгоритм Random forest применяется в работе команды по киберзащите – SOC, которая отвечает за оперативное реагирование на инциденты кибербезопасности. Он помогает специально разработанным моделям ранжировать возникающие инциденты, чтобы SOC мог сфокусироваться на наиболее рисковых и релевантных. Команда SOC с использованием графа связей инцидентов, данных о трафике, данных из карточек инцидентов построила большое пространство признаков и применила алгоритм Random forest. Получилась модель высокой точности и полноты – 99,99%, а время реакции на инциденты снизилось на 15%. Модель определяет ML-вероятность угрозы и ранжирует инциденты, чтобы, в первую очередь, брать в работу наиболее существенные. Также она определяет false positive срабатывания SIEM-систем.

Для применения данных алгоритмов не нужны большие объемы данных. Достаточно выборки в 100 кейсов, когда классы сбалансированы и в каждом есть не менее 30 представителей.Для задачи бинарных классификаций этого достаточно. Если стоит задача с сильным дисбалансом классов, то необходимо иметь 50-100 кейсов для минорного класса.

Например, когда Сбербанк начинал задачу классификации обращений, было всего около 100 размеченных кейсов. Специалисты обучали алгоритм, проводили итерацию, размечали другие кейсы жалоб на мошенничество по классам. Таким образом, собрали полную выборку, и после нескольких циклов была готова хорошая модель.

Удаленное обслуживание клиента может быть приостановлено и заблокировано, если естьподозрение, что он находится под мошенническим влиянием посредством социальной инженерии.

Примером open source-решения, используемого в Сбербанке - алгоритм Gradient boosting библиотеки LightGBM, которая была опубликована Microsoft. Алгоритм Random forest также является публичной реализацией.

Принципы приоритизации при ранжировании в технологии ML зависят от формулировки задачи. В рамках задачи есть релевантность кейсов, и постановщик задачи знает, как их ранжировать. Правила закладываются в модель и функцию, которая оптимизируется. Чем лучше модель определила ранг, тем большая метрика и качество ею достигаются. В задаче фрод-мониторинга ранжирование должно быть таково, чтобы мошеннические операции были со скорингом выше легитимных.

Модели ML по определению выбросов, в частности Isolation forest, используются в Сбербанке для изучения частотности взаимодействия клиентов по операциям. Аномалии могут носить злонамеренный характер, либо характер ботов. В алгоритме Gradient boosting применяется метод стохастического градиентного спуска, чтобы оптимизировать функцию потерь.

Концепция Embedding: применение в графах

Два подхода к созданию признаков (фичей) для моделей ИИ:

✓ **Экспертный, ручной подход.** Чтобы построить высоко эффективные модели противодействия мошенничеству, сырых данных недостаточно. Для этого привлекаютсяэксперты предметной области. В дополнение к структурированным данным, содержащие и сырые данные, эксперт придумывает дополнительные признаки, которые можно обсчитать по временным окнам, с использованием математических статистик и другими способами;

✓ **Representation learning (Deep learning)** – глубокое обучение. Суть подхода:закодировать структурную информацию о графе в пространство меньшей размерности,но с сохранением «близости» между вершинами. Данные передаются в сыром виде, отчеловека не требуется обогащение дополнительными признаками. Нейросеть самостоятельно послойно учится находить оптимальное представление, чтобы решить поставленную задачу. К последнему слою применяется классификатор, который решает,к какому классу отнести данный слой либо какое предсказание выдать. Embedding – последний слой сети, который представляет вектор из чисел. Последние embedding- слои необходимо передавать в классические модели, чтобы увеличить их эффективность.

В кибербезопасности Сбербанка регулярно рассчитывается 2 крупных графа. Первый применяется в антифроде. Это граф транзакций клиентов, их взаимодействия между собой, с устройствами. В нем свыше 1 млрд вершин и 6 млрд ребер. Второй граф применяется в киберзащите. Он отображает сетевое оборудование, в котором свыше 1,5 млн серверов, ПК пользователей, конечные устройства, протоколы и порты взаимодействия. В нем более 250 тыс. ребер.

Для усиления эффективности принятия решений в машинном обучении целесообразно использовать модели, которые анализируют графы. Поэтому необходимо задачу представлять не только в структурированном виде, но и в виде графа взаимодействия объектов. К графам можно применять подход ручного расчета признаков традиционными методами. Но такой подход не масштабируется на большие графы, это займет слишком много времени. А в противодействии мошенничеству и реагировании на инциденты SLA составляет секунды и миллисекунды.

Пример репрезентативного обучения на графе в сбербанке для решения задач антифрода

Задача - построить для каждой вершины (клиента) в графе с 250 млн вершин и 2,2 млрд ребер embedding-вектор из 256 параметров с важным свойством, чтобы в этом многомерном пространстве после применения математической операции (например, косинусной близости):

- ✓ большое значение означало, что эти вершины в графе близки и взаимодействуют;
- ✓ маленькое - говорило, что вершины никак не связаны и располагаются далеко другот друга.

Для анализа графа антифрода и среза данных за год использовано open source - решение PyTorch BigGraph, в котором было изменено только представление данных. Решение позволяет анализировать большие графы как с использованием одного мощного сервера, так и параллельно на нескольких с меньшими мощностями. По итогам 4,5 дней расчетов решением PyTorch BigGraph было получено 300 Gb данных и для каждой вершины построен вектор из 256 чисел.

Далее было выдвинуто две гипотезы для проверки полученных embedding-векторов: действительно ли взаимодействующие вершины-клиенты в графе находятся ближе друг к другу, чем случайные.

Гипотеза 1. Между клиентами, живущими в одном регионе, с большей вероятностью возникают транзакции, чем между клиентами, которые живут в удаленных друг от друга регионах.Было взято по 1000 клиентов из трех территориальных банков Сбера. Векторы данных, полученные по клиентам по итогам расчетов PyTorch BigGraph, были отображены в двухмерном пространстве на плоскости. Это

дало возможность отследить несколько закономерностей:

✓ Часть точек-вершин действительно распределилась по территориальному признаку и неперемешивалась;

✓ Появились отдельные кластеры, где вершины из разных банков перемешались, что говорило об общей хозяйственной деятельности или активном взаимодействии клиентов.

Важно отметить, что для анализа был взят граф транзакций между клиентами, о географической принадлежности которых модель решения PyTorch BigGraph не знала.

Гипотеза 2. Между графами взаимодействующих клиентов косинусная близость почти равна 1. Чем ближе косинусная близость к 1, тем ближе клиенты между собой. Гипотеза была проверенана нескольких сотрудниках. Ближайшими к ним точками в графе оказались родственники, друзья и близкие, затем - внешнее окружение (коллеги, бизнес-контакты, клиенты), чья близость была в два раза меньше. Близость произвольных клиентов к выбранным сотрудникам была равна 0.

Таким образом, embedding-векторы дали представление, насколько клиенты связаны между собой, если их вершины на графе близки. Это позволило снизить ложные срабатывания системы противодействия мошенничеству на 10-15% (когда легитимная операция приостанавливалась как мошенническая) и при этом не ухудшить выявление мошеннических операций.

Предрасчет embedding-векторов для клиентов проводится на регулярной основе, что позволяет использовать их в системах в режиме реального времени.

Идеальных моделей ИИ, которые не допускают ошибки в анализе данных, не существует. Поэтому в системах противодействия мошенничеству неизбежны ложные срабатывания из-за несовершенства алгоритмов. Преимущество графового представления данных в машинном обучении в том, что оно показывает взаимосвязь объектов между собой и наличие взаимодействия между ними. Если данные взаимодействия важны, то графовые модели закладываются в различные системы кибербезопасности и учитывают их. Если возникает интенсивное взаимодействие между группами, которого ранее не было, это может быть признаком аномалии.

Deep Neural Networks (DNN) для текстов

В задачах кибербезопасности много текстовой информации. Нейронным сетям предшествовали алгоритмы анализа текста, которые и сейчас активно применяются. Алгоритм **Bagof Words** («мешок слов») работает следующим образом. Корпус текстовых данных, которые необходимо проанализировать (сообщения, документы), представляется в виде отдельных слов. Незначимые слова (предлоги, междометия, союзы) исключаются из данного массива. Получается словарь слов, которые встречались во всех текстах. Словарь кодируется для использования в моделях классического машинного обучения. Т.е. для структурирования текстовых данных достаточно присвоить «1» словам, которые встречались в каждом документе. Недостаток алгоритма в том, что он не учитывает контекст и частотность, только встретилось слово или нет.

В отличие от Bag of Words алгоритм TD/IDF анализирует, сколько раз встретилось слово в документе, а также насколько оно специфично именно для данного документа или встречается в других. Слова могут быть более релевантными для определенного документа, что упрощает решение задачи. Далее каждому слову присваивается вес, показывающий, насколько часто оно встречается в документах. Чем больше вес, тем более значимо слово в рамках корпуса текстовых данных. В частности, это поможет решить задачу классификации. Недостаток алгоритма тот же – он не анализирует контекст, последовательность слов. Если взят большой словарь слов, векторы могутбыть разреженными (рис. 4).

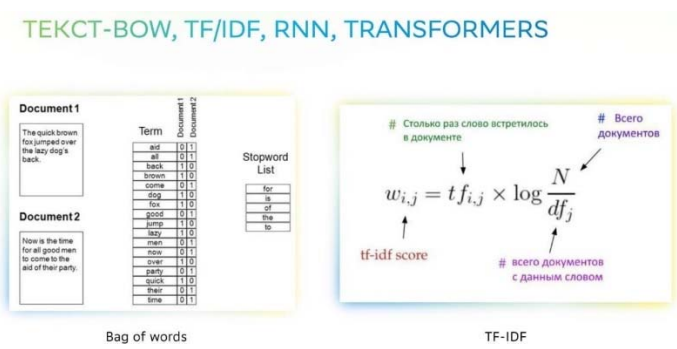

Рис. 4. Алгоритмы Bag of Words, TD/IDF

Следующий этап в развитии качества обработки текстовых данных – рекуррентные нейронные сети, RNN. Внутри RNN-сети есть матрица с обучаемыми параметрами. Они запоминаютинформацию, которая через них проходила, чтобы лучше выдавать ответ. Для анализа текстов в сеть последовательно передаются слова из предложений текста. Сеть выдает для каждого слова вектор или финальное представление, вероятность классификации текста (рис.5.) [4].

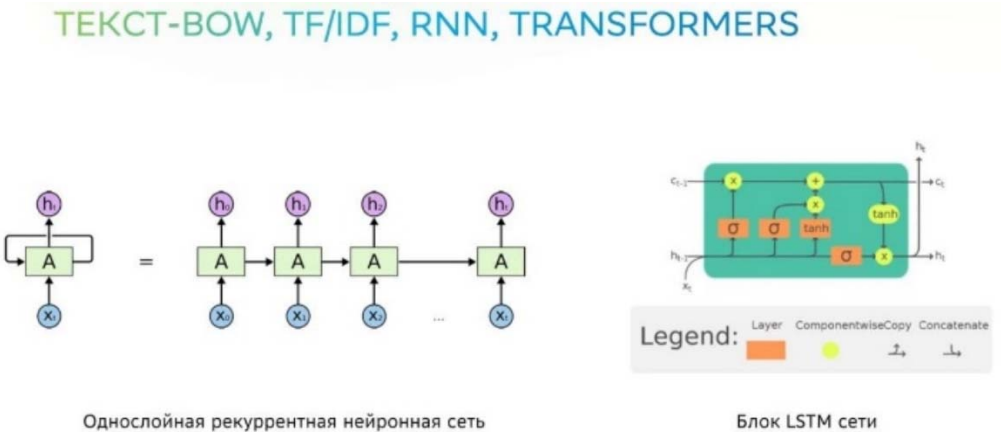

Рис. 5. Рекуррентные нейронные сети RNN

Пример задачи кибербезопасности по анализу текста с помощью алгоритма RNN

Задача – определить, относится ли письмо к спаму и является ли рассылка мошеннической.

На основании текста необходимо определить вероятность, где 0 – легитимное письмо, 1 – зловредное или спам. Сначала в RNN-сеть передается одно слово, алгоритм выдает результат, но при этом обновляет внутренние параметры. В алгоритм передается слово за словом, и он каждый раз учитывает контекст предыдущих слов, которые видел.

Самый известный представитель RNN-сети – рекуррентная сеть Long Short-Term Memory (LSTM). Это сеть с глубокой короткой памятью. Внутри нее есть элементы, которые позволяют эффективно запоминать слова, которые она видела ранее, и учитывать контекст недавних слов.

Важная особенность - слова не обязательно передавать слева направо, существуют двунаправленные сети.

RNN-сети совершили революцию в обработке текстов, так как существенно подняли уровеньи качество. Если важен именно контекст, рекуррентные сети – основной подход, который стоит применить. Недостаток: RNN-сетям требуются большие объемы данных, специализированное оборудование для эффективного обучения. Для классических моделей требуются обычные процессоры CPU, серверы, иногда много памяти, а для RNN-сетей необходимы графические ускорители и специализированные видеоадаптеры.

Наиболее передовой подход к обработке текстов – трансформеры. Он применяется в сложных больших задачах работы с текстами. В трансформерах много слоев, которые обучаются параллельно, данные передаются между слоями. Главное отличие трансформеров - на вход подаются не отдельные слова, а блоки текста. Трансформеры преобразуют текстовые данные, учитывают взаимозависимость положений слов между собой и понимают, на каких словах им стоит сфокусироваться. Для обучения трансформеров необходима определенная инфраструктура.

Трансформеры демонстрируют лучшие результаты по анализу и обработке текста. Зачастуюони переводят и генерируют текст на таком высоком уровне, что не всегда можно отличить, кто его автор - человек или машина.

Пример применения алгоритмов анализа текста - Threat Intelligence Platform.

Она выявляет на ранней стадии угрозы и уязвимости, реагирует на них. В рамках платформыосуществляется мониторинг текстовой новостной информации о выходе новых уязвимостей, их эксплуатации, угрозах.

Для оценки аналитиками релевантности, ранжирования новостной информации (новостей публикуется огромное количество, одними словами говорится об одном и том же) реализован ансамбль из нескольких моделей ИИ. Каждая модель обучалась на своем подмножестве: одна – на тексте самой

новости, другие – на заголовках. Для выявления упоминания определенных подверженных уязвимостей продуктов и самих уязвимостей использовался алгоритм TD/IDF, который представлял данную информацию через векторы. Далее использовался дополнительный собственный подход к векторному представлению текстов. После чего полученные данные применяли в обычных моделях. В частности, использовались:

- ✓ алгоритм Random forest (так как данные сильно «зашумлены» и несбалансированы);
- ✓ логистическая регрессия.

В данном случае нет необходимости использовать сложные алгоритмы, так как важен не контекст, а ключевые слова.

С использованием данных алгоритмов удалось построить модели, которые позволяют с точностью 93% выявлять релевантные новости и присваивать им необходимый скоринг для ранжирования, чтобы аналитики начинали разбирать их как можно раньше. Нерелевантные новости модели Threat Intelligence Platform не показывают. Нагрузка на аналитиков сократилась в 5 раз.

Пример по анализу текста для контроля конфиденциальной информации

Чтобы провести анализ массива документов различного формата, применяется система с ансамблем моделей. Модели не только выявляют конфиденциальную информацию, но и определяют, какого она рода. Они распознают 58 видов конфиденциальной информации. В этом ансамбле моделей используются транформер, алгоритм рекуррентной сети и сверточные нейронные сети. Система предоставляет отчет по итогам анализа текста, в котором выделяет цветом, в каких разделах выявлена конфиденциальная информация. При ее выявлении прекращается пересылка документов в сегменты, где данные не должны появиться. Документы обезличиваются, проходят повторную проверку и передаются дальше [5].

Convolutional neural network (CNN) для изображений. Объединение подходов

Для анализа и обработки изображений применяется алгоритм сверточной нейронной сети - CNN. Принцип работы данного алгоритма: имеющееся изображение сканируется сверткой - небольшой матрицей, которая проходит по изображению и из квадрата изображения трансформирует в пространстве меньшей размерности какой-то признак. Таких сверток много, с каждым слоем их становится все больше. Таким образом, изображение послойно дробится на более мелкие (рис. 6).

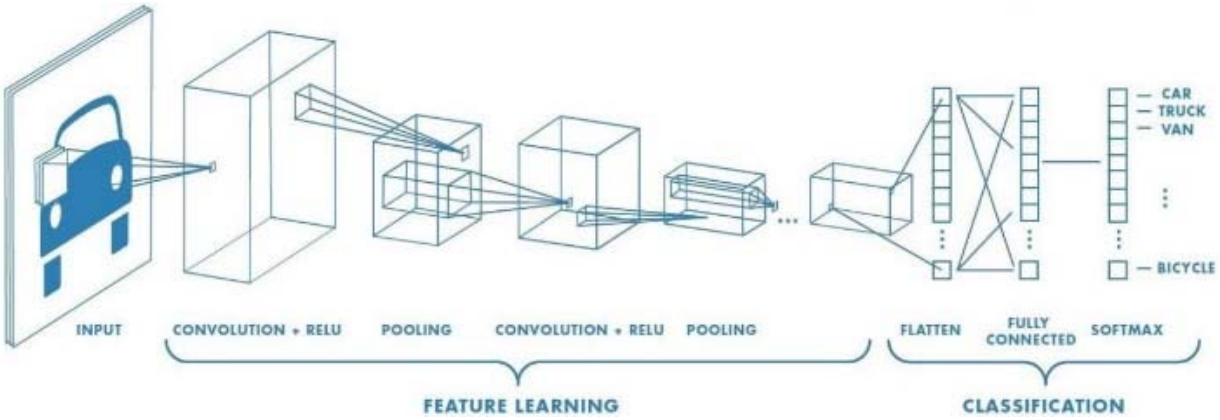

Рис. 6. Сверточная нейронная сеть – CNN

На конечном этапе после обработки последнего слоя изображения формируется embedding-вектор из чисел, который применяется в функциях классификации при обучении сети. CNN-сеть используется для распознавания лиц в биометрии. На ранних слоях алгоритм выучиваетуглы, светотени, линии, самые мелкие объекты. На срединных слоях получаются более «осмысленные» отдельные изображения: глаза, рот, нос. На последних – усредненныеизображения лиц людей.

Как и у других сетей, у CNN-сетей есть предобученные модели, в которых можно не обучать ранние слои, но необходимо обновить свертки на срединных слоях под задачи. Требуется гораздоменьше данных, чтобы модель привести к задаче.

Для решения некоторых задач кибербезопасности применяются комбинированные подходы, которые анализируют структурированные и неструктурированные данные в рамках одной задачи.

Например, выявление фишинговых сайтов. Крайне важно вовремя детектировать подобный сайт, чтобы отправить на разделегирование. Для этого построена система, которая использует несколько моделей. Для распознавания изображений, использовалась сверточная нейронная сеть. Сеть выявлять характерные паттерны обучали на примерах легитимного и мошеннических сайтов. Из NLP-моделей для анализа текста применялись рекуррентные сети. Информация о фишинговых сайтах собирается как сотрудниками компании, так и присылается клиентами. Данные аккумулируются, передаются в систему, где применяются алгоритмы, происходит скоринг. Сайты, у которых большая вероятность фишинга, отправляются аналитикам, которые, в случае подтверждения, передают их на разделегирование.

В системах противодействия мошенничеству также применяется набор моделей: real-time скоринг транзакций, гео-модели, графовые представления, embedding-векторы для текстов обращений клиентов о мошенничестве. После обработки текста строится кластеризация обращений, чтобы выявить новые схемы мошенничества.

При объединении моделей для анализа и обработки структурированных и неструктурированных данных получается лучший результат в решении задач. Чтобы применять ИИ- технологии необходимо иметь оцифрованные данные всевозможных процессов. Только на их основе можно строить модели машинного обучения.

Для обработки искусственным интеллектом структурированных данных используются кластеры с десятками серверов. Данные предварительно предобрабатываются, вычисляются признаки, чтобы сократить объемы данных и необходимой памяти для анализа. Для обучения моделей ИИ используется распределенный кластер или мощные серверы. Если говорить об учебных целях и небольших проектах, то для 32-64 Gb структурированных данных достаточно ПК с 32 Gb. Если памяти недостаточно, данные можно поделить на части. Для обучения небольших трансформеров достаточно одной видеокарты DX 20/80 или 30/60, 30/70, 38/100. Чем больше задача, тем большая инфраструктура необходима.

Для работы с библиотеками в ML чаще всего используется язык программирования Python. Также существует ряд библиотек по традиционным алгоритмам, которые написаны на языке R.

Заключение

В задачах кибербезопасности не используются специальные нейропроцессоры, только графические ускорители. Этапы исследования для построения графовой модели транзакций, которое проводилось в Сбербанке:

- ✓ Взяли граф клиентской активности за год, в котором присутствовали финансовые транзакции, взаимодействия с устройствами;
- ✓ Для графа построили embedding-векторы последнего слоя данных;
- ✓ Полученные векторы проверили перед использованием в реальных моделях. Стояла задача определить, смогли ли embedding-векторы уловить имеющуюся связь между вершинами графа;
- ✓ Выбрали по 1000 случайных клиентов из разных территориальных банков и отобразилина плоскости их близость между собой. Было выявлено, что граф отобразил географическую близость клиентов между собой. Значит, embedding-векторы вычислены верно;
- ✓ Данные экспортировали в систему противодействия мошенничеству. В режиме реального времени, когда осуществлялась транзакция, по ее участникам брали их embedding-векторы и вычисляли косинусную близость. Результаты вычислений учитывали для определения статуса транзакции [6], [7].

Литература

1. ИИ переопределил компьютеры https://www.technologyreview.com/2021/10/22/1037179/ai-reinventing-computers/

2. Applications for artificial intelligence in Department of Defense cyber missions https://blogs.microsoft.com/on-the-issues/2022/05/03/artificial-intelligence-department-of-defense-cyber-missions/

3. Магистерская программа "Искусственный интеллект в кибербезопасности https://cs.msu.ru/node/3732

4. Information Security Analysts https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

5. Cybersecurity Workforce Study https://www.isc2.org/News-and-Events/Press-Room/Posts/2021/10/26/ISC2-Cybersecurity-Workforce-Study-Sheds-New-Light-on-Global-Talent-Demand

6. *Kouliaridis Vasileios, Georgios Kambourakis.* A comprehensive survey on machine learning techniques for android malware detection // Information 12.5 (2021): 185.

7. *Zinatullin L.* Artificial Intelligence and Cybersecurity: Attacking and Defending. URL: https://www.tripwire.com/state-of-security /fea tured/artificial-intelligence-cybersecurity-attac king-defending/.

КОНТЕНТНО-ЗАВИСИМАЯ МОДЕЛЬ ОБЕСПЕЧЕНИЯ КАЧЕСТВА ОБРАБОТКИ СЕНСОРНЫХ ДАННЫХ В ICN СЕТЯХ

Боровская Яна Александровна,
ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики», аспирант кафедры сетей и систем связи, Самара, Россия
yana.borovskaya.98@mail.ru

Гребешков Александр Юрьевич,
ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики», профессор кафедры сетей и систем связи, доктор технических наук, Самара, Россия

Аннотация
Цель исследования состоит в совершенствовании мер по обеспечению качества обработки сенсорных данных, генерируемых разнородными устройствами IoT с учетом контента. Рассматриваются основные функциональный компоненты контент-зависимой модели качества обработки сенсорных данных в информационно-ориентированных сетях ICN.

Ключевые слова: *информационно-ориентированные сети, контент-зависимая модель, сенсорные данные, онтология, качество данных.*

Введение

С появлением Интернета вещей (Internet of Things, IoT) и беспроводных сенсорных сетей (Wireless Sensor Network, WSN) сенсорные устройства широко используются в производственной и непроизводственной сфере экономики, постоянно генерируя поток сенсорных данных и телеметрии. Эти данные передаются обрабатываются и сохраняются с учетом их содержания, что в совокупности формирует проблемно-ориентированный контент, где под контентом понимается семантически определяемый фрагмент больших данных, Big Data, сформированный посредством сбора характеристик физической среды или объекта (давление, температура, скорость и т.п.). Разнородность источников контента обуславливает актуальность задачи анализа содержания и качества сенсорных данных, формирующих контент, а также задачи поиска эффективных архитектурных решений хранения и передачи данных с минимальными задержками по времени при условии обеспечения актуальности статуса, когерентности и совместимости данных, в том числе для формирования обучающих последовательностей сенсорных данных (Data Set) для машинного обучения с обезличиванием данных, но при сохранении описания их содержания. В данной статье предлагается рассмотреть контент-зависимую модель обеспечения качества обработки данных с учетом возможностей информационно-ориентированных сетей (Information-Centric Network, ICN) [1] в качестве технической архитектуры для сбора, хранения и передачи контента, сформированного IoT-устройствами. Цель работы заключается в повышении эффективности контроля контентно-зависимой обработки сенсорных данных в информационно-ориентированных сетях ICN. Научная новизна работы заключается в предложенной системе и модели контроля качества сенсорных данных в ICN сетях.

Результаты исследований

В общем случае информация IoT рассматривается как отображение ситуации (сцены) физического мира с определенной степенью точности. Контентно-зависимая обработка сенсорных данных в информационно-ориентированных сетях ICN предполагает наличие семантического описание структуры обрабатываемой информации. Как показано на рисунке 1, такая контент-ориентированная модель представления информации в сети, которая является основой для ICN сетей, должна обеспечить своевременность обновления контента т.е. актуальность статуса данных, минимальные задержки по времени при передаче данных, а также совместимость и когерентность данных.

Рис. 1. Модель обработки сенсорных данных с применением ICN сети

Инструменты автоматизированного контроля качества контента позволяют обозначать/идентифицировать и исправлять обнаруженные ошибки данных, которые могут иметь разное происхождение. Ошибки в общем случае обусловлены несоответствием типов и содержания данных тем характеристикам реальных объектов или явлений, которые они описывают. Другой задачей инструментов управления данными в части контента является устранение причин возникающих ошибок путем их распознавания и изменения семантического описания. Управление качеством контента предусматривает текущий контроль качества сенсорных данных и проверку показателей качества данных.

В известных стандартах ISO 8000 и в руководстве «Свод знаний по управлению данными» (DAMA DMBOK2) описаны процессы текущего контроля качества данных, которые состоят в создании правил контроля качества данных бизнес-уровня, проверки соответствия данных этим правилам, определении проблем с качеством данных и создание отчетов о качестве данных. Эту схему в полной мере можно применить при создании контентно-зависимой модели обработки данных в ICN сетях.

В документе ГОСТ Р ИСО 8000-100-2019 [2] определяется таксономия данных, как показано на рисунке 2. Под качеством данных согласно ГОСТ Р ИСО 8000-2-2019 здесь и далее [3, 4] понимается степень, с которой набор характеристик, присущих данным, отвечает предъявляемым требованиям достоверности контента.

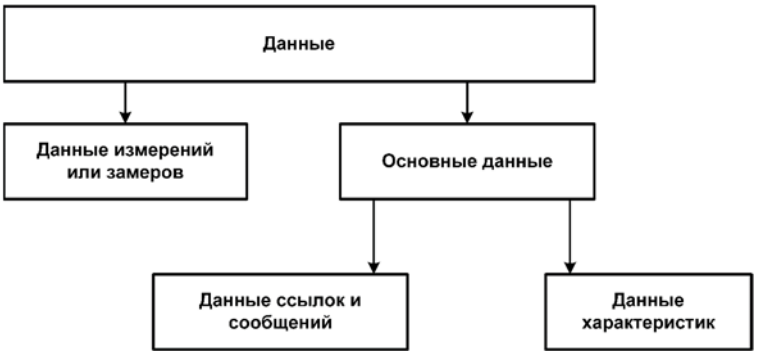

Рис. 2. Таксономия данных, формирующих контент

С помощью основных данных происходит описание значимых и основополагающих объектов IoT. В целом основные данные представляют собой данные, хранящиеся на цифровой платформе организации/предприятия и являющиеся основными и наиболее важными информационными активами организации/предприятия.

Примерами основных данных являются:

1. Данные, касающиеся собственника, в том числе относящиеся к объекту эксплуатации/автоматизации IoT.

2. Данные, касающиеся отдельных фрагментов контента, сенсорных сетей, систем IoT, с помощью которых описываются материальные предметы, отслеживаемые, сетей ICN.

3. Данные, касающиеся месторасположения или размещения источников контента, которые позволяют идентифицировать объект по его расположению на местности, включая координаты в заданной системе либо путем привязки с указанием принятых географических обозначений.

Согласно положениям ГОСТ Р ИСО 8000-2-2019 [4] и с учетом требований ГОСТ Р ИСО 8000-102-2011 [5] для анализа качества данных в контентно-ориентированной модели, применяется структура, представленная на рисунке 3.

Рис. 3. Структура основных данных контента согласно ГОСТ Р ИСО 8000-100-2019

Для обеспечения семантического единства, основные данные описываются (нормализуются) с помощью т.н. «концептов» в словаре данных, где концепт есть смысловая единица лексикона проблемной области, к примеру термин, или объект онтологии с описанием его свойств в виде атрибутов. Словарь данных представляет собой совокупность всех концептов, которым можно сопоставить объекты внешнего мира. Вводимые в словарь проблемно-ориентированные данные представляют собой описание в виде типа объекта, с указанием точного идентификатор, концепта и необходимых атрибутов концепта. В качестве концепта может использоваться термин, описывающий свойство физического мира. В свою очередь, спецификация сенсорных данных включает правила описания объектов и контента, принадлежащих к определенному классу, с применением терминов словаря. Основные данные соответствуют спецификации данных. Кроме того, спецификация данных соответствует установленной терминологию для концептов словаря. Формальный синтаксис представляет собой спецификацию правильных предложений формального языка с применением формальной грамматики для описания объекта на цифровой платформе, что важно, к примеру для поиска данных и систем распознавания речи. Основные данные соответствуют формальному синтаксису. Основные данные, спецификации данных контента и словари данных применяют идентификаторы согласно принятой схеме идентификации.

В руководстве DAMA DMBOK [6] указано, что схема контроля качества данных, в том числе формирующих контент, должна также предусматривать наличие качественной организации данных и использование инструментов контроля качества данных. Усилия организации/предприятия по управлению качеством данных, формирующих контент, должны быть сосредоточены в первую очередь на наиболее важных данных организации. Приоритетность данных контента может быть определена на основе таких факторов, как нормативные требования, финансовая и бизнес-ценность. Усилия по повышению качества данных, формирующих контент, начинаются с основных данных, которые по определению являются самыми важными в любой организации.

Согласно ГОСТ Р 56215-2014, часть 150 [7], процесс управления качеством данных состоит из следующих процедур:

– подготовка правил для оценки качества данных, которые предусматривают процедуры для оценки показателей качества;

– применение процедур для оценки качества данных, прежде всего оценку целевых данных в их совокупности и взаимозависимости по факту появления в системе в автоматическом или в автоматизированном режиме.

Для контроля качества сенсорных данных обеспечивается функционирование процессов анализа

качества контента верхнего, среднего и низшего (технического) уровня. Процесс управления структурой данных, формирующих контент, относится к процессам высокого уровня и основан на общепринятых моделях, например на онтологии SSN.

Процессы конструирования (формирования) сенсорных данных, подготовка критериев качества и анализ причины ошибок относятся к процессам среднего уровня. Для контроля, координации обработки данных и обеспечения действия технического персонала. Процесс конструирования данных помогает обеспечить качество операций над данными путем усовершенствования структуры данных. Процесс подготовки критериев качества обеспечивает методологию оценки качества данных.

Процессы, непосредственно осуществляемые техническим персоналом либо машинными средствами обработки, относятся к процессам низшего уровня и включают обработку данных, непосредственную оценка качества данных и исправление ошибок. Сначала выполняется обработка данных, прежде всего поиск, обновление, преобразование в соответствии с имеющимися правилами. Процесс оценки качества данных осуществляется либо в режиме реального времени, либо периодически, в отложенном времени по выборке. В случае обнаружения ошибки её исправление производится в соответствии с доступным способом исправления, например источник данных может быть отнесен к другому классу.

Проверка или оценка сенсорных данных предусматривает своевременное обнаружение ошибок в прикладных системах IoT или в процессах использования данных, при которых могут возникнуть затруднения у конечного пользователя, например при обучении промышленного интернета IIoT. В связи с этим проверку качества данных необходимо проводить систематически.

Наиболее состоятельным является подход, когда показатели качества данных проверяются сразу же после процесса получения данных в точках сбора сведений методами граничных вычислений. Время на проверку показателей качества может меняться в зависимости от свойств и особенностей метрик качества. Переход к анализу качества данных «на лету», в реальном времени и непосредственно в процессе замеров/измерений представляет собой сложную самостоятельную задачу, решение которой требует дополнительных разработок в области граничных вычислений в сетях ICN.

Основными критериями качества обработки сенсорных данных для ICN сетей являются:

- полнота сенсорных данных;
- актуальность данных по месту и времени сбора;
- точность сенсорных данных;
- согласованность сенсорных данных;
- семантическое единство данных.

Полнота данных в рамках единого информационного пространства обращения сенсорных данных означает требуемая степень соответствия данных совокупности установленных характеристик информационных объектов. Для обеспечения согласованности данных в рамках единого информационного пространства ICN сетей требуется:

- наличие единой методики типизации (классификации) информационных объектов, включающей задание семантического описания (соответствующего термина и определения) для каждого типа объектов;
- наличие единого способа идентификации информационных объектов, обеспечивающего единственность информационного объекта, описывающего каждый объект или явление реального мира, либо возможность однозначного связывания между собой информационных объектов, соответствующих одному объекту или явлению реального мира.

Процесс обработки ошибок согласованности данных, найденных благодаря процессу проверки показателей качества данных, предусматривает анализ причины возникновения каждой ошибки во всех прикладных системах–источниках информации. Далее для проверки качества данных предлагается применять функциональную схема контроля качества данных в ICN сетях, представленную на рисунке 4.

Уровень 1 есть верхний уровень контроля качества данных представляет собой сведения об используемых источниках данных и генерируемых ими информационных потоках. Для контроля качества данных на рис. 4. используются сведения из информационных систем, например систем промышленного интернета вещей, в той мере полноты и достоверности, в которой сведения были предоставлены для проведения контроля и анализа.

Уровень 2 контроля качества данных включает контроль достаточности классов объектов для описания информации, получаемой из источников на рисунке 2, где класс представляет собой описание

структуры объектов одного вида, а под объектом понимается физическая или абстрактная вещь в рамках рассматриваемой предметной области.

Рис. 4. Уровни контроля качества в контент-зависимой модели

Уровень 3 контроля качества данных включает контроль данных характеристик объектов и контроль значений свойств объектов. Данные характеристик предусматривают описание объекта предметной области в соответствии с набором допустимых свойств для объектов классов, к которым принадлежит объект, и совокупностью конкретных значений свойств этого объекта.

Для оценки качества данных могут быть введены метрики, позволяющие дать количественную оценку качества данных на предприятии или в организации. Имеется пример онтологического фреймворка для формализации таких оценок [8]. Разработанный словарь качества данных DQV (Data Quality Vocabulary) представляет модель метаданных для отображения качества данных. DQV расширяет словарь каталога данных (Data Catalog Vocabulary (DCAT) с помощью добавления свойств и классов, с помощью которых можно описывать качество множеств данных и их распределений с применением различных типов заявлений (положений) о качестве данных, которые включают «Аннотации по качеству» (Quality Annotations), «Стандарты, политики в области качества» (Quality Policies), «Измерения качества» (Quality Measurements) данных и обеспечение качества источников (происхождение) данных (Quality Provenance). При этом в аннотации по качеству данных включают рейтинги источников данных, сертификаты качества и реакцию пользователей в части качества, которые можно увязать с данными.

Для определения качества сенсорных данных используются параметры качества, систематически организованные в группы, называемые «категориями качества». Например, категории могут быть определены в соответствии с рассматриваемым типом информации, например, контентно-зависимый тип информации (Content-Based) зависит от собственно информационного содержания; контекстно-зависимый тип информации (Context-Based) зависит от контекста, в рамках которого была запрошена информация; рейтинг–зависимый тип информации определяется на основе рейтинга данных или рейтинг указывается поставщиком информации. В общем случае данные также можно определить и описать по другим критериям, что может привести к появлению сложно–составной иерархии в зависимости от того, насколько идея, определяющая качество оценки данных, пригодна к использованию. Имеется подтверждение наличия нескольких более специализированных онтологий для контроля качества данных, которые основаны на семантической сети (Semantic Web) и на открытых словарях данных [9].

Существует класс систем, которые можно рассматривать как основанные на онтологии схемы управления качеством данных (Ontology-Based Data Quality management frameworks) для информационных систем. Среди них необходимо выделить решение, основанное на онтологиях, в области повышения качества данных, названное Context Interchange (COIN).

Разработка COIN направлена на предотвращение проблем с качеством данных, связанных с неверным толкованием смысла терминов, для чего была разработана технология, позволяющая отчасти преодолеть семантическую неоднородность базовых данных источники. С помощью COIN упрощается взаимодействие между пользователями и разнородными информационными системами за счет предоставления доступ к знаниям в виде определения терминов, что позволяет преодолевать смысловые различия.

Также стоит отметить онтологию разрешения семантических конфликтов (Semantic Conflict Resolution Ontology, SCROL), которая позиционируется как независимая от предметной области онтология для обнаружения и разрешения семантических различий на уровень экземпляра данных и схемы

при интеграции данных из разнородных источников данных. На уровне экземпляра данных онтология может использоваться для хранения информации для решения задач неоднородности описания данных, таких как разные единицы измерения или разные уровни точности измерения.

Также имеет место и иной подход с помощью схемы SPIN (SPARQL Inferencing) для обработки требования к данным посредством RDF (Resource Description Framework) т.е. с помощью модели данных, используемой для представления ресурсов Semantic Web. SPIN представляет собой словарь, который может представлять запросы SPARQL в RDF. Исходя из требований к данным, отчеты/процедуры по контролю качества данных могут идентифицировать экземпляры с нарушениями требований, которые к ним предъявляются. Более того, сформулированные требования могут использоваться для проверки данных во время ввода данных.

Ожидаемым результатом исследования является создание контено-зависимой модели для ICN сетей в предметной области интернета вещей. Модель позволит сформировать единое и непротиворечивое описание сенсорных данных для поиска и использования на узлах ICN с использованием предметной онтологии и методологии семантической кэш-памяти. В модели правила увязываются с природой и характером контента, источниками и способами получения, представления данных, организационно-техническими мероприятиями по работе с данными и методами интерпретации полученной информации. Предлагаемый подход применительно к задачам управления последствиями отказов описан патентом [10].

Заключение

Таким образом, в статье предлагается контент-зависимая модель обработки сенсорных данных с применением свойств информационно-ориентированной сети ICN. Такая модель направлена прежде всего на анализ информационно-смысловой составляющей сенсорных данных от гетерогенных источников информации. Приводится таксономия данных, формирующих контент. Отмечается, что для контроля качества сенсорных данных могут быть введены уровни, позволяющие последовательно контролировать качество сенсорных данных, в частности для применения в качестве обучающих последовательностей в методах машинного обучения, в том числе непосредственно в ICN сетях. Дальнейшие исследования будут направлены на разработку метрик качества обработки сенсорных данных с учетом «времени жизни» или статуса актуальности контента, т.е. с учетом того на сколько часто необходимо обновлять информацию от сенсорных устройств, чтобы не перегружать систему ICN.

Литература

1. *Гребешков А.Ю., Боровская Я.А*. Построение информационно-ориентированных сетей 5G-ICN // Вестник связи. 2021. № 11. С. 13-18.

2. ГОСТ Р ИСО 8000-100-2019. Качество данных. Часть 100. Основные данные. Обмен данными характеристик. Обзор. Введ. с 1.05.2020. М.: Стандартинформ, 2019. 20 с.

3. ГОСТ Р ИСО 8000-100-2019. Качество данных. Часть 100. Основные данные. Обмен данными характеристик. Обзор. М.: Стандартинформ, 2019. 15 с.

4. ГОСТ Р ИСО 8000-2-2019. Качество данных. Часть 2. Словарь. М.: Стандартинформ, 2019. 12 с.

5. ГОСТ Р ИСО 8000-102-2011. Качество данных. Часть 102. Основные данные. Обмен данными характеристик. Словарь. Введ. 1.07.2012. Режим доступа URL: http://docs.cntd.ru/document/1200088546 (дата обращения 17.11.2020)

6. DAMA-DMBOOK. Data Management body of knowledge. 2nd edition/ Edited by Henderson, D., Earley S. Technics Publications. Basking Ridge, New Jersey, USA. 2017. 624 p.

7. ГОСТ Р 56215-2014/ISO/TS 8000-150:2011. Качество данных. Основные данные. Структура управления качеством. Часть 150. М.: Стандартинформ, 2014. – 20с.

8. *Albertoni R., Isaac A*. Introducing the data quality vocabulary (DQV). Semantic Web journal. 2021. Iss. 1. Vol. 12, P. 81-97.

9. *Fürber C*. Data quality management with semantic tecnologies. Springer Fachmedien Wiesbaden, Germany, 2016. 205 p.

10. *Гребешков А.Ю., Кузнецов Я.М., Пашин С.С*. Способ предсказания выхода их строя оборудования сенсорных и беспроводных сетей на основе онтологии и с применением методов машинного обучения: пат. 2786934 Российская Федерация: МПК H04L 43/04; патентообладатель Поволжский государственный университет телекоммуникаций и информатики. № 2021138728; заявл. 24.12.2021; опубл. 26.12.2022, Бюл. № 36.

БУМ НЕЙРОСЕТЕЙ И ИХ МЕСТО В БИЗНЕСЕ

Исаев Осман Абдурахманович,
Московский технический университет связи и информатики, магистрант, Москва, Россия
osmanisaev190501@mail.ru

Аннотация
Статья посвящена анализу использования решений на основе нейросетей в бизнесе. Рассмотрены вопросы опыта использования искусственного интеллекта в бизнесе, проблемы внедрения и перспективы развития. На основе вышеперечисленного рассмотрены возможности и перспективы замены человеческих ресурсов автоматизированными решениями на основе нейросетей.

Ключевые слова: *Нейросети, искусственный интеллект в бизнесе, роверы, беспилотный транспорт, промышленное производство, ChatGPT, Midjorney, Github Copilot, нейросети лишают работы*

Введение

Использование нейросетей с каждым днем получает все более широкое распространение. Обычно это происходит на стыке науки и бизнеса, ведь, по сути, уникальные бизнес-решения создаются впервые и их нельзя не назвать научными. Использование технологий, работающих на основе нейросетей настолько незаметно проникло в повседневную жизнь человека, что порой люди не могут представить себе возможность существования при отсутствии подобных решений. Это касается очень многих отраслей современной экономики [13, 14, 16], особенно в условиях перехода к импортозамещению. Голосовые ассистенты, поисковые системы и переводчики, рекомендательные системы – лишь некоторые из примеров, заполонивших нашу жизнь. Подобные решения, конечно же, имеют выгоду и для бизнеса, а качественный софт привлекает клиентов и увеличивает конверсию.

Самыми современными технологиями, которые начинают набирать популярность, являются ChatGPT и Midjorney. Они представляют собой публично доступные решения на основе нейросетей. Уже набралось достаточное количество отзывов пользователей, но до конца неясными остаются вопросы о пределе их возможностей и широты применения в частном использовании, научной и бизнес-среде.

Роль нейросетей в бизнесе

В качестве примеров, получивших широкое распространение можно привести решения Яндекса. В свое время неожиданностью стало появление голосового ассистента – Алисы. Также уникальной технологией, которая была представлена летом 2022 года стала нейромузыка. Медиасервис Яндекс.Музыка представил пользователям технологию, позволяющую слушать музыку, сгенерированную на основе нейросетии и, судя по огласке и отзывам, очень успешно с этим справилась.

Подобные решения появляются регулярно, что создает конкуренцию на рынке и в итоге улучшает качество жизни пользователей. Ассоциация электронных коммуникаций совместно с Высшей школой экономики провела исследование, посвященное использованию искусственного интеллекта [1]. В рамках этого исследования рассматривалось использование искусственного интеллекта компаниями России из различных областей, основные проблемы, с которыми сталкиваются компании и общие тенденции к росту в данной области. Результаты показали, что Россия относится к числу стран с высоким потенциалом внедрения искусственного интеллекта, а лидерами по внедрению являются ритейл, банки, промышленное производство и телекоммуникации. Взрывной рост же был обещан в двух областях: беспилотном транспорте и робототехнике. Столь стремительное развитие порождает дискуссии о возможной замене некоторых профессий [15], ведь логично, что бизнесу не нужны затраты на людей, когда деятельность можно автоматизировать. Рассмотрим этот вопросы через призму наиболее перспективных областей в отдельности.

Беспилотный транспорт

Беспилотный транспорт является одной из наиболее перспективных областей применения искусственного интеллекта. Одним из первых, кто начал массово поставлять софт с автопилотом стала компания Tesla. Казалось бы, с широким распространением автопилотов на автомобилях потребность в

управлении человеком пропадет. Это также могло бы дополнительно решить вопрос логистики, но использование технологии содержит в себе ряд проблем.

1. Плохая погода. Беспилотные автомобили оснащены камерами с искусственным интеллектом, которые помогают ориентироваться на улицах, идентифицируя объекты, дорожные знаки и людей. Однако проблема возникает зимой, когда камера просто не видит разметки на дорогах, что делает беспилотное вождение очень опасным. Решения данной проблемы до сих пор не удалось найти, поэтому многие испытания проводятся в странах с теплым климатом, или в любую погоду, когда на земле не лежит снег. В настоящее время инженеры работают над усовершенствованием лазерных датчиков с различной длиной волны, которые пытаются заставить видеть сквозь снег. Кроме того, разрабатывается и дополнительное программное обеспечение, которое позволит алгоритмам искусственного интеллекта отличать реальную разметку и препятствия от осадков.

2. Дорожная разметка. Проблема дорожной разметки заключается в том, что он может отличаться на дороге в зависимости от региона. Например, на одном перекрестке размечены широкие линии, которые определяют, где машины должны останавливаться перед перекрестком, а перед другим перекрестком эти линии могут быть затерты. В таком случае автомобиль не сможет распознать необходимость остановки и это может привести к аварии.

Также бывают случаи, когда здания расположены очень близко к дороге, и автомобиль не может распознать другие транспортные средства, которые едут справа и слева навстречу к перекрестку, что тоже может привести к аварийной ситуации. Поскольку существует множество типов перекрестков, может быть очень трудно понять, что делать в каждом конкретном случае. А на многих улицах не бывает даже бордюров, которые помогли бы определить ширину полосы движения. Решение этой проблемы остается одной из главных нерешенных задач для инженеров по сей день.

3. Повороты. Правила дорожного движения в ряде случаев разрешают поворачивать налево прямо перед встречным транспортом (например, если ехать по главной дороге, которая уходит налево на перекрестке), но даже людям бывает порой непросто принимать такие решения. Поэтому поворачивать без наличия на перекрестке светофора с разрешающей зеленой стрелкой алгоритмам машинного обучения по-прежнему очень сложно.

4. Взаимодействие с живыми водителями и пешеходами на дорогах. Когда человек самостоятельно управляет автомобилем, то часто можно заметить водителей, нарушающих правила дорожного движения. Человек, как правило, может находить способы обходить опасные ситуации, но автомобилям с автопилотом бывает трудно принимать подобные решения. И это, наверное, одна из самых сложных проблем, которую инженерам придется решить, если прогрессивное сообщество хочет увидеть беспилотные автомобили на дорогах в ближайшей перспективе. В решении данной проблемы немало усилий приложил Яндекс. В рамках тестирования автопилота в Иннополисе автомобиль научился распознавать мелких животных, а тестирование в Израиле помогло собрать данные о поведении мототранспорта.

Рис. 1. Беспилотный автомобиль Яндекса

Кроме массового передвижения на беспилотных автомобилях, еще одной похожей глобальной проблемой человечества является логистика. Одной из наиболее продвинутых компаний в области логистики является Amazon.

Начиная с 2021 года компания использует для фур, обеспечивающих магистральные перевозки, систему автоматизированного управления. Большим опытом логистики более меньшего масштаба обладает Яндекс, внедривший доставку роботами. Преимуществом использования роботов является их непрерывность работы, тогда как человеческие ресурсы нуждаются во сне и отдыхе. Экономические издержки и преимущества для бизнеса пока остаются не до конца ясными, так как технология достаточно новая, а для исследований необходимо больше времени, однако доставка роботами в сравнении с курьерской доставкой не отличается ценой, на основе чего можно сделать вывод о экономической выгоде данного метода доставки. В то же время этот способ логистики имеет проблемы, присущие любому беспилотному транспорту, которые были описаны раннее [3].

Рис. 2. Робот курьерской доставки Яндекса

В столь большом разнообразии и стремительном развитии может показаться, что технологии скоро вытеснят людей в логистике, ведь иначе получается, что одна половина человечества должна обеспечивать доставку для другой. На самом деле проблема логистики в том, что спрос с каждым годом увеличивается, а покрыть его становится все сложнее, поэтому беспилотный транспорт призван снять определенную нагрузку в данной сфере [4]. Что же касается логистики магистральных перевозок и беспилотного автотранспорта, то эти области содержат еще достаточное количество нерешенных технических проблем, но даже если удастся их решить, то без массового использования беспилотного транспорта и возможности делиться данными между автомобилями не получится достичь должного уровня безопасности, т.к. достаточно сложно предсказать маневры автомобиля, управляемого человеком. Из-за того, что данный вопрос содержит в себе вопросы безопасности, наибольшей проблемой массового применения таких технологий является законодательное ограничение. Пока еще большинство стран не готовы к применению беспилотных технологий на дорогах, так как в случае аварийной ситуации нужно определить ответственное лицо. Поэтому, можно сделать вывод, что несмотря на большие тенденции к широкому применению, беспилотный транспорт и логистика, призванные сэкономить траты бизнеса, не способны в ближайшие годы вытеснить человека.

Промышленное производство. Одной из ключевых сфер, ожидающих взрывной рост использования искусственного интеллекта является промышленность. Согласно оценкам McKinsey, использование решений на основе нейросетей в промышленности может привести к ежегодным доходам в размере трех миллионов долларов. Наибольший рост ожидается в автомобилестроении и электронике, а максимальный эффект по отношению к выручке, согласно прогнозам, будет в секторе высоких технологий [5]. Росту подобной автоматизации промышленного производства также способствовала пандемия ковида. Такая ситуация, например, наблюдалась в Сингапуре из-за оттока иностранцев и в связи с карантинными мерами.

Действительно, прогнозы McKinsey оказались верными, уже в мае 2022 года американское издание The Wall Street Journal опубликовало статью со ссылкой на отчет ассоциации развития автоматизации США, в которой утверждается, что американская промышленность увеличила заказы на промышленных роботов в первом квартале 2022 года на 40% по сравнению с тем же периодом прошлого года. В США использование роботов в производстве было традиционно меньше, чем в Южной Корее или

Германии, и чаще всего использовалось в производстве тяжелой и рутинной работы. В 2022 году был замечен рост использования искусственного интеллекта для автоматизации таких сфер бизнеса, как металлургия, производство пластмассы, лекарств и товаров народного потребления. Специалисты объясняют подобный рост использования технологий нехваткой рабочей силы и квалифицированных специалистов. С учетом таких тенденций, наиболее выгодным для бизнеса является автоматизация производства. Это позволяет уменьшить время производства и повысить качество разрабатываемой продукции [6]. Но в то же время автоматизированное производство нуждается в контроле со стороны человека. Со временем необходимо бывает анализировать износ и заниматься техническим обслуживанием оборудования, контролем качества и управлять складскими запасами. Подобным анализом все чаще занимается специальное ПО с использованием искусственного интеллекта, однако при всех возможностях автоматизации не исключаются возможные сбои, что не позволяет полностью заменить присутствия людей на производстве. Тем не менее, это позволяет уменьшить потребность в человеческих ресурсах в значительной степени.

Рис. 3. Автоматизированная конвейерная линия производства автомобилей

Подобная автоматизация позволяет нарастить производство не только из-за того, что роботам необходимо меньше времени по сравнению с человеком, но и из-за возможности более непрерывного производства. Человек ограничен физически в своих ресурсах и не способен работать 24 часа в сутки, как, например, автоматизированная сборочная линия. Так, с 2017 года по 2020 год медианная цена одного из самых популярных промышленных роботов – автоматического робота-манипулятора упала дважды и составила 22.6 тысяч долларов, тогда как средняя зарплата инженера производства в США составляет 80 тысяч долларов [7].

Таким образом, стоимость оборудования и его обслуживание в перспективе обходится бизнесу значительно дешевле, что и склоняет к решению в сторону автоматизации. Исходя из вышеперечисленных фактов и тенденций к увеличению автоматизации промышленного производства, можно сделать вывод, что в данной области применение решений на основе нейросетей способно вытеснить человека.

Разработка ПО, языковые модели и дизайн

Летом 2022 года компания Microsoft представила Github Copilot – инструмент, основанный на нейронной сети, который помогает разработчикам писать код. Появление данной технологии породило жаркие дискуссии о том, способен ли будет искусственный интеллект заменить разработчиков. Copilot способен выполнять три основные функции:

- Написать код, проанализировав комментарии;
- Дописать комментарии к готовому коду;
- Определить типовые алгоритмы и дописать их за разработчика.

Использовать софт можно при помощи интеграции с Github-аккаунтом. Хоть Copilot и представляется средством, способным оказать помощь разработчику, возникает вопрос: «А не способен ли он со временем заменить программистов»? Собрав статистические данные, разработчики сервиса обнаружили, что пользователи, использующие Copilot принимают в среднем 26% генерируемых подсказок, что говорит о неспособности на данный момент заменить разработчиков. Кроме того, проводились исследования безопасности генерируемого кода. В декабре 2021 года специалисты инженерной школы Нью-Йоркского университета обнаружили, что Github Copilot в 40% случаев генерирует код, содержащий уязвимости и ошибки [8]. Ровно спустя год аналогичное исследование было проведено группой исследователей Стэндфордского университета.

Согласно результатам, участники, которые использовали ассистент для написания кода, смогли предоставить корректный и безопасный код в 67% случаев, тогда как группа, которая не пользовалась ассистентом, смогла предоставить безопасный и корректный код в 79% случаев [9]. Можно сделать вывод, что нейросеть учится и улучшает свои показатели, но тем не менее, она не способна заменить разработчиков. Ее использование способно местами облегчить работу программиста, однако это несет в себе вопросы безопасности и корректности кода. Результат, предоставленный нейросетью все равно нуждается в проверке, а иногда и в более тщательной, так как разработчик, предоставивший сгенерированное решение, несет ответственность перед командой разработки и компанией. Microsoft использует для обучения нейросети репозитории Github и предполагается, что качество работы будет улучшаться.

Еще одной новостью, которая взбудоражила умы является появление 30 ноября 2022 года ChatGPT – чат-бота с использованием искусственного интеллекта, который отвечает на вопросы и позволяет вести диалог на естественных языках. В отличие от большинства имеющихся решений, в том числе голосовых ассистентов, чат-бот умеет работать в формате диалога и может отвечать, улавливая контекст на основе истории ранних сообщений. Используемая нейросеть обучалась с помощью метода обучения с учителем и обучения с подкреплением. За короткое время публично доступного решения уже появилось очень много статей об использовании данной технологии. Она способна составлять текст на практически любую тему и таких примеров предостаточное количество в интернете. Нейросеть по сути уникальна и удивляет пользователей своими результатами по сей день. К примеру, недавно нейросеть смогла успешно сдать MBA-экзамен в одну из самых известных бизнас-школ мира – Уортон [10]. Технология по сей день не обуздана до конца и продолжает совершенствоваться. Однако одно стало точно ясно — она поможет усовершенствовать работу поисковиков и голосовых ассистентов, которые используются сегодня повсеместно. Кроме того, ChatGPT способен составлять письма, генерировать статьи, решать задачи и даже писать код.

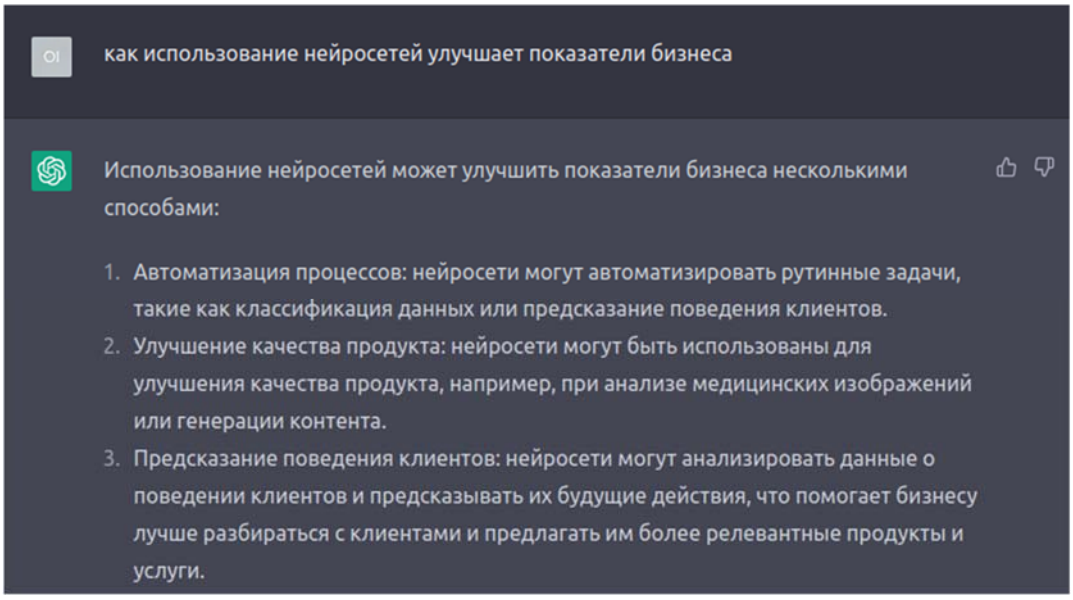

Рис. 4. Пример ответа на вопрос от ChatGPT

Подобное решение способно по-настоящему заменить профессии, требующие работы с текстом. Посмотрим, что говорит сам ChatGPT на этот счет. Задав вопрос: «Какие профессии заменит ChatGPT?», получаем следующий овтет: «ChatGPT является технологией глубокого обучения, которая может быть использована для автоматизации и облегчения работы в различных областях. Одним из применений является генерация текста, так что возможно, что технология может заменить некоторые профессии, связанные с написанием, например, копирайтер, переводчик или журналист. Но она не может заменить такие профессии как дизайнер, инженер или медик и т.д. Так же она не может заменить такие качества как творчество, эмпатия и интуиция, которые являются основой работы многих профессий». Вероятно, что ChatGPT, как и Github Copilot после периода тестирования и более качественного обучения станет платной, но пока технология остается публично доступной для любого пользователя.

Еще одним примером является нейросеть Midjorney, позволяющая генерировать картинки на основе текстовых запросов. В середине июля 2022 года она вышла на фазу бета-тестирования и стала доступна пользователям по всему миру. Работу нейросети обеспечивают два технологических прорыва, произошедших относительно недавно: умение понимать человеческую речь и генерировать образы. Для этого Midjorney обучалась выстраивать соответствия между текстовыми описаниями и визуальными образами. Результаты такого обучения позволяют решать различные кросс-модальные задачи — генерацию картинок по текстовому описанию, генерацию текстовых описаний по картинкам, дорисовку частей изображения, и так далее, говорит руководитель управления экспериментальных систем машинного обучения SberDevices Сергей Марков [11].

Midjourney не является первой нейросетью, имеющей подобные свойства. Раннее подобным уже удивляла нейросеть DALL-E от OpenAI, которая была разработана благодаря гранту от Microsoft. Еще успешными примерами являются Imagen от Google и нейросеть Kandinsky от Сбера. Разработчики нейросети Kandinsky заявили, что процесс ее обучения стал самой большой вычислительной задачей в России [12]. У таких решений на основе нейросетей, как Midjorney или Kandinsky находится достаточно областей применения. К примеру, данная технология способна генерировать NFT, создавать художественные произведения и участвовать в разработке дизайна. Кроме того, эти нейросети способны участвовать в разработке дизайнов интерьера, персонажей в среде геймдева, генерации эмодзи, стикеров, стиле одежды. Подобные решения пока могут лишь в малой степени влиять на рынки профессий, связанных с творческой составляющей, скорей они призваны помочь в этом деле, однако можно сделать вывод, что с улучшением качества работы таких нейросетей, их воздействие на трудовой рынок будет нарастать.

Заключение

С ростом возможностей нейросетей, возрастает их роль в жизни человека. Прорывные решения, разрабатываемые на сегодняшний день, дают новый толчок технологическому прогрессу и позволяют искать новые пути развития человечества. Технологии с использованием нейросетей позволяют сэкономить огромное число человеческих ресурсов, что также положительно сказывается на развитии человечества. В основном использование подобных решений нашло себя в бизнесе или научной среде. Исследования показывают, что нейросети очень быстро находят применение во многих профессиях, что беспокоит людей, ведь бизнесу выгоднее приобрести автоматизированные решения, нежели тратить ресурсы на содержание сотрудников. Такие тенденции имеют место быть, однако в большинстве случаев нейросети не способы полностью заменить деятельность человека, а призваны помочь ему в этом. Нет сомнений, что через некоторое время благодаря технологическому прогрессу изживут себя множество профессий, однако эта экономя человеческих ресурсов позволяет перенаправить их на другие области, в которых есть потребность, что позволит ускорить развитие человечества и идти дальше к освоению еще не известных областей.

Литература

1. Цифровая экономика от теории к практике: как российский бизнес использует искусственный интеллект // RB.RU. URL: https://media.rbcdn.ru/media/reports/5.pdf (дата обращения: 26.01.2023)

2. О проблемах беспилотных автомобилей. URL: https://habr.com/ru/company/first/blog/681956/ (дата обращения: 27.01.2023)

3. *Воробьев П.* Будущее уже наступило: как мы запустили доставку роботами в России и США // Доклад Яндекса. 27 декабря 2021. URL: https://www.youtube.com/watch?v=YzSRhRNqMNQ&t=2132s (дата обращения: 28.01.2023)

4. *Худавердян Т.* YaC 2021: Чем живет Яндекс // Ежегодная конференция Яндекса. 8 декабря 2021. URL: https://www.youtube.com/watch?v=ph8T4fmP-ag&t=543s (дата обращения: 28.01.2023)

5. Notes from the AI frontier: Applications and value of deep learning // McKinsey & Cimpany. URL: https://www.mckinsey.com/featured-insights/artificial-intelligence/notes-from-the-ai-frontier-applications-and-value-of-deep-learning (дата обращения: 28.01.2023)

6. *Bob Tita B. T.* Robots Pick Up More Work at Busy Factories // The Wall Street Journal : электронный журнал. – URL: https://www.wsj.com/articles/robots-pick-up-more-work-at-busy-factories-11653822002. Дата публикации: 29.05.2022.

7. *Eugene Demaitre E.D*. Robot Prices Drop as AI Investments, Ethics Worries Increase, Finds Stanford HAI AI Index 2022 Report // Robotics 24/7 : электронный журнал. URL: https://www.robotics247.com/article/robot_prices_drop_ai_investments_ethics_worries_increase_finds_stanford_hai_ai_index_2022_report. Дата публикации: 16.03.2022.

8. *Pearce H., Ahmad B., Tan B., Dolan-Gavitt B., Karri R.* Asleep at the Keyboard? Assessing the Security of GitHub Copilot's Code Contributions // 43rd IEEE Symposium on Security and Privacy. Institute of Electrical and Electronics Engineers Inc., 2022. С. 754-768.

9. Do Users Write More Insecure Code with AI Assistants? // arXiv : сайт. URL: https://arxiv.org/pdf/2211.03622.pdf (дата обращения: 28.01.2023)

10. *Terwiesch C.T*. Would Chat GPT Get a Wharton MBA? New White Paper By Christian Terwiesch // Mack Institute News, White Papers. 2023. № 01. С. 1-26. 17 января. URL: https://mackinstitute.wharton.upenn.edu/wp-content/uploads/2023/01/Christian-Terwiesch-Chat-GTP-1.24.pdf (дата обращения: 28.01.2023).

11. *Пешкова П.Н*. Хайп мирового масштаба от исследователя NASA. Кто придумал нейросеть Midjourney и отберет ли она работу у живых художников и дизайнеров // Inc. Russia : электронный журнал. URL: https://incrussia.ru/understand/midjourney-creator/. Дата публикации: 8.08.2022.

12. ruDALL-E: генерируем изображения по текстовому описанию, или Самый большой вычислительный проект в России. URL: https://habr.com/ru/company/sberbank/blog/586926/ (дата обращения: 28.01.2023)

13. *Ванина М.Ф., Ерохин А.Г., Ерохина Ю.А*. Архитектура информационной системы консолидации финансовой отчетности с учетом требований российских стандартов // Сборник трудов XV Международной отраслевой научно-технической конференции «Технологии информационного общества». М.: Медиа Паблишер, 2021. С. 224-228.

14. *Ванина М.Ф., Ерохин А.Г., Фролова Е.А*. Системы поддержки принятия решения для бухгалтерских информационных систем // Сборник трудов XVI Международной отраслевой научно-технической конференции. М.: Медиа Паблишер, 2022. С. 215-219.

15. *Ерохин А.Г., Ванина М.Ф.* IT-подготовка специалистов-экономистов в техническом вузе в условиях импортозамещения // Информатизация образования и методика электронного обучения: цифровые технологии в образовании. Материалы V Международной научной конференции. В 2-х частях. Часть 1, под общей редакцией М.В. Носкова. Красноярск, 2021. С. 155-159.

16. *Ванина М.Ф., Ерохин А.Г*. Повышение эффективности бизнеса компании на основе технологий Big data и machine learning // Сборник трудов XIV Международной отраслевой научно-технической конференции «Технологии информационного общества». М.: Медиа Паблишер, 2020. С. 336-338.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ АЛГОРИТМОВ ОБРАТНОГО РАСПРОСТРАНЕНИЯ ОШИБКИ И ИМИТАЦИИ ОТЖИГА

Маклачкова Виктория Валентиновна,
Московский Технический Университет Связи и Информатики, ст. преподаватель кафедры СИТиС, Москва, Россия
v.v.maklachkova@mtuci.ru

Шведов Андрей Вячеславович,
Московский Технический Университет Связи и Информатики, ст. преподаватель кафедры СИТиС, Москва, Россия
a.v.shvedov@mtuci.ru

Шульпина Полина Дмитриевна,
Московский Технический Университет Связи и Информатики, студентка гр. БСТ1901, Москва, Россия
polli-lionet@yandex.ru

Гадасин Денис Вадимович,
Московский Технический Университет Связи и Информатики, доцент кафедры СИТиС, к.т.н., Москва, Россия
dengadiplom@mail.ru

Аннотация

Оптимизация сходимости нейросетевого классификатора (Neural Net Classifier) является важной задачей для повышения скорости и точности процесса принятия решений. Для облегчения процесса оптимизации используются алгоритмы обучения. Алгоритм имитации отжига (Simulated Annealing) и Метод обратного распространения ошибки (Back propagation) - два популярных алгоритма оптимизации. Цель анализа - сравнить оптимизационные характеристики имитационного отжига и обратного распространения ошибки на нейросетевом классификаторе с прямой передачей, который в большей степени полагается на обратное распространение. Для анализа рассматриваются пять стандартных наборов данных, таких как WINE, IRIS, DIABETES, TEACHING ASSISTANT EVALUATION (TAE) и GLASS.

Ключевые слова: *Метод обратного распространения ошибки, алгоритм имитации отжига, нейронные сети, классификатор, машинное обучение, оптимизация, Neural Net Classifier, Simulated Annealing, Back propagation.*

Введение

Искусственная нейронная сеть (ИНС) является математическим представлением сетей нейронов в мозге и имеет схожие функции, такие как получение входных данных, их обработка и последующая генерация выходных данных. Она напоминает связный граф узлов, которые переплетены взвешенными связями, подобно биологическому нейрону. Среди различных типов искусственных нейронных сетей можно выделить многослойный перцептрон, сеть с прямой передачей, сеть Кохонена, адаптивную резонансную сеть и т.д. [1]. Первые две сети ведут себя как классификаторы, т.е. они могут обучаться на примерах, в то время как другие сети обучаются на основе наблюдений, а затем обновляют веса сети. Таким образом, используется метод обучения без учителя, что видно в случаях кластеризации [2, 3, 14-28]. В данной работе для целей классификации была разработана сеть с прямой передачей (feed-forward network). Сеть с прямой передачей позволяет сигналу/информации поступать от входного слоя к выходному в прямом направлении через скрытый слой [4]. Все сети с прямой передачей могут быть обучены с учителем, чтобы они могли изучать модели признаков, имеющиеся в данных. Цель процесса обучения состоит в том, чтобы заставить сеть наилучшим образом изучать признаки [5], что выражается в минимизации квадратичной ошибки (т.е. квадратичной разницы между расчетным и желаемым выходом).

Метод обратного распространения ошибки - один из самых популярных алгоритмов обучения нейронной сети для обучения с учителем [6]. Веса корректируются и обновляются с помощью обобщенного дельта-правила, чтобы минимизировать ошибку предсказания путем итераций. Методология коррекции весов состоит в обратном распространении ошибок от выходного слоя к скрытому, что позволяет найти оптимальный набор весов [7].

Алгоритм имитации отжига — это вероятностный мета-алгоритм для глобальной оптимизации [8]. Это аналогия с физическим процессом, когда твердое тело медленно охлаждается, пока его структура не перейдет в «замороженное» состояние, что происходит при минимальной энергетической конфигурации. Как и в алгоритме обратного распространения ошибки, в алгоритме имитации отжига веса должны пройти через ряд конфигураций в процессе, пока не достигнут глобального минимума. Среди множества алгоритмов оптимизации можно выделить эволюционные алгоритмы, например, метод роя частиц (МРЧ) [9], генетический алгоритм (ГА), генетическое программирование (ГП) и т.д.

Основной целью данной работы является сравнение показателей алгоритма имитации отжига и метода обратного распространения ошибки в архитектуре ИНС с прямой передачей для распознавания образов.

Данные и инструменты для сравнительного анализа

Для проведения сравнительного анализа алгоритмов, применяемых в процессе обучения ИНС, будем использовать следующие составные части.

1. *Данные*. Пять стандартных наборов данных, таких как WINE (178 × 13; класс: 1-3), IRIS (150 x 4; Class: 1-3), TEACHING ASSISTANT EVALUATION (TAE: 149 x 5; Class: 1-3), GLASS (214 × 10; Class: 1-6) и DIABETES (150 x 8; Class: 1-2), которые собраны из репозитория UCI Machine Learning Repository [10].

2. Инструмент. В качестве инструмента разработки и реализации ИНС может быть использована среда разработки Dev C++, а для построения графиков результатов - MATLAB 9.

3. *Методы*:

3.1. *Нейронная сеть прямого распространения*. В качестве способов построения нейронной сети выбирается сеть прямого распространения с использованием особенностей структуры на языке С. Количество скрытых слоев каждой сети ограничено одним для каждого используемого набора данных. Количество нейронов в скрытом слое составляет половину нейронов во входном слое. В таблице 1 описана структура каждой разработанной сети.

Таблица 1

Описание разработанных сетей

Описание сети	**Wine**	**Iris**	**Diabets**	**TAE**	**Glass**
количество слоев	3	3	3	3	3
количество скрытых слоев	1	1	1	1	1
количество нейронов во входном слое	13	4	8	5	9
количество нейронов в выходном слое	1	1	1	1	1
количество нейронов в скрытом слое	6	2	4	3	5

Логарифмическая сигмоидная функция – одна из самых часто используемых типов передаточных функций. Сигмоидные функции полезны для приложений машинного обучения [11], где действительное число необходимо преобразовать в вероятность. Сигмоидная функция, размещенная в качестве последнего слоя модели машинного обучения, может служить для преобразования выходных данных модели в оценку вероятности, с которой легче работать и интерпретировать. Сигмоидные функции являются важной частью модели логистической регрессии.

Функции передачи такого типа присущи нейронам, находящимся во внутренних слоях нейронной сети [12]. Логарифмическая сигмоидная функция в (1) используется в качестве передаточной функции, связанной с нейронами в скрытом и выходном слоях для получения нормализованных [0, 1] узловых выходов.

$$f(x) = (1 + e^{-x})^{-1} \tag{1}$$

3.2. *Нормализация*. При использовании логарифмического сигмоида в качестве передаточной функции, необходимо нормализовать входные значения [0,1]. Это уменьшит сложность вычислений. Значения классов для каждого набора данных также нормализованы в диапазоне от 0 до 1 для однородности данных.

3.3. *Метод обратного распространения ошибки*. Алгоритм работает в два этапа. Сначала на входной слой подается обучающий входной шаблон, который передается на выходной слой через скрытый слой для создания выходного сигнала сети. Средняя квадратическая ошибка (Mean Square Error) затем рассчитывается путем сравнения вычисленного выхода (Calculated Output) и целевого выхода (Target Output) для каждого входа (уравнение 2, где « N » обозначает количество всех экземпляров).

$$MSE = \frac{1}{N}\sum_{i=1}^{N}(TO - CO)^2 \tag{2}$$

На следующем этапе, при средней квадратичной ошибке, сигнал/информация сети обратно распространяется от выходного слоя к входному, и соответствующие веса коннекторов обновляются с помощью «обобщенного правила Δ», которое состоит из скорости обучения и константы импульса [13]. Уравнения 3 и 4 выражают правило Δ обновления веса. В этих уравнениях обозначение «w» означает веса между коннекторами «i» и «j», а «t» - состояние итерации.

$$\Delta w_{i,j}^{t} = -\lambda \frac{\partial MSE}{\partial w_{i,j}^{t}} + \alpha . W_{i,j}^{t} \tag{3}$$

$$w_{i,j}^{t+1} = \Delta w_{i,j}^{t} + w_{i,j}^{t} \tag{4}$$

Получение наилучших значений λ (минимальная среднеквадратичная ошибка) производится исходя из строгого параметрического анализа. Для сравнения с алгоритмом имитационного отжига выбирается процент, при котором ошибка наименьшая. Константа импульса (α) установлена равной 0,9 для всех случаев, чтобы ускорить процесс обучения. Размер эпохи задается равным 100.

3.4. *Алгоритм имитации отжига*. Температура (T) - очень важный, который является аналогом T в физических системах. Начиная с высокой T, алгоритм достигает самой низкой T с постепенным понижением и достижением состояния «теплового равновесия» при каждой T. При каждом T весовые коэффициенты рандомизируются. Новый набор весов принимается в качестве нового оптимизированного набора, если средняя квадратическая ошибка с этим набором меньше, чем с предыдущим набором или с вероятностью, что текущий набор весов приведет к глобальному минимуму. Как и в методе обратного распространения ошибки, используются целевая функция и передаточные функции. В целях сравнения предполагается, что если число изменений в наборе весов больше 10 или число итераций больше 15000, то считается, что равновесное состояние при определенной T достигнуто. Начальная T выбрана равной 10°C, а конечная T - 1°C произвольно. Кроме того, T понижается в 0,95 раз произвольно, поскольку трудно найти точные значения начальной, конечной и пониженной T. Диапазон поиска устанавливается от 2 до +2. Алгоритм реализации – это $(E(s))$ - объективная функция.

Сравнение метода обратного распространения ошибки и алгоритма имитации отжига

Обучение и тестирование сети с методом обратного распространения ошибки проводится для заданного размера эпохи для всех наборов данных со всеми возможными значениями λ (см. рис. 1). Для сравнения с алгоритмом имитации отжига выбирается λ с минимальным значением средней квадратичной ошибки (MSE) для тестовых случаев. Из рис.1 можно отметить, что для (a) данных IRIS, MSE составляет 0.0062 при λ = 0.2, (b) для данных WINE минимальная MSE составляет 0.0037 при λ = 0.8; (c) для данных DIABETES минимальная MSE составляет 0.0980 при λ = 0.7; (d) для TAE минимальная MSE составляет 0.0558 при λ = 0.2; и, наконец, (e) для данных GLASS, значения составляют 0.0363 при λ = 0.1, соответственно. Эти оптимальные значения λ (т.е. λ^*) используются для сравнения между методом обратного распространения ошибки и алгоритмом имитации отжига. В случае метода

обратного распространения ошибки вычисляется MSE по эпохам, в то время как для алгоритма имитации отжига для измерения MSE рассматриваются этапы охлаждения.

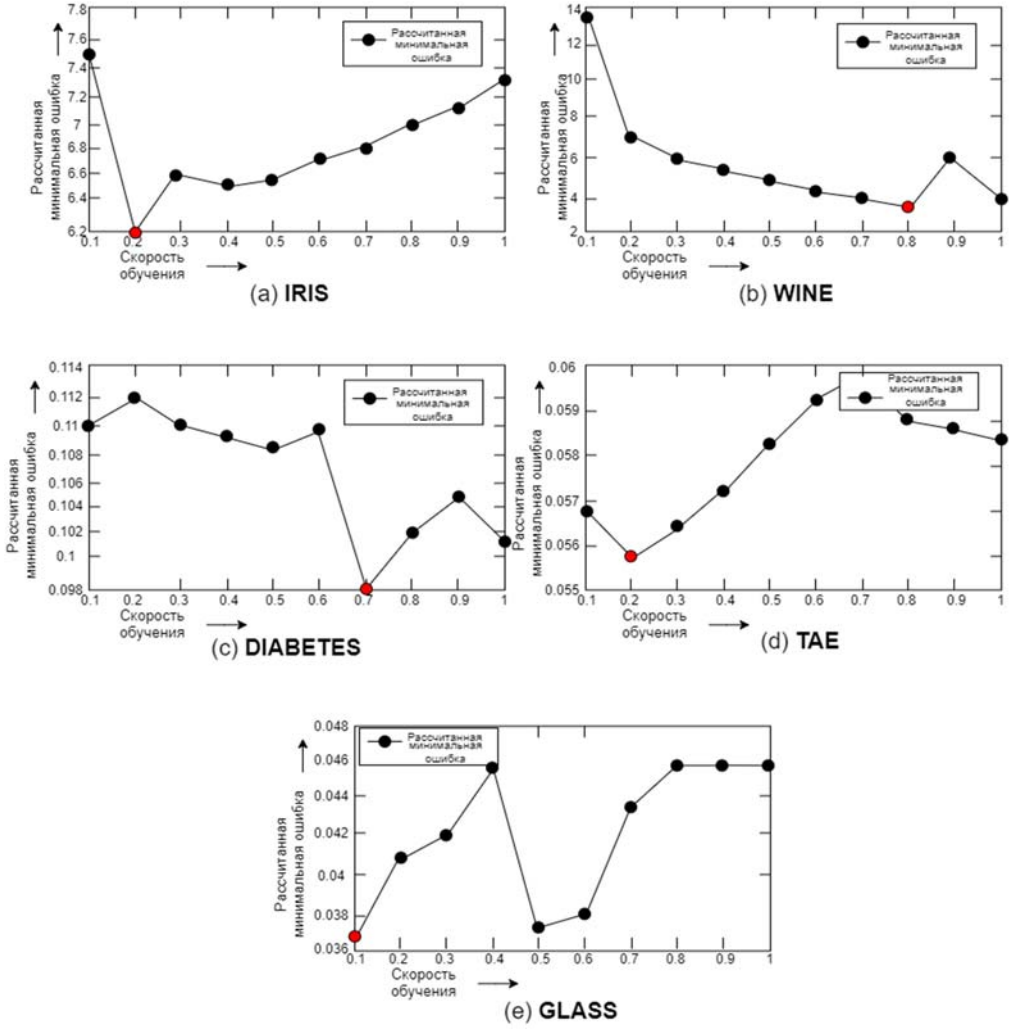

Рис. 1. Параметрическое сравнение MSE и λ для наборов данных (a) WINE; (b) IRIS; (c) DIABETES; (d) TAE; (e) GLASS

Диапазон параметра «Температура» (T) был выбран от 10° C до 1° C. «Равновесное состояние» для него состоит либо из 10 изменений набора весов, либо из 15000 итераций, тогда как размер эпохи в случае метода обратного распространения ошибки составляет 100. Поэтому очевидно, что на обучение алгоритма имитации отжига отводится больше времени. На рис. 2 показаны результаты обучения и тестирования для всех пяти данных. В табл. 2 и 3 приведены результаты обучения и тестирования, соответственно.

Таблица 2

Сравнение характеристик метода обратного распространения ошибки и алгоритма имитации отжига (во время обучения)

Набор данных	**Метод обратного распространения ошибки (λ *)**		**Алгоритм имитации отжига (-2, 2)**	
	Эпоха	Средняя квадратическая ошибка	T	Средняя квадратическая ошибка
1. IRIS	96	0.0071	1.577	0.0048
2. WINE	44	0.0017	1.498	0.0001
3. DIABETES	100	0.0748	1.046	0.0672
4. TAE	100	0.0634	1.046	0.0541
5. GLASS	100	0.0125	1.046	0.0041

Таблица 3

Сравнение характеристик метода обратного распространения ошибки и алгоритма имитации отжига (во время тестирования)

Набор данных	**Метод обратного распространения ошибки**		**Алгоритм имитации отжига**	
	Эпоха	Средняя квадратическая ошибка	*T*	Средняя квадратическая ошибка
1. IRIS	100	0.0062	4.876	0.0043
2. WINE	32	0.0037	5.403	0.0050
3. DIABETES	89	0.0980	9.025	0.0940
4. TAE	62	0.0558	9.025	0.0549
5. GLASS	5	0.0363	9.500	0.0268

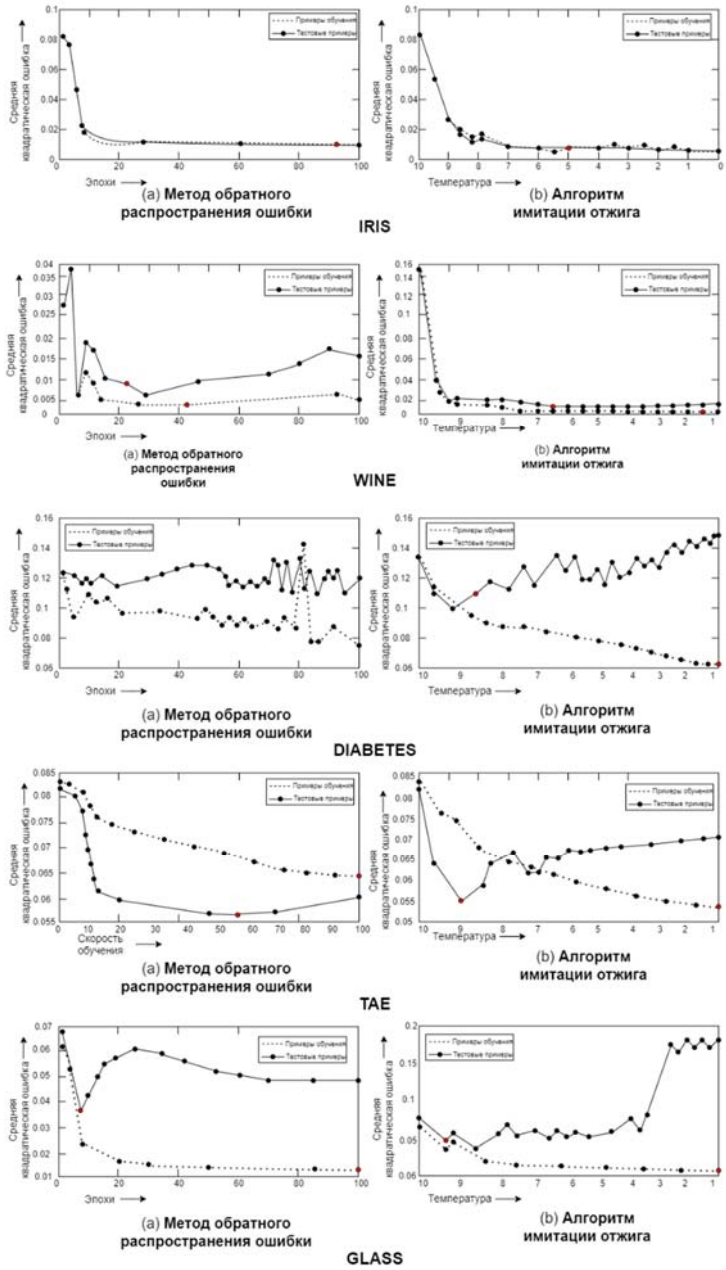

Рис.2. Сравнение между (a) оптимизированным методом обратного распространения ошибки и (b) алгоритмом имитации отжига на всех 5 наборах данных

Таблицы 2 и 3 показывают, что в процессе обучения алгоритм имитации отжига превосходит метод обратного распространения ошибки для всех наборов данных. За исключением данных WINE (хотя разница незначительна), он также показал лучшие результаты, чем метод обратного распространения ошибки при тестировании сети. Это наблюдение показывает, что подход имитационного отжига для поиска решения в пространстве поиска приводит нас к глобальному оптимуму, в то время как метод обратного распространения ошибки мог застрять в локальных минимумах. Таким образом, задача классификации лучше решается с помощью алгоритма имитации отжига по сравнению с методом обратного распространения ошибки.

Заключение

В работе сравниваются различные показатели алгоритмов обратного распространения ошибки и имитационного отжига на классификаторе на основе нейронной сети прямого распространения исходя из пяти наборов данных, таких как IRIS, WINE, DIABETES, TAE и GLASS. Перед фактическим сравнением, лучшие λ для каждого набора данных были получены путем параметрических исследований во время метода обратного распространения ошибки (рис. 2).

При сравнении показателей метода обратного распространения ошибки и алгоритма имитации отжига анализ показал, что алгоритм имитации отжига может предсказать как примерные, так и неизвестные паттерны более точно по сравнению с методом обратного распространения ошибки, за исключением данных WINE, однако разница в средней квадратической ошибке незначительна.

Это объясняется тем, что при методе обратного распространения ошибки невозможно преодолеть локальный минимум из-за его хорошо направленного сопряженного градиентного подхода и зависимости от оптимальной скорости обучения (полученной во время обучения). Имитация отжига, будучи случайным поиском, может иметь больше пространства и поэтому имеет меньше шансов застрять в локальных минимумах.

Литература

1. *Вакурин И.С., Гадасин Д.В.* Аспекты легальности принятия решений системами искусственного интеллекта // Искусственный интеллект и цифровая экономика: взгляд студенчества: материалы I Всероссийской студенческой научно-практической конференции, Москва, 13 ноября 2019 года / Министерство науки и высшего образования Российской Федерации, Государственный университет управления. М.: Государственный университет управления, 2020. С. 235-237. EDN AMDKSH.

2. *Гадасин Д. В., Юдина А.А.* Кластеризация в крупномасштабных сетях // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2020. № 1. С. 19-26. EDN OYSXON.

3. *Гадасин Д.В., Шведов А.В., Кузин И.А*. Трехмерная реконструкции объекта по одному изображению с использованием глубоких свёрточных нейронных сетей // T-Comm: Телекоммуникации и транспорт. 2022. Т. 16. № 7. С. 29-35. DOI 10.36724/2072-8735-2022-16-7-29-35. EDN YTLCNW.

4. *Gadasin D.V., Shvedov A.V., Vakurin I.S.* Determination of Semantic Proximity of Natural Language Terms for Subsequent Neural Network Training // 2022 Systems of Signals Generating and Processing in the Field of on Board Communications, SOSG 2022 – Conference Proceedings, Moscow, 15-17 марта 2022 года. Moscow, 2022. DOI 10.1109/IEEECONF53456.2022.9744290. EDN LASMDY.

5. *Gadasin D.V., Shvedov A.V., Kuzin I.A*. Reconstruction of a Three-Dimensional Scene from its Projections in Computer Vision Systems // 2021 Intelligent Technologies and Electronic Devices in Vehicle and Road Transport Complex, TIRVED 2021 - Conference Proceedings, Moscow, 11-12 ноября 2021 года. Moscow, 2021. DOI 10.1109/TIRVED53476.2021.9639161. EDN CKSNPA.

6. *Гадасин Д.В., Шведов А.В., Кольцова А.В.* Вероятностная оценка построения виртуального кластера // Труды международного симпозиума "Надежность и качество". 2021. Т. 1. С. 87-92. EDN BCNSGB.

7. *Jung G. Wang.* Pattern Classification of Back-Propagation Algorithm Using Exclusive Connecting Network // World Academy of Science, Engineering and Technology, 2007, pp. 1785-1789, doi: 10.5281/zenodo.1071960.

8. Kirkpatrick S., Gelau C.D., Vechhi M.P. Optimization by Simulated Annealing // Science. Vol. 220, 1983, pp. 671-680, doi: 10.1126/science.220.4598.671.

9. *Гадасин Д.В., Смальков Н.А., Кузин И.А*. Использование метода роя частиц для балансировки нагрузки в сетях Интернета вещей // Системы синхронизации, формирования и обработки сигналов. 2022. Т. 13. № 2. С. 17-23. EDN LIUWNT.

10. *Theodoridis S., Koutroumbas K.* Pattern Recognition // Academic Press, 2009, p. 984, doi: 10.1109/TNN.2008.929642.

11. *Гадасин Д.В., Шведов А.В., Пантелеева К.А*. Предобработка информации для систем машинного обучения // Актуальные проблемы и перспективы развития экономики: Труды XXI Международной научно-практической

конференции, Симферополь-Гурзуф, 20-22 октября 2022 года. Симферополь: Крымский федеральный университет им. В.И. Вернадского, 2022. С. 268-269. EDN QVIOMF.

12. *Шведов А.В., Гадасин Д.В., Цыгулёва А.В., Вакурин И.С*. Разгрузка очереди сети при помощи Гамильтонова цикла // REDS: Телекоммуникационные устройства и системы. 2021. Т. 11. № 3. С. 45-53. EDN XWXWQX.

13. *Shvedov A.V., Gadasin D.V., Pak E.V*. Application of the Backman Model for the Distribution of Traffic Flows in Networks with Segment Routing // 2022 Systems of Signals Generating and Processing in the Field of on Board Communications, SOSG 2022 - Conference Proceedings, Moscow, 15-17 марта 2022 года. Moscow, 2022. DOI 10.1109/IEEECONF53456.2022.9744344. EDN RBMTBQ.

14. *Гадасин Д.В., Кольцова А.В., Полякова А.Н.* Модель построения кластера для пограничных вычислений // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2020. № 1. С. 86-92.

15. *Shvedov A.V., Gadasin D.V., Alyoshintsev A.V*. Segment routing in data transmission networks // T-Comm. 2022. Vol. 16. No. 5. P. 56-62. DOI 10.36724/2072-8735-2022-16-5-56-62. EDN VAYLJQ.

16. *Шведов А.В., Гадасин Д.В., Клыгина О.Г.* Организация взаимодействия туманных вычислений и сегментной маршрутизации для предоставления сервисов IOT в smart grid // Системы синхронизации, формирования и обработки сигналов. 2022. Т. 13. № 3. С. 40-49. EDN TRRYZN.

17. *Назаров М.Д., Шведов А.В*. Корреляция атрибутов соглашения об уровне обслуживания с основными параметрами QoS в корпоративных сетях // Телекоммуникации и информационные технологии. 2020. Т. 7. № 2. С. 73-79. EDN VQHDTJ.

18. *Гадасин Д.В., Шведов А.В., Клыгина О.Г., Гадасин Д.Д.* Реализация платформы туманных вычислений для предоставления сервисов IoT // REDS: Телекоммуникационные устройства и системы. 2021. Т. 11. № 2. С. 65-75.

19. *Kalmykov N.S., Dokuchaev V.A*. Segment routing as a basis for software defined network // T-Comm. 2021. Т. 15. № 7. С. 50-54.

20. *Dokuchaev V.A., Maklachkova V.V., Statev V.Yu*. Classification of personal data security threats in information systems // T-Comm. 2020. Т. 14. № 1. С. 56-60.

21. *Докучаев В.А., Маклачкова В.В., Статьев В.Ю.* Цифровизация субъекта персональных данных // T-Comm: Телекоммуникации и транспорт. 2020. Т. 14. № 6. С. 27-32.

22. *Pavlov S.V., Dokuchaev V.A., Mytenkov S.S*. Model of a fuzzy dynamic decision support system // T-Comm. 2020. Т. 14. № 9. С. 43-47.

23. *Pavlov S.V., Dokuchaev V.A., Maklachkova V.V., Mytenkov S.S*. Features of supporting decision making in modern enterprise infocommunication systems // T-Comm. 2019. Т. 13. № 3. С. 71-74.

24. *Гадасин Д.В., Кольцова А.В., Гадасин Д.Д., Полякова А.Н.* Оценка вероятности формирования виртуального кластера // Системы синхронизации, формирования и обработки сигналов. 2021. Т. 12. № 1. С. 4-12.

25. *Кузин И.А., Гадасин Д.В*. Модель контейнера данных для минимизации трафика при передаче субъективных характеристик объектов на изображении трехмерной сцены // Телекоммуникации и информационные технологии. 2021. Т. 8. № 2. С. 96-100.

26. *Усачева Д.И., Шишкин М.О., Гадасин Д.В., Гузеев А.В.* Применение OLAP-технологий для анализа многомерных данных в контакт-центре // Телекоммуникации и информационные технологии. 2019. Т. 6. № 1. С. 142-149.

27. *Гадасин Д.В., Кузин И.А*. Модель представления цветовых и глубинометрических характеристик объектов на изображении // DSPA: Вопросы применения цифровой обработки сигналов. 2021. Т. 11. № 1. С. 31-38.

28. *Гадасин Д.В., Нестерова Е.А.* Особенности проведения практических занятий по дисциплине мультимедийные информационные системы для стадии "исследование и обоснование создания информационной системы" // Методические вопросы преподавания инфокоммуникаций в высшей школе. 2021. Т. 10. № 1. С. 15-21.

БЕЗОПАСНОСТЬ ВИРТУАЛЬНЫХ КОНТЕЙНЕРОВ

Михалевич Игорь Феодосьевич,
Российский университет транспорта, доцент, к.т.н., старший научный сотрудник, Москва, Россия
mif-orel@mail.ru

Савицкий Даниил Дмитриевич,
Российский университет транспорта, Москва, Россия
4613799@gmail.com

Станчук Полина Николаевна,
Российский университет транспорта, Москва, Россия
pn_stanchuk@mail.ru

Аннотация
В статье рассмотрены векторы атак и актуальные угрозы безопасности систем контейнеризации программного обеспечения и оркестрации контейнеров. Для указанных систем приведены примеры уязвимостей и условий их эксплуатации, рекомендации по обеспечению информационной безопасности контейнеров

Ключевые слова: *Безопасность информации, виртуализация, информационная безопасность, система контейнеризации, угрозы, оркестрация контейнеров, уязвимости, Docker, Kubernetes*

Введение

Пандемия COVID-19 вызвала ускорение цифровой трансформации в различных сферах экономики и жизнедеятельности [1], массовый переход к удаленной работе сотрудников, обострив проблемы цифровой гигиены [2] и информационной безопасности. Решение указанных проблем неразрывно связано с обеспечением безопасности программного обеспечения (ПО) [3] и реализацией мероприятий по его безопасной разработке [4].

В этой области широко используется виртуализация. Ее появление и развитие связано с технологиями, обеспечивающими преобразование формата и/или параметров системных (программных, сетевых) запросов к вычислительным ресурсам для устранения зависимости процессов обработки информации от конкретной аппаратной или программной платформы автоматизированной (информационной) системы [5].

Посредством виртуализации могут создаваться виртуальные машины и виртуальные контейнеры. В последнем случае слово «виртуальные» обычно не используется.

Контейнеризация и виды контейнеров

Виртуальная машина представляет собой вычислительную систему, в состав которой входят виртуальные устройства обработки, хранения и передачи данных, а также, в необходимых случаях, программное обеспечение (далее – ПО) и пользовательские данные. Чаще всего виртуальные машины используются для обеспечения работы гостевых операционных систем, что особенно важно при необходимости использования прикладного (программного) ПО, разработанного под устаревшие версии операционных систем. В этом случае дополнительные накладные расходы, связанные с поддержкой виртуальных машин гипервизором, являются оправданными.

В остальных случаях предпочтение может отдаваться контейнерам, способным виртуализировать ПО (приложения), аппаратное обеспечение и вычислительные системы. В случае виртуализации ПО контейнером создается изолированная программная среда, содержащая специфический набор компонентов имитируемой операционной системы, обеспечивающих работу отдельных программ [5]. При виртуализации аппаратного обеспечения и вычислительных систем контейнер образует изолированную программную среду в составе специфического набора компонентов имитируемого микропрограммного и аппаратного обеспечения, обеспечивающих работу отдельных операционных систем.

И в том и другом случае системы контейнеризации, образы контейнеров, средства управления ими и сами контейнеры должны быть безопасными, для чего должны своевременно выявляться и устраняться их уязвимости [6].

Средства контейнеризации

Для работы нескольких контейнеров достаточно одной операционной системы (хостовой), ядро которой используется совместно [7, 8]. Пример такого использования ядра представлен на рисунке 1.

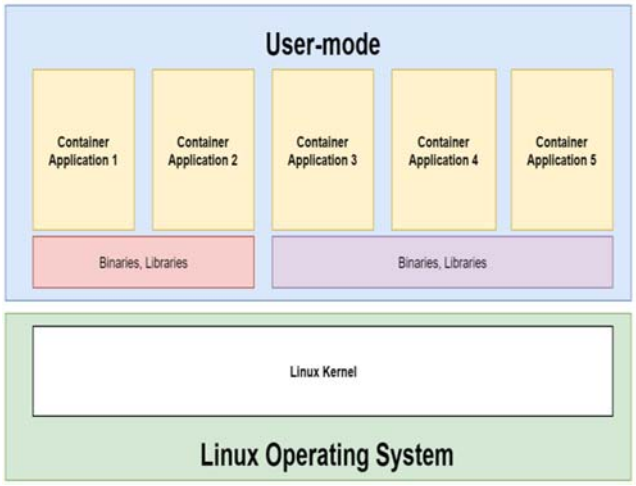

Рис. 1. Пример системы контейнеризации (Источник: [8])

В действительности контейнер содержит не только приложение, но, как было отмечено выше, в его составе имеется «легковесная» операционная система, адаптированная под конкретное приложение. Именно под их управлением находятся процессы запущенных программ. Поэтому можно согласиться с мнением [9], что с точки зрения хоста в контейнере осуществляется контейнеризация процессов.

В [10] проведен анализ существующих систем контейнеризации. Результаты анализа приведены на рисунке 2. Исследователи выделили в лучшую сторону LXC и Docker, отметили, что Docker базируется на LXC, но более прост в создании и настройке контейнеров, отдали приоритет Docker.

Аналогичные выводы содержатся в [11].

Критерии \ Система управления контейнерами	Linux-VServer	OpenVZ	LXC	Docker
Изоляция процессов, IPC	+ (собственная модификация ядра Linux)	+ (kernel namespaces)	+ (kernel namespaces)	+ (kernel namespaces)
Изоляция файловой системы	+	+	+	+
Изоляция сети	+/- (использования сети физического сервера)	+	+ (network namespaces)	+
Планирование процессора	+ (Token Bucket Filter)	+ (Fair Scheduler)	+	+
Ограничение использования системных ресурсов	+ (rlimit, cgroups)	+ (User Beancounters, Disk Quota и VCPU Affinity)	+ (cgroups)	+ (cgroups)
Возможность сохранения /восстановления	-	+	+	+
Возможность живой миграции	-	+	+	+

Рис. 2. Характеристики систем контейнеризации [10]

Docker – это платформа для создания, запуска и управления контейнерами. Как уже отмечалось ранее контейнер содержит в себе всё необходимое для запуска приложения, включая код, библиотеки, настройки и данные. Контейнеры запускаются на хостовой операционной системе и, хотя совместно используют ресурсы хоста, остаются изолированными и от хоста и друг от друга. Это позволяет развёртывать и запускать приложения в различных окружениях без взаимных конфликтов и проблем с зависимостями.

Для развертывания контейнеров используются их образы, которые представляют собой статические шаблоны, содержащие все необходимые компоненты для запуска приложения. Это обеспечивает возможность развертывания образов на различных платформах, сохраняя согласованность и предсказуемость их тиражирования

Docker организован на архитектуре клиент-сервер и выполняет следующие действия:

- проверка наличия образа на хосте. При отсутствии загрузка из хранилища образов (публичного с сайта Docker Hub или частного);
- создание контейнера из образа;
- разметка файловой системы и добавление слоя для записи;
- создание сетевого интерфейса;
- присвоение контейнеру IP-адреса;
- запуск приложения в контейнере.

В состав Docker входят следующие основные компоненты, которые необходимо защищать:

- демон. Выполняет функции сервера контейнера;
- клиент. Обеспечивает взаимодействие пользователя с демоном (демонами);
- образ контейнера (файл, содержащий зависимости, данные и конфигурацию контейнера);
- файл с набором правил, используемых при построении образа;
- контейнер. Автономно исполняемый пакет, содержащий все необходимое для запуска приложения: код, среду выполнения, системные инструменты, системные библиотеки и настройки;
- Volume. Эмулятор файловой системы. Необходим для выполнения операций чтения и записи;
- реестр. Зарезервированный сервер хранения образов.

Политика безопасности и встроенные механизмы защиты

Политика безопасности Docker и встроенные механизмы защиты предусматривают следующие меры:

- минимизация контейнера. В контейнере должно быть только минимально необходимое ПО для поддержки работающих процессов. Это снижает риски, связанные с уязвимостями ПО;
- выполнение контейнерами специфических задач. То есть должно быть заранее известно, что должно выполняться в контейнере, определены пути к директориям, открыты порты, конфигурации демонов, точки монтирования и т.д. Это упрощает обнаружение аномалий, связанных с безопасностью, и значительно уменьшает поверхность для атак;
- изоляция контейнеров от хоста и друг от друга. При этом необходимо помнить, что ресурсы ядра делятся между хостом и контейнерами;
- наблюдаемость. Выполнение требований к программной документации обеспечивает администраторам возможность выяснить, из чего и как был сделан контейнер.

Модель угроз безопасности контейнеров

Моделирование угроз информационной безопасности предполагает анализ возможных действий злоумышленников, направленных на компрометацию защищаемой системы и ее элементов, формирование векторов атак и перечней актуальных угроз. Сведения о векторах атак и актуальных угрозах позволяют разработать и внедрить адекватную систему защиты информации и управления безопасностью.

Вектор актуальных угроз для контейнеров Docker и поражаемые при реализации угроз элементы защищаемой системы представлены на рисунке 3. При исполнении рисунка использовались результаты исследований, приведенные в [12].

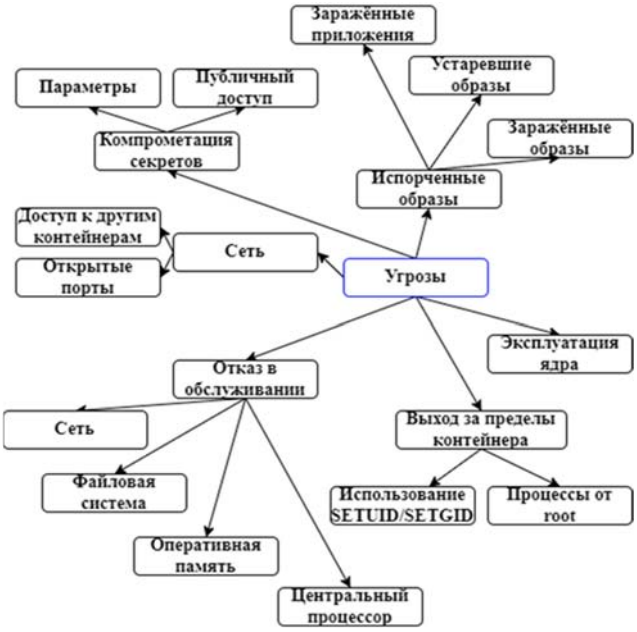

Рис. 3. Модель угроз Docker-контейнера

Для примера рассмотрим реализацию угрозы «Выход за пределы контейнера» [13].

Совершить выход из Docker-контейнера возможно при запуске контейнера в привилегированном режиме. Чтобы запустить контейнер в таком режиме используется флаг --privileged, или --cap-add, а в качестве параметра должна быть передана привилегия SYS_ADMIN.

 # На хосте

docker run --rm -it --cap-add=SYS_ADMIN --security-opt apparmor=unconfined ubuntu

 # В контейнере

bash

После перехода внутрь контейнера можно создать каталог /tmp/cgrp, смонтировать контроллер контрольной группы RDMA (remote direct memory access), получить прямой доступ к памяти, и добавить дочернюю контрольную группу (в данном случае x):

mkdir /tmp/cgrp && mount -t cgroup -o rdma cgroup /tmp/cgrp && mkdir /tmp/cgrp/x

Затем можно активировать функцию release_agent:

echo 1 > /tmp/cgrp/x/notify_on_release,

и прописать путь до release_agent:

host_path=`sed -n 's/.\perdir=\([^,]*\).*/\1/p'*

/etc/mtab`

echo "$host_path/cmd" > /tmp/cgrp/release_agent.

Далее атакующий создаст bash-скрипт и впишет в него команды, которые будут выполняться на основном хосте. Пусть файл с выполняемыми командами имеет название cmd, а файл, куда будут записываться результаты выполнения – output:

echo '#!/bin/sh' > /cmd

echo "ps aux > $host_path/output" >> /cmd

Чтобы скрипт запустился, он должен быть исполняемым, то есть иметь следующие права:

chmod a+x /cmd

Для выполнения атаки необходимо запустить процесс, который завершится внутри ранее созданной дочерней контрольной группы x. После этого на основном хосте будет инициализировано выполнение сценария /cmd:

sh -c "echo \$\$ > /tmp/cgrp/x/cgroup.procs"

Предотвратить данный или схожий способ атаки можно с использованием следующих правил [13, 14]:

- минимизировать контейнеры с ключом --privileged. Контейнеры обычно запускаются с ключом -- privileged, когда необходимо получить доступ к специфичным устройствам хост-системы. Но иногда при определённой архитектуре приложения подразумевается запуск контейнеров только в привилегированном режиме;

- минимизировать контейнеры с привилегией SYS_ADMIN. Помимо полного представления прав с помощью флага --privileged можно разрешить выполнение только определённых действий в системе. Это можно достичь при помощи механизма, встроенного в ядро Linux под названием Linux capabilities (привилегии Linux). В Docker также присутствует данный механизм. Привилегия SYS_ADMIN позволяет запускать в контейнере такие команды, как mount, setdomainname, swapon, sethostname, quotactl. А команда mount как раз необходима для реализации побега из контейнера. Но если запускать контейнеры без привилегией SYS_ADMIN, то команду mount выполнить не удастся;
- использовать отличную от root учётную запись внутри контейнера. Реализовать побег из контейнера может только пользователь root, который обладает всеми правами в системе. Данная уязвимость, в частности, монтирует механизм remote direct memory access;
- использовать внутри контейнера файловую систему только для чтения (--read-only=true). Благодаря этому контейнер не сможет создавать или изменять какие-либо данные внутри себя, тем самым запись новых или редактирование существующих файлов становится невозможны.

Системы оркестрации контейнеров

Для управления контейнерами на физических и виртуальных машинах система Docker имеет встроенное решение Swarm. При его использовании некоторые узлы настраиваются как управляющие (Manager), остальные - как рабочие (Worker). Задача менеджеров - управлять кластером и делегировать задачи рабочим узлам. Однако де-факто «стандартом» для оркестрации Docker называют Kubernetes [15].

Kubernetes является платформой управления контейнеризованными рабочими нагрузками и сервисами, имеет открытый исходный код и обеспечивает [16]:

- мониторинг сервисов и распределение нагрузки. Kubernetes может обнаружить контейнер, используя имя DNS или IP-адрес. Если трафик в контейнере высокий, Kubernetes может сбалансировать нагрузку и распределить сетевой трафик, чтобы развертывание было стабильным;
- оркестрацию хранилища. Kubernetes позволяет автоматически смонтировать систему хранения (локальное хранилище, облака и так далее);
- автоматическое развертывание и откаты. Kubernetes позволяет описать целевое состояние развернутых контейнеров и изменить фактическое состояние на целевое. Например, автоматизировать Kubernetes на создание новых контейнеров для развертывания, удаления существующих контейнеров и распределения всех их ресурсов в новый контейнер;
- автоматическое распределение нагрузки. Kubernetes может разместить контейнеры на узлах так, чтобы ресурсы использовались наиболее эффективно;
- самоконтроль. Kubernetes перезапускает отказавшие контейнеры, приостанавливает и завершает работу контейнеров, которые не проходят проверку работоспособности, и не показывает их, пока контейнеры не будут готовы к работе;
- управление конфиденциальной информацией и конфигурацией. Kubernetes может хранить и управлять конфиденциальной информацией, такой, например, как пароли, OAuth-токены и ключи SSH. Это даёт возможность развертывать и обновлять конфиденциальную информацию и конфигурацию приложения без изменений образов контейнеров, не раскрывая конфиденциальную информацию в конфигурации стека.

Однако, как и любое другое ПО, Kubernetes может подвергаться атакам. В частности, в [17] отмечается:

- безопасность контейнеров находится в ужасном состоянии: 56 % разработчиков в настоящее время даже не сканируют свои контейнеры;
- к 2023 году более 70 % компаний будут использовать контейнерные приложения.
- в 2022 году неправильные настройки составили 59% всех инцидентов безопасности Kubernetes.

Векторы атак начального доступа в средах Kubernetes

Исследователи безопасности Kubernetes [18] выделили два наиболее встречающихся вектора атак, реализующих угрозу начального доступа: использование уязвимых образов и неправильно сконфигурированная система управления базами данных PostgreSQL [19]. Устранив эти угрозы, можно обнаруживать уязвимости в проектах и минимизировать риски, возникающие при наличии доступа.

Рассмотрим примеры.

Метод 1. Уязвимые образы

Некоторые образы нередко заражены вирусом Kinsing (вредоносное программное обеспечение, целью которого является добыча криптовалюты.) Большинство из таких образов позволяет злоумышленнику удалённо выполнить код для использования контейнера в своих целях. Это довольно частое явление. Ниже представлен перечень некоторых приложений, в которых были найдены уязвимости: PHPUnit, Liferay, WebLogic, WordPress.

Пример эксплуатации уязвимости в WebLogic

В 2020 году компания Oracle раскрыла серию уязвимостей высокого уровня, которые позволяли удалённое выполнение кода (CVE-2020-14882, CVE-2020-14750, CVE-2020-14883).

Атакующие сканировали широкий диапазон IP-адресов, в поисках открытых портов WebLogic (по умолчанию 7001). Если сервер был уязвим и на нём установлена одна из прошлых версий WebLogic, то злоумышленники могли использовать один из эксплойтов для запуска вредоносного программного обеспечения. Основным методом был запуск вредоносной команды со следующей структурой:

/bin/bash -c (curl -s Attacker_IP/Payload_Name.sh || wget -q -O- Attacker_IP/Payload_Name.sh) | bash

Обнаружение уязвимости

Одним из способов обнаружения может служить оповещение при идентификации подозрительных загрузок в контейнер, а также подозрительных ресурсов, с которых она проводилась:

- обнаружение загрузки и исполнения файла - файл был загружен в контейнер, выданы права на исполнение, затем - исполнен;
- обнаружение поведения, подобного ботам Linux - выполнение процесса, связанного с сетями botnet Linux;
- обнаружение загрузки подозрительных файлов - выявление подозрительных загрузок бинарных файлов, которые могут представлять опасность для хоста;
- обнаружение подозрительных загрузок и запусков активности - поиск подозрительных файлов, которые были загружены и исполнены (распространено для майнеров).

Минимизация рисков

Существует несколько способов снизить риски. Первое, на что следует обратить внимание при развёртывании - образ должен быть загружен из доверенного источника и обновлён до последней версии. Кроме того, нужно просканировать все образы на наличие уязвимостей, чтобы определить, какие из них уязвимы, и в чём заключаются слабые места. Особенно это важно для контейнеров с доступом в сеть.

Также возможно снизить риски, сведя к минимуму доступ к контейнеру, применив белый список IP-адресов и правила наименьших привилегий к пользователю.

Метод 2. Неправильно сконфигурированный PostgreSQL

Второй по популярности метод получения первоначального доступа и запуска вредоносной полезной нагрузки – это неправильно сконфигурированный контейнер PostgreSQL с доступом в сеть. Было обнаружено большое количество заражённых майнером Kinsing кластеров с запущенными контейнерами PostgreSQL. Существует несколько неправильных настроек, которые злоумышленники могут использовать, чтобы получить доступ к серверу.

Неправильная конфигурация заключается в использовании небезопасных параметров, например, параметр “доверительная аутентификация” (trust authentication). В [19] отмечается, что “Когда указана доверительная аутентификация, PostgreSQL предполагает, что любой, кто может подключиться к серверу, авторизован для доступа к базе данных с любым указанным именем пользователя базы данных (даже с именами суперпользователей)”.

Способы конфигурации и угрозы

Для изменения конфигурации контейнера PostgreSQL имеется несколько способов: отредактировать файл pg_hba.conf или задать переменные окружения (например, POSTGRES_HOST_AUTH_METHOD). Чтобы назначить конфигурацию доверия для определённого IP-адреса, необходимо отредактировать файл pg_hba.conf и добавить следующую строку:

“Host all [IP_Address/range] trust”

В некоторых случаях, когда диапазон адресов шире, чем должен быть или принимает соединения с любого IP-адреса (например, 0.0.0.0/0), злоумышленник может свободно подключаться к серверам PostgreSQL без аутентификации, что может привести к выполнению вредоносного кода. Кроме того,

некоторые сетевые конфигурации в Kubernetes подвержены заражению ARP (ARP Poisoning), протокола канального уровня модели OSI, предназначенного для определения MAC-адреса по известному IP-адресу другого компьютера. Это позволяет злоумышленникам выдавать себя за приложение в кластере, перенаправляя сетевой трафик с помощью использования слабых мест. Следовательно, даже указание частного IP-адреса в доверии может представлять угрозу безопасности.

Предоставление доступа к широкому диапазону IP-адресов подвергает контейнер PostgreSQL потенциальной угрозе. Даже если вместо незащищенного метода аутентификации “доверие” используются другие методы, перед злоумышленниками открываются другие варианты, такие как грубая сила (brute force) для перебора учётных записей, атака на доступность контейнера с помощью DoS- и DDoS-атак и т.д.

Обнаружение уязвимости

Необходимо проверить все параметры, касающиеся разрешающих настроек, и определить неправильные конфигурации контейнеров и манифестов. По возможности использовать систему мониторинга.

Минимизация рисков

Минимизация рисков в ключе неправильно сконфигурированного PostgreSQL заключается в:

- использовании образов из доверенных источников;
- удалении пользователей и всех расширенных разрешений по умолчанию;
- удалении доверительной конфигурации;
- ограничении сетевого доступа к базе данных.

Заключение

Рассмотренные в статье векторы атак и угрозы безопасности систем контейнеризации программного обеспечения и оркестрации контейнеров отражают лишь актуальные на данный момент проблемы обеспечения безопасности информации в виртуальных средах.

Это же касается и приведённых примеров уязвимостей и условий их эксплуатации, рекомендаций по обеспечению информационной безопасности контейнеров.

Развитие технологий виртуализации несомненно вызовет появление новых угроз и возможно приведет к изменению векторов атак, что постоянно будет находиться в поле наблюдения авторов статьи.

Литература

1. *Михалевич И.Ф.* Цифровая трансформация систем управления в условиях пандемии COVID-19 // REDS: Телекоммуникационные устройства и системы. № 4. 2021. С. 26-32.

2. *Михалевич И.Ф.* Цифровая гигиена информационного общества: влияние пандемии COVID-19 // REDS: Телекоммуникационные устройства и системы. № 3. 2022. С. 10-17.

3. Mikhalevich I.F. Priority Ways to Ensure Cybersecurity of Cooperative Intelligent Transport Systems // 2022 International Conference “Systems of Signals Generating and Processing in the Field of on Board Communications”, IEEE. 2022. doi.org/10.1109/IEEECONF53456.2022.9744337. https://ieeexplore.ieee.org/document/9744337 (доступ 13.10.2022).

4. ГОСТ Р 56939-2016. Защита информации. Разработка безопасного программного обеспечения. Общие требования.

5. ГОСТ Р 56938-2016. Защита информации. Защита информации при использовании технологий виртуализации. Общие положения.

6. Требования по безопасности информации к средствам контейнеризации (утв. приказом ФСТЭК России от 4 июля 2022 г. № 118). https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/120-normativnye-dokumenty/2557-vypiska-iz-trebovanij-po-bezopasnosti-informatsii-utverzhdennykh-prikazom-fstek-rossii-ot-4-iyulya-2022-g-n-118 (доступ 12.01.2023).

7. *Shashank Mohan Jain.* Linux Containers and Virtualization: A Kernel Perspective. 2020. https://link.springer.com/book/10.1007/978-1-4842-6283-2 (доступ 13.10.2022).

8. *Piotr Tylenda.* Hands-On Kubernetes on Windows. Effectively orchestrate Windows container workloads using Kubernetes. 2020. Published by Packt Publishing Ltd, Birmingham, UK, 2020. ISBN 978-1-83882-156-2. https://international.scholarvox.com/catalog/book/88884071 (доступ 13.10.2022).

9. *Райс Л.* Безопасность контейнеров. Фундаментальный подход к защите контейнеризованных приложений. СПб: Питер, 2021. 224 с.

10. *Адрова Л.С., Полежаев П.Н.* Сравнительный анализ существующих технологий контейнеризации. http://elib.osu.ru/bitstream/123456789/1955/1/2473-2477.pdf (доступ 27.01.2023).

11. *Дибиров Г.М., Бабков И.Н., Ковцур М.М*. Сравнительный анализ решений для контейнеризации // Молодежная школа-семинар по проблемам управления в технических системах имени А.А. Вавилова. https://www.elibrary.ru/download/elibrary_48665313_86616952.pdf (доступ 27.01.2023).

12. Threat Modeling. https://github.com/OWASP/Docker-Security/blob/main/001%20-%20Threats.md (доступ 29.12.2022).

13. Уязвимость Docker Escape: побег из контейнера всё ещё возможен. Блог компании FirstVDS. https://habr.com/ru/company/first/blog/650553/ (доступ 21.12.2022).

14. Docker – Container Escape. Сайт Exploit Database. https://www.exploit-db.com/exploits/47147 (доступ 21.12.2022).

15. *Дмитрий Лазаренко*. Как жили до Kubernetes: сравниваем самый популярный оркестратор с другими решениями. https://mcs.mail.ru/blog/sravnenie-kubernetes-s-drugimi-resheniyami (доступ 27.01.2023).

16. Kubernetes Documentation. Concepts. Kubernetes Components. https://kubernetes.io/docs/home/ (доступ 21.12.2022)

17. How to security harden Kubernetes in 2022 // Cloud Native Computing Foundation URL: https://www.cncf.io/blog/2022/06/07/how-to-security-harden-kubernetes-in-2022/ (доступ 21.12.2022).

18. Initial access techniques in Kubernetes environments used by Kinsing malware // Microsoft Defender for Cloud Blog URL: https://techcommunity.microsoft.com/t5/microsoft-defender-for-cloud/initial-access-techniques-in-kubernetes-environments-used-by/ba-p/3697975 (доступ 21.12.2022).

19. Postgre SQL 15. Documentation. 21.4. Trust Authentication. https://www.postgresql.org/docs/current/auth-trust.html (доступ 21.12.2022).

ПОДХОД К ФОРМИРОВАНИЮ ИНДЕКСА ДЛЯ ОЦЕНКИ СТЕПЕНИ ГАРМОНИЗАЦИИ СУБЪЕКТОВ РОССИЙСКОЙ ФЕДЕРАЦИИ ПО УРОВНЮ РАЗВИТИЯ ЭЛЕКТРОСВЯЗИ/ИКТ С УЧЕТОМ РЕЗУЛЬТАТОВ ПК-22

Резникова Наталья Петровна,
ФГБУ НИИР, главный научный сотрудник, профессор, д.э.н., Москва, Россия,
reznikova.natalya1946@yandex.ru

Артемьева Галина Станиславовна,
Московский Технический Университет Связи и Информатики, доцент кафедры «Цифровая экономика, управление и бизнес-технологии», к.э.н., Москва, Россия,
artemieva-g-s@yandex.ru

Аннотация
Уровень развития электросвязи в регионах России влияет на решение многих задач Стратегии пространственного развития страны на период до 2025 г. Поставлен вопрос о возможности строить рейтинг регионов на основе индекса, структура которого соответствует концепции Стратегического плана МСЭ до 2027 гг.

Ключевые слова: *сбалансированное пространственное развитие, Субъект Российской Федерации/регион (СРФ), макрорегион, ЭИКТ, индекс, показатели/индикаторы, рейтинг СРФ/регионов, Международный союз электросвязи (МСЭ), Индекс развития ИКТ (IDI), индекс развития телекоммуникаций, методы сравнительной комплексной оценки, стратегический план, тематические приоритеты, национальная статистическая система.*

Введение

В стране стоит задача по сбалансированному пространственному развитию Российской Федерации. Для этого Минэкономразвития России разработана Стратегия пространственного развития Российской Федерации на период до 2025 года [1] (далее Стратегия), являющаяся одним из приоритетных направлений работы Правительства, и подготовлен План по ее реализации.

В качестве важнейшей цели Стратегии определено обеспечение устойчивого и сбалансированного пространственного развития РФ, направленного на:

– сокращение межрегиональных различий в уровне и качестве жизни населения;
– ускорение темпов экономического роста и технологического развития;
– обеспечение национальной безопасности страны.

При этом в [1] охарактеризованы основные тенденции, проблемы и вызовы, сформулированы цели, задачи, приоритеты и направления пространственного развития РФ, меры выполнения задач Стратегии, механизмы ее реализации, носящие общий характер и предполагающие разработку соответствующих инструментов, позволяющих осуществлять мониторинг и контроль ее исполнения.

Российская Федерация состоит из равноправных субъектов (СРФ) – республик, краёв, областей, городов федерального значения, автономных округов и автономной области. От сбалансированности уровня развития в СРФ инфраструктуры систем и средств связи, от их доступности, приемлемого в ценовом отношении использования, от компетенций пользователей зависит решение многих из перечисленных в Стратегии задач.

В качестве возможного инструмента, позволяющего проводить сопоставления регионов по уровню развития и использования электросвязи/ИКТ (ЭИКТ), являются разнообразные сводные индексы, широко использующиеся в настоящее время для решения разнообразных задач, которые вытекают из области их применения [2-7].

Разработанных в настоящее время индексов, имеющих отношение к электросвязи, цифровизации, информационному обществу и т.п., достаточно много. Но можно достаточно уверенно говорить о том, что на текущий момент отсутствует надежный и сравнительно простой индекс, с помощью которого можно было бы получать определенное представление о сравнительном уровне развития ЭИКТ в СРФ

(ранжировать их), что связано с трудностями формирования структуры такого индекса. И это – совершенно объективная ситуация.

Постановка проблемы формирования индекса для сопоставления уровня развития ЭИКТ в регионах/субъектах России (СРФ)

В силу разных причин, в зависимости от целей заказчика, решение проблем выбора структуры индекса и адекватного набора показателей для ее наполнения, обоснования методики его расчета и осуществления рейтинга сравниваемых объектов на его основе вызывает у разработчиков как методологические, статистические, организационные, так иные проблемы не только в нашей стране, но и на международном уровне.

Используемые в настоящее время для определения рейтингов сравниваемых объектов индексы, предложенные отечественными исследователями и разработчиками, по тем или иным причинам применимы, в основном, для анализа уровня развития цифровой экономики в целом, информационного общества и т.п. Но они не позволяют в полной мере выделить информацию в части оценки уровня развития именно телекоммуникационной отрасли (направление деятельности Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации).

Вместе с тем нужен индекс, который бы давал возможность лицу, принимающему решения (ЛПР)/регулятору:

– учитывать в комплексе различные аспекты/факторы влияния на уровень развития инфраструктуры систем и сетей связи, используемых для оказания услуг населению и потребителям из других сфер социально-экономической деятельности,

– проводить анализ и оценку влияния тех или иных факторов и вырабатывать управленческие решения с целью управления сбалансированным развитием телекоммуникационной отрасти в отдельных СРФ и в выделенных в Стратегии макрорегионах;

– давать представление об общем направлении развития отрасли, а не только о том, что уже достигнуто.

Для выбора подхода к формированию такого индекса можно будет обратиться к результатам работы МСЭ, которые ожидаются к концу 2023 г. во исполнение решений и поручений, которые содержатся в Резолюции 131 (Пересм. Бухарест, ПК 2022 г.) «Измерение информационно-коммуникационных технологий для построения объединяющего и открытого для всех информационного общества» [8]. Резолюция подчеркивает «насущную потребность в предоставлении результатов измерения доступа к электросвязи/ИКТ и их использования, с тем чтобы отслеживать использование ИКТ всеми гражданами во всех странах, с особым вниманием к жителям отдаленных районов». Среди прочего в Резолюции 131 также отмечается, что:

– технологические инновации, цифровизация, электросвязь/ИКТ обладают потенциалом для достижения Целей Устойчивого Развития, создают новые возможности, при этом содействуя краткосрочному и долгосрочному социально-экономическому развитию, а также росту цифровой экономики и построению открытого для всех информационного общества;

– миссия МСЭ, утвержденная в Резолюции 71 «Стратегический план МСЭ на 2024-2027 годы» (Пересм. Бухарест, 2022 г.), нацелена на содействие, упрощение и стимулирование приемлемого в ценовом отношении и универсального доступа к электросвязи/ИКТ;

– большое значение для измерения информационного общества и уровня цифрового разрыва при международных сопоставлениях имеют корзина цен на услуги ИКТ (IPB) и Индекс развития ИКТ (IDI) [8].

МСЭ, путем работы в рамках групп экспертов и проведения официальных консультаций с Государствами-Членами, должен принимать дальнейшие необходимые меры в целях разработки действенной структуры и методики для IDI, позволяющих публиковать IDI на ежегодной основе, при условии наличия достаточного объема достоверных данных по большинству Государств-Членов.

При этом решено, что структура и методика IDI будут действительны в течение четырехлетнего периода и что МСЭ следует установить критерии минимального объема данных, наличие которого необходимо для включения Государств-Членов в IDI. МСЭ следует проводить консультации с Государствами-Членами, не соответствующими этим критериям, с тем чтобы получить их согласие относительно предлагаемых методов дополнения данных, в том числе за счет других источников или оценок, в целях их включения в IDI [9-11].

Подчеркнуто также, что с целью обеспечения государственных директивных органов каждого Государства-Члена надлежащей информацией МСЭ должен продолжать стремиться:

– собирать и периодически публиковать разного рода статистические данные в области ЭИКТ, которые дают определенное представление о степени прогресса и о распространении услуг ЭИКТ в различных регионах мира;

– обеспечить, по мере возможности, полное соответствие политики и стратегии Союза постоянно меняющейся среде электросвязи, а также соответствие между показателями, характеризующими развитие ЭИКТ и целевыми показателями деятельности МСЭ, сформулированными в Стратегическом плане МСЭ на 2024-2027 годы;

– укреплять сотрудничество с другими международными организациями, занятыми сбором связанных с электросвязью/ИКТ статистических данных, и по мере необходимости обновлять стандартизированный набор показателей, повышающий качество, сопоставимость, доступность и надежность данных и показателей в области электросвязи/ИКТ, а также способствующий разработке стратегий и государственной политики на национальном, региональном и международном уровнях в области электросвязи/ИКТ;

– предпринимать соответствующие шаги для того, чтобы данные и материалы МСЭ при их использовании содержали надлежащие ссылки на источник.

Отмеченные выше положения в Резолюции 131 следует учитывать исследователям, которые в дальнейшем будут или могут разрабатывать индекс, не только отражающий прошлое состояние российских ЭИКТ, но соответствующий вновь возникающим условиям. Здесь существенную роль могут сыграть концепция формирования стратегического плана МСЭ и показатели, предложенные на уровне стратегического плана (СП МСЭ), которые нашли отражение в Резолюции 71 «Стратегический план МСЭ на 2024-2027 годы» (Пересм. Бухарест, 2022 г.) [8-10].

Возможный подход к формированию концепции индекса ЭИКТ

Индекс для оценки уровня развития ЭИКТ должен работать «на упреждение», т.е. его показатели следует соотносить с целями развития ЭИКТ в регионах. Что в этом смысле может дать Резолюция 71?

Резолюция 71 является системообразующей, так как содержащиеся в ней вопросы отражают направления стратегического развития МСЭ в четырехлетнем периоде и могут влиять на выбор направлений развития национальной системы ЭИКТ. Любой СРФ также имеет планы стратегического развития, в том числе – сферы ЭИКТ.

На ПК-22 представлена концептуально новая версия (по сравнению с 2018 г.) структуры Стратегического плана (СП). К основному тексту Резолюции 71 (с обоснованиями и поручениями) прилагаются три Приложения, являющиеся ее неотъемлемой частью. В Резолюции 71 представлен структурированный, четкий и ориентированный на цели СП МСЭ на 2024-2027 гг. В нем основное внимание уделяется двум стратегическим целям – «Универсальная возможность установления соединений» и «Устойчивая цифровая трансформация». Он включает пять Тематических приоритетов (ТП), связанных с целями, а также ключевые предлагаемые продукты и услуги МСЭ и общие средства достижения целей.

С нашей точки зрения, Резолюция 71 дает методологический подход для сравнительного сопоставления уровня развития ЭИКТ в СРФ путем формирования соответствующего индекса.

На рисунке 1 показана интерпретированная для дальнейшего использования общая схема Стратегического плана МСЭ на период 2024-2027 гг. и такие его ключевые компоненты, как стратегические цели и целевые показатели, тематические приоритеты (ТП) и конечные результаты, предлагаемые продукты и услуги, а также − средства достижения целей.

Органы, регулирующие развитие электросвязи/ИКТ в регионах РФ, в перспективе могут, в принципе, ставить перед собой стратегические цели, аналогичные тем, которые стоят перед сферой электросвязи/ИКТ в мире, и формулировать аналогичные ключевые компоненты стратегического плана, что и в СП МСЭ. Поэтому можно строить индекс для оценки уровня развития ЭИКТ на основе структуры и показателей СП МСЭ.

В свою очередь, это в дальнейшем может помочь адаптировать структуру индекса к новым характеристикам сферы ЭИКТ и условиям в Российских регионах, обеспечивая улучшенное представление о степени прогресса и о распространении услуг электросвязи/ИКТ в различных СРФ и возможность формировать новые требования к национальной статистике в сфере ЭИКТ, в том числе, необходимой для участия РФ в международных сопоставлениях на основе обновленного IDI.

Кроме того, при условии, что в МСЭ будет разработана приемлемая методика дополнения данных, отсутствующих в национальной статистике ГЧ, ее можно будет использовать, с тем чтобы получить

согласие ЛПР относительно использования предлагаемых показателей, числовые значения которых отсутствуют в национальной статистике, но могут быть получены из других источников или оценок, в целях их включения в индекс (или в IDI).

ТП, охарактеризованные в СП МСЭ, являются теми областями работы, которым ЛПР должен уделять основное внимание, и в ходе осуществления которых могут быть получены конечные результаты для достижения стратегических целей в области использования и развития сферы ЭИКТ СРФ.

Показатели, используемые для измерения ТП, приведены в [8]. Конечно, не все они могут быть использованы в настоящее время на уровне СРФ, но в будущем, по мере необходимости, могут находить отражение в национальной статистической системе.

Например, в настоящее время отсутствует возможность измерять «некоторые из форм альтернативных процедур вызова, которые используются для направления голосового трафика в обход стандартных международных механизмов осуществления и оплаты вызовов, широко используются на рынках электросвязи/информационно-коммуникационных технологий (ИКТ)», как показано в Резолюции 21 (Пересм. Бухарест, 2022 г.) «Меры, относящиеся к альтернативным процедурам вызова в сетях международной электросвязи». Эта проблема требует решения, так как: «…альтернативные процедуры вызова преобразовали экономические системы как развитых, так и развивающихся стран, и в этой области необходимо сотрудничество с участием многих Государств-Членов и Членов Секторов, которое следует настоятельно рекомендовать». Одним из элементов этого решения может стать соответствующий показатель и методика его измерения.

Далее, в дальнейшем можно ставить вопросы о необходимости и целесообразности учета в индексах показателей, измеряющих: характеристики эксплуатационных аспектов взаимодействия традиционных сетей электросвязи и вновь создаваемых и появляющихся архитектур, возможностей, технологий, приложений и услуг электросвязи/ИКТ; темпы и размеры ускорения инвестиций в разработку и масштабирование инновационных и технологических решений самых острых проблем, с которыми сталкиваются наименее развитые регионы и преодоление которых способствует их переходу к цифровым технологиям и активизации усилий по преодолению цифрового разрыва.

При объективной ограниченности возможностей любого индекса в полной мере отражать уровень развития электросвязи/ИКТ, они способствуют рассмотрению состояния электросвязи/ИКТ в СРФ, нуждающихся в особых мерах для развития электросвязи/ИКТ, позволяют выявить области с самым сильным отставанием, требующие приоритетных мер, способствующих экономическому росту и развитию электросвязи/ИКТ.

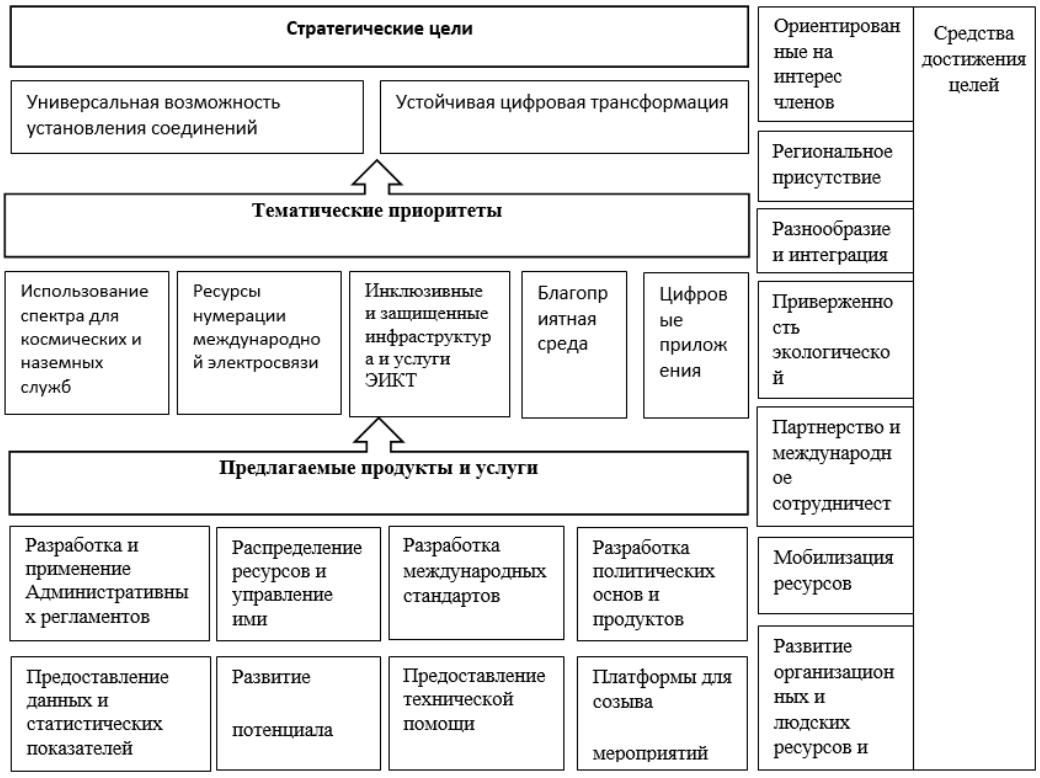

Рис. 1. Схема Стратегического плана МСЭ

В соответствии с информацией, представленной на рисунке 1, можно будет, в принципе, сформировать индекс со следующей структурой, представленной на рисунке 2:

0. Название индекса
1. Субиндексы первого уровня: отражают стратегические цели сравниваемых объектов (в данном случае – названия субиндексов не обсуждаются). Но тогда, следует иметь ввиду, что, хотя цели МСЭ, имеющие отношение ко всем Государствам-Членам, носят универсальный характер, на страновом уровне они могут иметь разные формулировки у каждого из СРФ. Этот методологический разрыв преодолим, например, если в качестве целей выбраны цели национальной программы в области электросвязи/ИКТ.
2. Субиндексы второго уровня могут иметь общее название для всех сравниваемых объектов – тематические приоритеты, но здесь возникает проблема отнесения тех или иных ТП к субиндексам первого уровня. В силу взаимосвязанности сетей, технологий и услуг, такая структуризация будет всегда достаточно условной.
3. Субиндексы третьего уровня (при необходимости создания), также, как и субиндексы второго уровня, могут иметь общее название – Предлагаемы продукты и услуг (ПиУ), но и здесь возникает аналогичная проблема отнесения тех или иных ПиУ к субиндексам второго уровня.
4. Показатели/индикаторы, отнесенные к каждому типу ПиУ.

Отдельные элементы средств достижения целей тоже могут быть включены в индекс.

Рис. 2. Возможная структура индекса

Выводы и предложения

Сказать априори, будет ли такой индекс адекватным, эффективным и не требующим чрезмерных ресурсов для его расчетов и формирования соответствующих рейтингов, трудно. Но уже сейчас ясно, что потребуется нормирование всех показателей индекса, что в плане расчетов не вызывает проблем (используются возможности модификаций метода комплексного сравнительного анализа). Вместе с тем, сохранятся другие вопросы: наличие обоснованных нормативов для выбора эталонного значения каждого из показателей; правильное отнесение показателей к группам стимуляторов/дестимуляторов и субиндексам; полноты статистических данных на основе прозрачных и доступных методов исчисления показателей; формирования обоснованной оценки значимости показателей и субиндексов, что возможно делать, например, с помощью метода анализа иерархий (МАИ), но требует значительных затрат времени на осуществление экспертизы.

1. Как показывают наши исследования, основная проблема – выбор структуры индекса, т.е. его субиндексов и показателей. Возможные риски, связанные с любыми показателями:

2. Расчеты индекса должны осуществляться системно (для всех регионов России) в организации по выбору заказчика, как это делается для любых других индексов, в том числе в МСЭ для всех Государств-Членов.

3. Выбор метода расчета индекса (следовательно, и определения рейтинга) зависит от наличия или отсутствия таких показателей в индексе, для которых существуют нормативы.

4. Изменение набора показателей в Индексе может привести к изменению рейтинга регионов, но незначительному, в пределах статистической погрешности, так как, в конечном итоге, все определяется спросом и предложением на телекоммуникационных рынках особенностями этих рынков.

5. Если есть уникальные регионы с явно лучшими (например, Москва) или худшими показателями, чем у остальных регионов, то лучше их исключать из общего рейтинга, так как с точки зрения методологии никакой дополнительной информации не будет получено: они займут первые или последние места. Кроме того, сильно исказят базу для сравнения.

6. Проблему также может создавать отсутствие официальных статистических данных по ряду показателей в регионе (нулевые значения показателей). Включение нулевых значений показателей в общий расчет может существенно искажать рейтинговую картину. В этом случае отдельно следует разбирать ситуацию с причинами отсутствия статистических данных по каждому из регионов.

7. При отсутствии нормативов для абсолютных значений показателей можно/следует расчетным путем устанавливать удельные значения показателей. Но тогда возникает вопрос о выборе делителя, что также может приводить к изменению значений индекса и положения регионов в рейтинге.

8. Хотя, как уже отмечалось, при выборе показателей для включения в индекс следует опираться на данные официальной национальной статистки, возможно, в дальнейшем потребуются и новые показатели, отсутствующие в официальной статистике на момент проведения исследований и разработки индекса. При этом исключается возможность искаженного представления данных.

Концепция СП МСЭ дает методологическую основу/возможность избегать хотя бы частично эти риски и строить индекс для оценки развития ЭИКТ в регионах России в расчете на перспективу.

Литература

1. Распоряжение Правительства РФ от 13.02.2019 N 207-р (ред. от 30.09.2022) «Об утверждении Стратегии пространственного развития Российской Федерации на период до 2025 года» https://www.consultant.ru/document/cons_doc_LAW_318094/?ysclid=laxpfokdo3913736861 (дата обращения: 15.10.2022 г.).

2. *Резникова Н.П., Артемьева Г.С., Калюга Д.В.* Роль МСЭ в развитии потенциала в области статистики электросвязи/ИКТ. Нерешенные проблемы. Часть I // Электросвязь. 2019. № 2. С. 18-22.

3. *Резникова Н.П., Артемьева Г.С., Калюга Д.В.* Роль МСЭ в развитии потенциала в области статистики электросвязи/ИКТ. Нерешенные проблемы. Часть II // Электросвязь. 2019. № 4. С. 14-19.

4. *Резникова Н.П., Артемьева Г.С., Калюга Д.В*. О подходах к расчету индекса развития электросвязи/ИКТ (IDI) для повышения значимости международных сопоставлений стран // Труды НИИР. 2019. № 1. С. 55-62.

5. *Резникова Н.П., Артемьева Г.С., Калюга Д.В*. Новый индекс МСЭ и Индекс развития ИКТ (IDI): к вопросу о преодолении противоречий // Труды НИИР. 2020. № 3. С. 60-66.

6. *Резникова Н.П., Артемьева Г.С., Калюга Д.В*. Роль гармонизации деятельности по повышению рейтинга России при международных статистических сопоставлениях в сфере электросвязи/ИКТ // Электросвязь. 2020. № 6. С. 46-50.

7. *Резникова Н.П., Артемьева Г.С., Калюга Д.В*. К вопросу о путях повышения места России в рейтинге по Индексу развития ИКТ (IDI) // Технологии информационного общества: сборник трудов XIV Международной отраслевой научно-технической конференции. 2020. С. 376-378.

8. Международный союз электросвязи. Заключительные акты Полномочной конференции (Бухарест, 2022 г.). Решения и Резолюции https://www.itu.int/dms_ties/itu-s/md/22/pp/c/S22-PP-C-0202!!PDF-R.pdf (дата обращения: 28.11.2022 г.).

9. *Резникова Н.П., Артемьева Г.С*. Особенности современного этапа жизненного цикла Международного союза электросвязи // Электросвязь. 2022. № 8. С. 32-38.

10. *Резникова Н.П., Артемьева Г.С*. Подход к обоснованию стратегических направлений развития МСЭ на период 2024-2027 гг. с использованием SWOT-анализа // Электросвязь. 2022. № 2. С. 12-19.

11. *Резникова Н.П., Артемьева Г.С., Калюга Д.В.* Роль и результаты анализа вкладов на Совет МСЭ для выявления приоритетов в позициях Государств-Членов при подготовке к ПК-22 // REDS: Телекоммуникационные устройства и системы. 2022. Т. 12. № 1. С. 44-50.

ИССЛЕДОВАНИЕ СОВМЕСТНОЙ РАБОТЫ СИСТЕМ РАСПРЕДЕЛЕННОГО РЕЕСТРА И СИСТЕМЫ ИНТЕРНЕТА ВЕЩЕЙ С ТОЧКИ ЗРЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Эйнман Анастасия Дмитриевна,
Московский Технический Университет Связи и Информатики, студент, Москва, Россия

Панков Константин Николаевич,
Московский Технический Университет Связи и Информатики, доцент кафедры «Информационная безопасность», к.ф.-м.н., Москва, Россия
pankov_kn@mtuci.ru

Аннотация
Работа посвящена актуальной теме – обеспечению информационной безопасности работы системы распределенного реестра в системе Интернета вещей, охватывающей концепцию взаимодействия устройств, принадлежащих разным отделам информационной системы. В работе рассматривается сеть с использованием различных сервисов интернета вещей в децентрализованной распределенной архитектуре. Приведены преимущества использования блокчейна в системе интернета вещей.

Ключевые слова: *Интернет вещей, система распределенного реестра, СРР, блокчейн, информационная безопасность, взаимодействие СРР и интернета вещей*

Введение

Понятие интернета вещей (Internet of Things или IoT) связано с интеграцией ограниченных по ресурсным и вычислительным возможностям устройств с поддержкой интернет-протоколов (IP) в существующую инфраструктуру Интернета. Системы интернета вещей, которые в соответствии с [1] тесно связаны со «сквозной» цифровой технологией «Новые производственные технологии», развертываются все чаще, но разработка общепринятых стандартов для регулирования системы «Интернет вещей» является сложным процессом.

В частности, вопросы информационной безопасности подобных систем, такие как авторизация, проверка и контроль доступа, в настоящее время далеки от полного решения. Обычно требуется подключение, согласованная работа и управление распределенным количеством интеллектуальных устройств, которым необходимо идентифицировать и доверять друг другу.

Перспективной децентрализованной платформой для «Интернет вещей» является система распределенных реестров (далее – СРР). Его структура данных состоит из связанных блоков данных, где одноранговые узлы в СРР транслируют блоки, используя криптографию с открытым ключом. Использование СРР для обеспечения информационной безопасности интернета вещей уже рассматривалось в [1].

На данный момент, услуги сервиса работают за счет комбинации сетевых устройств. Безопасность сети, а именно: хранение, обработка, передача конфиденциальной информации осуществляется за счет сложной архитектуры сетевых устройств, таких как маршрутизаторы, коммутаторы, криптошлюзы, межсетевые экраны, средства обнаружения вторжений и т.д.

В данной работе исследуется концепция взаимодействия устройств, принадлежащих разным отделам информационной системы за счет совместной работы СРР и системы «Интернет вещей».

Система распределенных реестров

Одним из инструментов обеспечения информационной безопасности систем различных государственных и коммерческих структур является технология СРР [2] вообще и технология цепной записи данных (блокчейн), как вариант реализации сети распределенных реестров, в частности. В силу уже сложившихся представлений в экспертном сообществе, отразившихся в принятой в конце 2019 года Дорожной карте развития СРР, можно использовать термины СРР и блокчейн (как это делают ряд западных и отечественных исследователей) в качестве синонимов [3].

В 2008 году один или несколько анонимных разработчиков по имени Сатоши Накомото объединили криптографию с открытым и закрытым ключом, цифровую подпись и одноранговые технологии для создания новой распределенной базы данных, которая стала известна как блокчейн [4]. Технология блокчейн получила свое развитие и нашла применения во многих приложениях помимо криптовалют.

В 2013 году Виталий Бутерин начал разработку новой вычислительной платформы на основе блокчейна под названием Ethereum [5].

Главным нововведением стало появление смарт-контрактов. Смарт-контракт – это компьютерная программа, которая отслеживает и обеспечивает исполнение обязательств. Такие программы размещаются и подписываются в системах распределенного реестра и могут использоваться для осуществления транзакции без привлечения посторонних лиц при соблюдении определенных условий. Использование данных программ как транзакций дает возможность рассматривать блокчейн как децентрализованный компьютер. СРР имеет основные характеристики децентрализации и безопасности. Цепочка блоков – это цепочка данных, которые содержат определенную информацию, безопасным и подлинным образом сгруппированная вместе. Другими словами, СРР – это комбинация компьютеров, (если компьютеры выступают в качестве устройств хранения данных) связанных друг с другом, а не с центральным сервером, что означает, что вся сеть децентрализован. Наиболее важным атрибутом СРР является возможность обновления цепочки лишь с общего согласия всех узлов системы, в этом заключается позитивная сторона децентрализации. В такой системе отсутствует какой-либо центральный орган, который бы отвечал за обновление реестра. Любое изменение или обновление системы строго контролируется, отслеживается и осуществляется только после достижения общего консенсуса между всеми участниками (узлами) сети. Достижение согласования осуществляется за счет одобрения всех узлов системы.

Рассмотрим элементы СРР, в обобщенном виде структуру системы можно изобразить так, как представлено на рисунке 1.

Рис. 1. Элементы СРР

Рассмотрим в обобщенном виде создание блоков, их связь с соседними блоками и транзакциями. Узел создает первоначальную транзакцию, подкрепляет ее цифровой подписью, используя закрытый ключ. Транзакция в СРР означает любое действие, который может совершить узел системы. Каждый блок содержит определенный набор данных и состоит из двух основных частей: «головная часть» содержит следующую информацию: номер версии, код целостности [6] или хеш предыдущего блока, хеш всех транзакций в текущем блоке, метка времени, означающую дату создания текущего блока. «Полезная нагрузка» включает список всех транзакций, которые должны содержаться в данном блоке и попасть в СРР. С установленной частотой каждый участник сети случайным образом выбирает другого соседнего участника и передаёт тому обновлённую информацию. После проверки транзакции несколькими узлами, данная транзакция включается в блок и считается подтвержденной. Созданный блок становится частью СРР, последующий блок будет уже криптографически привязан к данному блоку. Такая связь называется «указателем хеша». Если попытаться изменить какой-либо хеш блока, соседний блок автоматически заметит данное изменение [7].

Система «Интернет-Вещей»

Интернет вещей (IoT) – это концепция сети передачи данных между физическими объектами («вещами»), оснащёнными встроенными средствами и технологиями для взаимодействия друг с другом или с внешней средой [8].

Устройствами технологии являются: датчики, снаряжение, оружие (в случае военного интернета вещей), транспортные средства, роботы, электроника. Устройства способные регистрировать информацию, обрабатывать, анализировать и выполнять операции, оказывать воздействие и быть полезными в бою. Решая широкий круг задач при взаимодействии друг с другом и людьми, устройства станут непрерывно координировать и согласовывать свои действия, выполняя задания.

Для успешной работы таких устройств, должны быть соблюдены ряд задач: обеспечение быстрой связи между вещами среди изменяющихся условий. Для этого должно быть организованно успешное управление большим количеством мобильных устройств и каналов. Работа людей должна быть минимизирована, то есть адаптация устройств и управление должно происходить автономно. Управление в больших потоках информации, генерируемой «Интернет вещей». Технология должна уметь работать с минимальными перебоями, извлекать пользу из большого массива данных с учетом меняющихся условий [8].

Перспективной платформой для «Интернет вещей» являются CPP. Их структуры данных состоят из связанных блоков данных, где одноранговые узлы в CPP транслируют блоки, используя асимметричную криптографию.

Когда дело доходит до «Интернет вещей», CPP может использоваться для хранения критически важных межмашинных коммуникаций, отправляемых в виде транзакций CPP, обеспечивая подотчетность и безопасность хранимых данных. Он также может предоставить идентификационные данные и подтверждение происхождения устройств с помощью своих криптографических функций. Одна из самых больших проблем при интеграции CPP в систему «Интернет вещей» — это масштабируемость. Фактически, из-за огромного количества устройств и ограничений ресурсов развертывание CPP в IoT является особенно сложной задачей. Оптимальная архитектура CPP должна масштабироваться на многие устройства «Интернет вещей» (они становятся одноранговым узлами в сети CPP), и должны иметь возможность обрабатывать высокую пропускную способность транзакций.

Безопасность является критическим параметром в системе «Интернет вещей». Проблема целостности данных для устройств IoT является важной проблемой, которую необходимо решать. В то время как целостность данных по замыслу обеспечивается доказательством работы.

Доказательство работы (Proof of Work или PoW) – это определенные действия в системе, которые выполняют пользователи для подтверждения и добавления новой транзакции, в свою очередь майнер должен выполнить некоторые предопределенные действия, которые часто представляют собой математическую головоломку или задачу, которую трудно вычислить, но легко проверить. PoW запрашивается для каждой проверки блока. Сложность математической задачи может быть адаптирована в зависимости от времени необходимого для проверки блока и для вычислений мощности [9].

С одной стороны, PoW имеет преимущество в защите транзакций и блоков от изменения, поскольку злоумышленнику необходимо проверить все свои поддельные запросы и изменить часть блоков цепочки, чтобы предоставить новый PoW для каждого измененного блока, а также как обновление его версии цепочки на всех узлах, что требует огромных вычислительных мощностей и энергии.

Исследование совместной работы CPP и системы «Интернет-вещей»

Исследованием совместной работы системы распределенных реестров и системы «Интернет Вещей» является возможность показать альтернативу существующим защищённым средам передачи данных в информационных системах.

Популярные методы построения защищенных сетей передачи данных основываются на архитектуре программно-аппаратных комплексов.

Совместная работа двух систем, описанных в предыдущих разделах работы, позволяют осуществить передачу конфиденциальной информации с одного устройства на другое, находящиеся в разных сетях, минуя возможность получения доступа для злоумышленника. Система может быть построена как на частной CPP, так и на публичной, разница заключается в масштабируемости системы. В публичном CPP информацией могут обмениваться только предопределенные пользователи, это в свою очередь уменьшает гибкость системы. В другом случае можно использовать публичный блокчейн, реализующий смарт-контракты [10].

Каждое совершенное действие в системе, а также отправленное сообщение фиксируется в CPP в виде транзакции.

В каждой отдельной сети системы выбирается главный участник сети, который владеет парой закрытого-открытого ключей. Остальные пользователи сети генерируют пару ключей с помощью криптографического алгоритма на эллиптических кривых ECC, помимо этого пользователи получают сертификат, состоящий из идентификатора сети, который показывает, к какой сети принадлежит пользователь, идентификатор пользователя, публичный адрес пользователя – представляет собой код целостности открытого ключа пользователя, а также цифровую подпись пользователя с использованием секретного ключа главного пользователя сети. Подпись пользователя включает код идентификатора сети, идентификатора пользователя, публичный адрес [11].

Далее рассмотрим алгоритм работы СРР и системы «интернет вещей», представленный на рисунке 2.

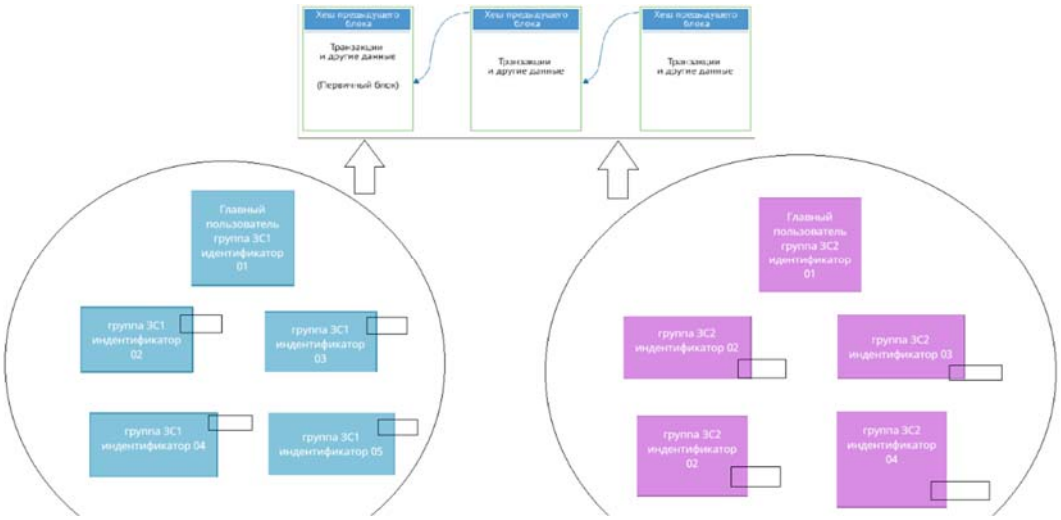

Рис. 2. Алгоритм работы СРР и системы «интернет вещей»

Первым этапом выбирается главный пользователь, который присваивает идентификатор сети, а также подписывает сертификат каждого пользователя. Далее главному пользователю необходимо отправить первую транзакцию в СРР, чтобы объявить о своей сети. В зависимости от количества подсетей, СРР проверяет их уникальность и добавляет транзакции. После этого каждый пользователь своей сети инициирует себя в системе, для этого необходимо отправить транзакцию в блокчейн, чтобы связать себя с сетью. На уровне блокчейна работает смарт-контракт, который проверяет уникальность идентификатора пользователя, срок действия сертификата с использованием открытого ключа главного пользователя своей подсети. Если хотя бы одно из условий не выполняется – пользователь не может быть авторизован в сети. После успешной регистрации в подсети – для дальнейшей отправки сообщений не нужно использовать сертификат пользователя.

На рисунке 3 рассмотрим взаимодействие СРР и системы «Интернет Вещей».

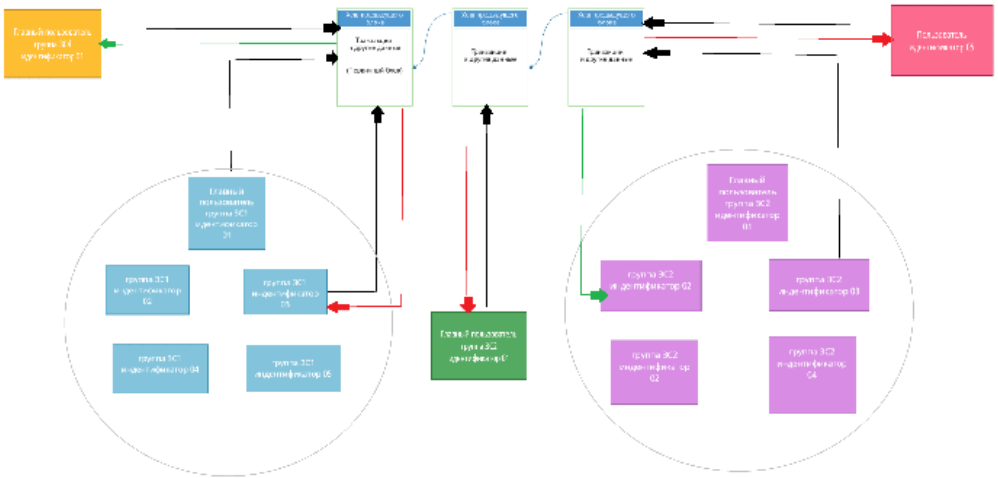

Рис. 3. Взаимодействие СРР и системы «Интернет Вещей»

– Передача сообщений осуществляется только в своей подсети. Пользователь 03 в сети ЗС2 отправляет сообщение пользователю 02. Блокчейн обрабатывает транзакцию и доставляет сообщение.

– Пользователь с идентификатором 03 подсети ЗС1 пытается отправить сообщение вне своей сети – блокчейн отклоняет транзакцию.

– Регистрировать новую подсеть может только главный пользователь данной подсети.

– Подсеть должна быть уникальной, иначе блокчейн отклонит транзакцию.

– Сторонний пользователь, который не является членом ни одной из зарегистрированных сетей в блокчейне не может отправлять сообщения другим пользователям.

Заметим, что в связи с использованием СРР в системах интернета вещей, которые могут быть критически важны, к примеру, в промышленном интернете вещей становится особенно актульаной задача тестирования верификации и валидации блокчейн-систем [12-14] как отдельного инструмента обеспечения информационной безопасности.

Заключение

Говоря о совместной работе систем распределенных реестров с системой интернет вещей можно выделить следующие преимущества:

– Децентрализация системы

– Блокчейн устойчив к изменению данных, таким образом данные надежно хранятся в системе.

– Существует множество открытых и доступных блокчейн систем, таких как Эфириум и Биткоин.

– Публичные блокчейны автономны в собственном функционировании.

– Неизменность смарт-контракта после подтверждения.

– Масштабируемость системы при использовании публичных блокчейн систем.

Данный подход передачи данных может интегрироваться в большинство систем с IoT устройствами, данный подход обеспечивает легкую интеграцию новых устройств и варианты использования.

В данном исследовании рассматривается сеть с использованием различных сервисов IoT в децентрализованной распределенной архитектуре. Каждая вещь сети общается с большим количеством других вещей.

В наши дни большое количество умных вещей в сети увеличивает риск включения скомпрометированных устройств. Кроме того, существующие устройства относятся к разнородным типам и не имеют один и тот же вариант использования. Сетевая функция заключается только в пересылке пакетов и не дает никаких гарантий безопасности, таких как как целостность или аутентификация. Таким образом, злоумышленник может скомпрометировать данные. Использование технологии Систем распределённых реестров обеспечивает гарантии пересылки сообщений без компрометации данных.

Литература

1. *Панков К.Н., Эйнман А.Д.* Исследование технологии системы распределенного реестра в системе промышленного Интернета вещей с точки зрения информационной безопасности // Системы синхронизации, формирования и обработки сигналов. 2022. Т. 13. № 2. С. 33-40.

2. *Колесников П., Бекетнова Ю., Крылов Г.* Технология блокчейн. Анализ атак, стратегии защиты. Саарбрюккен, LAP LAMBERT Academic Publ., 2017. 76 с.

3. Дорожная карта развития «сквозной» цифровой технологии «Системы распределенного реестра» // Электрон. дан. Заглавие с экрана. Режим доступа: https://digital.gov.ru/uploaded/files/07102019srr.pdf

4. *Nakamoto S.* Bitcoin: A Peer-to-Peer Electronic Cash System, 2008 // Электрон. дан. – Заглавие с экрана. – Режим доступа: https://bitcoin.org/bitcoin.pdf.

5. *Антонопулос А.М., Вуд Г.* Осваиваем Ethereum: создание смарт-контрактов и децентрализованных приложений. М.: ЭКСМО, 2021, 512 с.

6. *Лось А.Б, Нестеренко А.Ю., Рожков М.И.* Криптографические методы защиты информации: учебник для академического бакалавриата. 2-е изд., испр. М.: Юрайт, 2016. 473 с.

7. *Панков К.Н., Эйнман А.Д.* Сертификация систем распределенного реестра как инструмент обеспечения информационной безопасности // REDS: Телекоммуникационные устройства и системы. 2021. Т. 11. № 2. С. 37-49.

8. *Ли П.* Архитектура интернета вещей. М.: ДМК-Пресс, 2019. 455 с.

9. *Biryukov A. Khovratovich D.* Equihash: Asymmetric Proof-of-Work Based on the Generalized Birthday Problem // Ledger, no. 2, 2016, pp. 1-30.

10. *Башир И.* Блокчейн: архитектура, криптовалюты, инструменты разработки, смарт-контракты. М.: ДМК-Пресс, 2019. 538 с.

11. *Yeh H.-L., Chen T.-H., Liu P.-C., Kim T.-H., Wei H.-W*. A secured authentication protocol for wireless sensor networks using elliptic curves cryptography // Sensors, no. 11(5), 2011, pp. 4767-4779.

12. *Pankov K.N.* Testing, Verification and Validation of Distributed Ledger Systems // 2020 Systems of Signals Generating and Processing in the Field of on Board Communications, Moscow, 19-20 марта 2020 г. P. 9078541.

13. *Панков К.Н*. Оценки мощности классов отображений, применяемых в протоколах квантового распределения ключей // Наукоемкие технологии в космических исследованиях Земли. 2022. Т. 14. № 4. С. 4-18.

14. *Миронов Ю.Б., Казанцев С.Ю., Шаховой Р.А., Колесников О.В., Машковцева Л.С., Зайцев А.И., Коробов А.В.* Анализ перспектив развития источников одиночных фотонов в системах квантового распределения ключей // Наукоемкие технологии в космических исследованиях Земли. 2021. Т. 13. № 6. С. 22-33.

ФОРМИРОВАНИЕ ИМПЕДАНСНЫХ СВОЙСТВ ЦИЛИНДРИЧЕСКОЙ КОНСТРУКЦИИ ЗА СЧЕТ ИЗМЕНЕНИЯ ЕЕ ГЕОМЕТРИЧЕСКИХ ПАРАМЕТРОВ ПОПЕРЕЧНОГО СЕЧЕНИЯ

Сухопаров Павел Евгеньевич,
Краснодарское высшее военное авиационное училище лётчиков имени Героя Советского Союза А.К. Серова, Краснодар, Россия

Романенко Владимир Александрович,
Краснодарское высшее военное авиационное училище лётчиков имени Героя Советского Союза А.К. Серова, Краснодар, Россия

Юхнов Василий Иванович,
Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО «Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия

Аннотация
В статье рассмотрен один из типов структур, позволяющих реализовать импедансные граничные условия. Проведены исследования взаимосвязи геометрических параметров структуры и достигаемого значения поверхностного импеданса.

Ключевые слова: *цилиндрическая антенна, поверхностный импеданс, диаграмма направленности, ряд Фурье.*

Введение

На современном этапе развития антенной техники в условиях постоянного ее усложнения становится актуальной задача реализации импедансных свойств поверхностей и управления их характеристиками для цилиндрических антенн. Импедансные граничные условия, с помощью которых можно добиться заданных характеристик излучения и согласования, можно получить на металлических цилиндрах со слоем магнитодиэлектрика, с использованием высокоимпедансных, а также гофрированных структур [1, 2]. Однако применение радиопоглощающих покрытий приводит к увеличению веса самой антенны, что является немаловажным фактором при применении таких антеннах на мобильных объектах, например, самолетах, автомобилях, антеннах базовых станций. Также можно отметить, что при моделировании антенн с радиопоглощающими покрытиями можно столкнуться с отсутствием эффективных в вычислительном плане электродинамических моделей структуры электромагнитного поля вблизи покрытия, позволяющих изменять вид и характеристики покрытия.

В то же время реализовать импедансные граничные условия можно с помощью звездного контура, обеспечивающего данные свойства для поверхности идеально проводящего кругового цилиндра. Решение данного вопроса возможно путем использования численно-аналитических методов, позволяющих наряду с обеспечением приемлемых вычислительных затрат учитывать и физические свойства объектов исследования. Основой таких методов может служить использование -2π – периодичности спектрального представления возбуждаемых полей.

Рассмотрим бесконечный вдоль образующей идеально проводящий цилиндр, с поперечным сечением, контур которого описывается соотношением (1). Данный цилиндр возбуждается электрическим диполем с электрическим моментом zI_0l.

$$R(\varphi) = R_0 + \Delta R \cos(N\varphi), \quad (1)$$

В соотношении (1) R_0, ΔR, N – геометрические параметры звездообразного контура, определяющие радиус, глубину канавки, и количество вершин соответственно. Геометрия задачи приведена на рисунке 1.

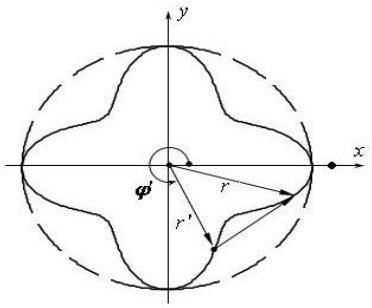

Рис. 1

С использованием спектрального представления выражение для z -компоненты полного поля имеет вид [3]:

$$E_z = -\frac{iW_0}{k}\int_{-\infty}^{\infty}\beta^2\exp(-ih|z-z_0|)\left\{I_0 lH_0^{(2)}(\beta r)+\int_L j_z^{sc}(\beta x',\beta y')H_0^{(2)}(\beta r')dx'dy'\right\}dh, \quad (2)$$

где $j_z^{sc}(\cdot)$ – плотность поверхностного тока, возбуждаемого на цилиндре; $H_0^{(2)}(\cdot)$ - функция Ганкеля 2-го рода нулевого порядка; $\beta^2 = h^2 - k^2$; k – волновое число свободного пространства.

Функция Ганкеля отраженного поля по углу φ является периодической с периодом 2π. Следовательно, её можно разложить в ряд Фурье по тригонометрическим функциям:

$$H_0^{(2)}(\beta r') = \sum_{k=1}^{\infty}(C_k\cos(k\varphi)+D_k\sin(k\varphi)). \quad (3)$$

Аргумент функции Ганкеля отраженного поля можно представить в виде:

$$\beta r = \beta\sqrt{(\rho(\varphi)\cos\varphi-\rho(\varphi'\cos\varphi'))^2+(\rho(\varphi)\sin\varphi-\rho(\varphi')\sin\varphi')^2}, \quad (4)$$

где $\rho(\varphi),\rho(\varphi')$ – расстояние до излучателя и точки излучения соответственно.

Из выражения (4) видно, что аргумент зависит от двух переменных φ и φ', и так как координаты точки наблюдения являются 2π – периодическими функциями по углу φ', то коэффициенты C_k, D_k также можно разложить в ряд Фурье:

$$C_k = \sum_{m=0}^{\infty}N_m^k\cos(m\varphi')+M_m^k\sin(m\varphi'),$$
$$D_k = \sum_{m=0}^{\infty}P_n^k\cos(m\varphi')+Q_n^k\sin(m\varphi'). \quad (5)$$

Аналогично, раскладывая в ряд Фурье падающее поле и ток на поверхности цилиндра, получаем:

$$I_0 lH_0^{(2)}(\beta r) = \sum_{q=0}^{\infty}S_q\cos(q\varphi)+R_q\sin(q\varphi),$$
$$j_z^{sc} = \sum_{l=0}^{\infty}A_l\cos(l\varphi')+B_l\sin(l\varphi'). \quad (6)$$

Подставляя выражения (5), (6) в соотношение (2) получаем интегральное выражение с двумя неизвестными коэффициентами A_l, B_l, которое позволяет свести решение данного интегрального уравнения к системе (7) линейных алгебраических уравнений:

$$\begin{cases} I_0 l S_t = -\sum_{m=0}^{\infty} (\pi A_m N_m^t + \pi B_m M_m^t) \\ I_0 l R_t = -\sum_{m=0}^{\infty} (\pi A_m P_m^t + \pi B_m Q_m^t) \end{cases}, \qquad (7)$$

Решение системы линейных уравнений (7) дает возможность найти распределение тока на поверхности цилиндра, с помощью которого возможно определить диаграмму направленности (ДН) продольного вибратора в присутствии цилиндра со звездным контуром.

Результаты исследований влияния параметров звездного контура на ДН приведены на рис. 2-4. Во всех случаях рассматривалось положение вибратора, показанное на рис.1 при удалении вибратора на расстояние 0,25 λ от поверхности эквивалентного кругового цилиндра. При этом на рисунке 2 показаны ДН продольного вибратора в присутствии звездного контура для случая $R_0 = 2\lambda$, $\Delta R = 0{,}1\lambda$ при различных значениях параметра N.

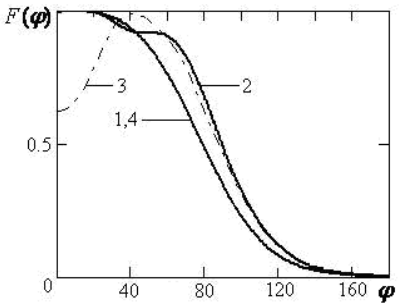

Рис. 2

Из приведенных результатов следует, что при $N = 0$ ДН излучателя полностью совпадает с диаграммой направленности продольного вибратора, расположенного вблизи эквивалентного кругового цилиндра радиуса $R_0 + \Delta R$ (кривая 1). При увеличении значения N диаграмма направленности приобретает вид, характерный для продольного вибратора, расположенного вблизи эквивалентного кругового цилиндра с импедансными граничными условиями (кривые 2, 3) [3]. Однако дальнейшее увеличение значения N, соответствующее уменьшению периода следования «канавок», приводит вновь к обращению в нуль значения поверхностного импеданса. Данный эффект, как показано в [4], имеет место и в случае гребенчатой структуры.

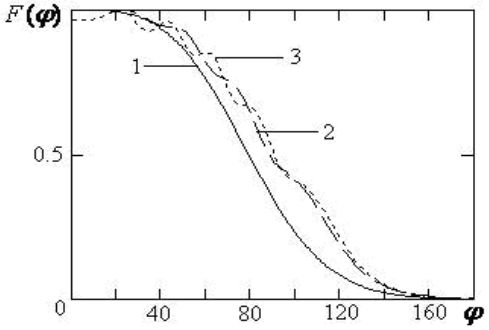

Рис. 3

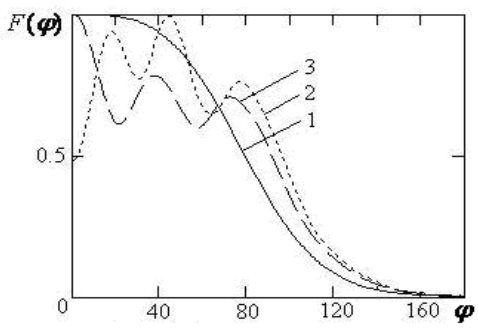

Рис. 4

На рисунках 3 и 4 представлены результаты исследований влияния глубины канавки звездообразного контура ΔR на ДН вибратора при $N = 4$ (рис. 3) и $N = 8$ (рис. 4) соответственно. Приведенные кривые показывают, что при $\Delta R = 0$ в обоих случаях ДН (кривые 1) совпадает с диаграммой вибратора идеально проводящего кругового цилиндра, возбуждаемого продольным электрическим диполем. Увеличение значения ΔR, т.е. глубины «канавки», приводит к увеличению поверхностного импеданса эквивалентного кругового цилиндра и соответствующему изменению ДН. Однако при $N = 64$ значения поверхностного импеданса практически равны нулю независимо от величины ΔR.

Заключение

Таким образом, в статье исследованы вопросы реализации импедансных свойств цилиндрической поверхности путем изменения геометрических параметров идеально проводящей цилиндрической поверхности с сечением в виде звездного контура

Литература

1. *Вайнштейн Л.А*. Электромагнитные волны. М.: Радио и связь, 1988. 440 с.

2. *Clavijo S., Diaz R.E., McKinzie W.E.,* Design Methodology for Sievenpiper High-Impedance Surfaces: An Artificial Magnetic Conductor for Positive Gain Electrically Small Antennas. // IEEE Trans. Antennas and Propag. 2003. Vol.51. No. 10. P. 2678-2690.

3. *Габриэльян Д.Д., Звездина М.Ю., Синявский Г.П.* Методы решения задач дифракции для цилиндрических поверхностей с радиопоглощающими покрытиями // Успехи современной радиоэлектроники. 2006. №6. С. 68-80.

4. *Марков Г.Т., Чаплин А.Ф.* Возбуждение электромагнитных волн. М.: Радио и связь, 1983. 296 с.