ISSN 2072-0297

МОЛОДОЙ УЧЁНЫЙ

МЕЖДУНАРОДНЫЙ НАУЧНЫЙ ЖУРНАЛ

21
2021
ЧАСТЬ II

16+

Молодой ученый

Международный научный журнал

№ 21 (363) / 2021

Издается с декабря 2008 г. Выходит еженедельно

На обложке изображен *Лев Семенович Понтрягин* (1908–1988), советский математик.

Лев Семенович внес значительный вклад в алгебраическую и дифференциальную топологию, теорию колебаний, вариационное исчисление, теорию управления. В теории управления Понтрягин — создатель математической теории оптимальных процессов, в основе которой лежит так называемый принцип максимума Понтрягина; имеет фундаментальные результаты по дифференциальным играм. Работы школы Понтрягина оказали большое влияние на развитие теории управления и вариационного исчисления во всем мире.

Понтрягин родился в Москве, в семье служащего; отец — счетовод, мать — портниха. Биография Льва Семеновича является живым примером вдохновенного труда, несгибаемой воли, железного упорства и могущества человека.

В одной из статей академик Игорь Ростиславович Шафаревич пишет: «Громадную роль в жизни Понтрягина сыграла, конечно, трагедия, пережитая им в возрасте 13 лет: он пытался починить примус, тот взорвался, и в результате ожогов и неудачного лечения Понтрягин полностью ослеп. И наиболее характерно для Понтрягина то, как он нечеловеческим напряжением воли преодолел эту трагедию. Он просто отказался ее признать. Он никогда не пользовался никакой техникой, предназначенной для слепых. Всегда пытался ходить сам, без сопровождения других. В результате у него обычно на лице всегда были ссадины и царапины. Он научился кататься на коньках, на лыжах, плавал на байдарке. Представьте себе, каково было учиться студенту, который не мог записывать лекций! Он как-то сказал: «Я потерял сон в 20 лет. Я запоминал все лекции, которые за день прослушал в университете, а всю ночь курил и восстанавливал их в памяти». Или каково ему было хотя бы ежедневно добираться до университета. Понтрягин пишет: «Сама поездка в трамвае была мучительна... Были случаи, когда кондуктор внезапно объявлял: «Прошу граждан покинуть вагон, трамвай дальше не идет». Это для меня означало необходимость поисков другого трамвая в совершенно неизвестном для меня месте, что я сделать один не мог. Приходилось кого-нибудь просить о помощи». Пожалуй, самое трудное, что Понтрягин сделал, — это преодолел чувство ущербности, недостаточности, которое могло бы возникнуть в результате его несчастья. Он никогда не производил впечатления несчастного, страдальца. Наоборот, жизнь его была предельно напряженной, полной борьбы и побед».

Беда усугубилась тем, что вся эта история с примусом произошла на глазах отца Левы. Его здоровье не справилось с этим кошмаром — вскоре он скончался. И сын при поддержке матери принялся обживать новый мир незрячего человека.

Лева продолжал ходить в обычную школу. Но настоящая работа была дома — освоение математических премудростей (он сам выбрал эту науку). Мать прочитывала сыну приблизительно по сотне страниц в день. Тех самых страниц с формулами. Обнаружилось, что лучшие математические книги написаны на немецком, и Татьяна Андреевна с нуля выучила немецкий. Лева его более или менее знал еще по школьным занятиям. В результате он окончил школу с золотой медалью и поступил в Московский университет на физико-математический факультет, затем благополучно получил диплом и пошел в аспирантуру к знаменитому Павлу Сергеевичу Александрову.

Лев Семенович из принципа не пользовался тяжеленными томами, написанными шрифтом Брайля. Очень любил танцы. Еще студентом как-то поразил аудиторию. Прервал лекцию профессора Бухгольца громкой фразой: «Профессор, вы ошиблись в чертеже». Он слушал стук мела о доску, и в какой-то момент обнаружил несоответствие реальных звуков и тех, что раздавались у него в голове.

Однако даже родная мать, та самая, благодаря которой Лев Семенович и состоялся как ученый, с годами стала создавать проблемы. Взрослому ученому хотелось завести семью. Она же всеми правдами и неправдами отгоняла от сына потенциальных невест. В результате оба брака (первую невесту подобрала лично Татьяна Андреевна, вторую Лев Семенович нашел сам) вышли несчастливыми, давали больше нервотрепки и проблем, чем счастья и отдохновения.

В семидесятые Лев Семенович сделался «общественником». Писал в журнале «Коммунист» о неудачном реформировании преподавания математики в школе. Академик лучше многих понимал, что математика и без того сложна, чтобы усложнять ее сверх меры, да еще и школьникам. К нему прислушались. Учебники переписали. Он также выступал против поворота сибирских рек (была такая сумасшедшая идея). Исключительно с позиций математики он доказал необоснованность расчетов. И тут к нему тоже прислушались.

К концу жизни у математика начались проблемы со здоровьем. По настоянию своей второй жены Лев Семенович сделался вегетарианцем, почти полностью перешел на сыроедение, и проблемы отступили. Но вечной жизни не бывает, и академик Понтрягин скончался. Его похоронили на Новодевичьем кладбище. В честь него назвали астероид и улицу в Москве, а также установили два бюста. Один из этих бюстов находится в Российской государственной библиотеке для слепых.

Екатерина Осянина, ответственный редактор

СОДЕРЖАНИЕ

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

БИОЛОГИЯ

МЕДИЦИНА

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Искусственный интеллект и проблемы кибербезопасности. Технология Deepfake

Власенко Александра Владимировна, кандидат технических наук, доцент;
Киселёв Пётр Сергеевич, студент;
Склярова Екатерина Александровна, студент
Кубанский государственный технологический университет (г. Краснодар)

Новые цифровые технологии позволяют все сложнее отличить настоящие медиа от поддельных. Одним из последних событий, усугубляющих эту проблему, является появление дипфейков, представляющих собой гиперреалистичные видеоролики, в которых используется искусственный интеллект (ИИ). Он используется для объединения и наложения существующих изображений и видео на исходные изображения или видео с использованием техники машинного обучения, называемой «генеративно-состязательной сетью» (GAN). Сочетание существующего и исходного видео приводит к поддельному видео, которое показывает человека или людей, выполняющих действие на мероприятии, которое никогда не произошло на самом деле. В сочетании с охватом и скоростью социальных сетей убедительные дипфейки могут быстро охватить миллионы людей и оказать негативное влияние на наше общество. В данной статье представлен всесторонний обзор дипфейков и предлагаются возможные способы для борьбы с подделками СМИ и фейковыми новостями.

Ключевые слова: *информационная безопасность, киберпреступность, искусственный интеллект, deepfake технология, фейковые новости, обнаружение.*

В настоящий момент технологии переживают переломный момент в истории. Искусственный интеллект (ИИ) и машинное обучение (МО) развиваются быстрее, чем способность общества понимать их. Хотя термины ИИ и МО часто используются как синонимы, они относятся к двум взаимосвязанным понятиям. Созданный в 1950-е годы ИИ — это область информатики, которая относится к программам, предназначенным для моделирования «интеллекта». На практике это относится к алгоритмам, которые могут рассуждать или учиться с учетом необходимых входных данных и базы знания и используются для таких задач, как планирование, распознавание, автономное принятие решений (например, прогноз погоды). МО — это специализированная ветвь искусственного интеллекта, которая использует алгоритмы для понимания моделей явлений из примеров (например, статистическое машинное обучение) или опыта (например, подкрепляющее обучение) [1].

Недавние достижения в области ИИ трансформируют и уже превосходят человеческий уровень в таких задачах, как распознавание изображений, обработка естественного языка и анализ данных. В то же время вычислительные системы, ИИ и МО, становятся все более распространенными и критическими. Эти новые возможности могут сделать мир безопаснее и более доступным, справедливым, но и наоборот, они создают проблемы безопасности, которые могут поставить под угрозу общественную и частную жизнь.

По данным исследования Cybersecurity Ventures за 2020 год в список 15 тенденций киберпреступлений, которые представляют и будут представлять угрозу в ближайший период времени, входит немалое количество угроз, связанных с уязвимостями ИИ [2]. Одной из них является технология Deepfake, о которой и будет рассказано в данной статье.

Что же такое Deepfake и чем опасна данная технология? Deepfake (от англ. deep learning — «глубокое обучение» и fake — «фальшивый») — так называемая реалистичная манипуляция аудио- и видеоматериалами с помощью искусственного интеллекта, т. е поддельный контент с наложением лиц и голосов людей на видеоматериалы различного содержания [3]. Эта технология заставляет человека говорить то, чего он не произносил, и делать то, чего он никогда не совершал.

История дипфейков начинается с появления фотоманипуляции, разработанной в 19 веке, которая вскоре стала применяться в кино. В течение XX века технологии неуклонно совершенствовались исследователями академических институтов. Особенно ускорился данный процесс с появлением цифрового видео. Так, к девяностым годам

подобными инструментами обладали лишь эксперты по спецэффектам в киноиндустрии. Впоследствии же технология была доработана в интернет-сообществе, а впервые термин Deepfake был придуман и использован в конце 2017 года одноименным пользователем Reddit. Этот пользователь предоставил пользователям Интернета доступ к инструментам на базе искусственного интеллекта (ИИ), которые необходимы для создания собственных дипфейков. В настоящий момент в открытом доступе существует достаточное количество программного обеспечения для этой цели.

Технология Deepfake применяет возможности искусственного интеллекта для синтеза человеческого изображения: объединяет несколько снимков, на которых человек запечатлён с разных ракурсов и с разным выражением лица и делает из них видеопоток. Процесс создания дипфейка изменился по мере того, как различные приложения и бесплатное программное обеспечение попадают в публичное пространство, но основная концепция более сложных видео дипфейка следует тем же принципам. Обычно есть автокодировщик и генеративная состязательная сеть (GAN). Проще говоря, автокодировщик — это способ компьютера видеть лицо и определять все способы его «оживления». Он обрабатывает то, как это лицо моргает, улыбается, ухмыляется и так далее. Генеративная состязательная сеть — это система, с помощью которой изображения из автокодировщика сравниваются с реальными изображениями целевого человека. Он отклоняет неточные изображения, вызывая новые попытки, и цикл продолжается бесконечно, постепенно приближаясь к «идеальному» воссозданию человека. В итоге: первая нейросеть создает изображение выражения лица человека, вторая сообщает ей, если выражения выглядят фальшивыми, и спорят, пока все изображения не станут почти идеальными.

На рис. 1 изображен процесс работы генеративной состязательной сети.

Deepfake работает при помощи открытых алгоритмов машинного обучения и библиотек, что позволяет достичь контента высшего качества. Нейросеть получает изображения из библиотеки и обучается при помощи роликов на видеохостингах. Искусственный интеллект тем временем сопоставляет фрагменты исходных портретов с тем, что есть на видео, и в итоге получается правдоподобный материал [4].

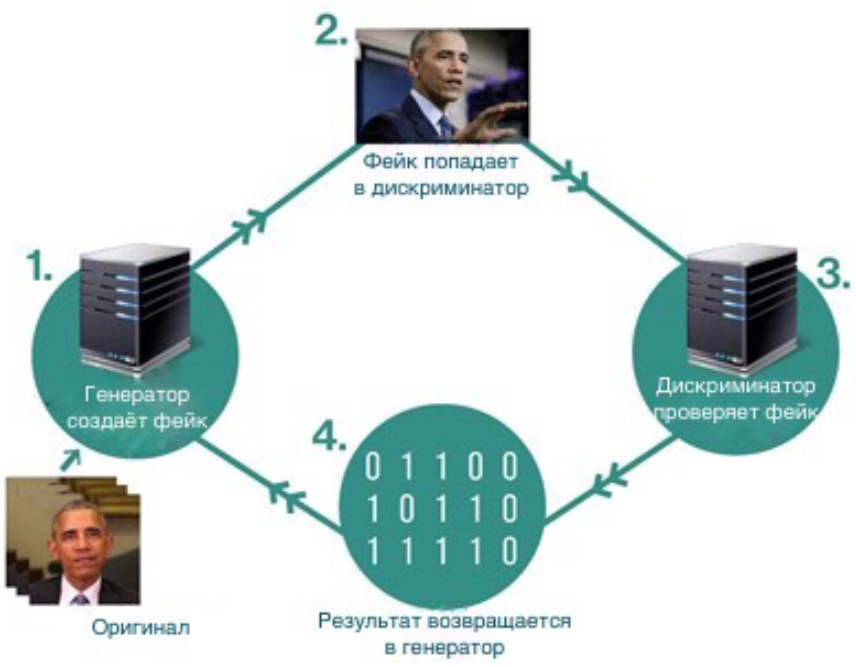


Рис. 1. **Работа генеративной состязательной сети**

Согласно технологическому отчету Массачусетского технологического института, устройство, позволяющее использовать дипфейки, может быть «идеальным оружием для поставщиков фейковых новостей, которые хотят влиять на все, от цен на акции до выборов» [5].

На самом деле, «инструменты ИИ уже используются, чтобы положить фотографии лица других людей на телах порнозвезд и поставить слова в устах политиков», пишет Мартин Джайлс, Сан-Франциско глава бюро MIT Technology Review в отчете. Он сказал, что сети GAN не создали эту проблему, а лишь усугубили ее.

Хотя манипулирование изображениями имеет значительную историю, часто используемую в качестве пропаганды во время конфликтов, легкая доступность цифровых инструментов, высокореалистичный характер подделанного контента и наличие новых медиаканалов для распространения дезинформации превратили дипфейки в жизнеспособный механизм атаки.

Дипфейки раннего поколения уже использовались для воспроизведения аудио и визуального сходства общественных деятелей, таких как политики, знаменитости и генеральные директора. Правдоподобность этих упро-

щенных примеров невысока, и зрители могут определить, является ли видео подлинным или поддельным.

Одними из громких дипфейк-видео были выпущены в открытом доступе, например, заявление режиссера Джордана Пила о Бараке Обаме (PSA), предназначенное как предупреждение об опасностях и убедительности видео дипфейков, и фейковое видео, где генеральный директор Facebook Марк Цукерберг рассказывает CBS News «правду о Facebook и о том, кому действительно принадлежит будущее», демонстрируя свою силу.

С ростом числа важных государственных выборов, которые пройдут во всем мире в 2020/2021 годах, влияние дипфейков, вероятно, намного превзойдет влияние существующих «фейковых новостей».

Так, в 2020 году главный оппонент Трампа, Джо Байден, стал жертвой фальсификаций. В начале марта обманчиво отредактированное видео с выступлением Джо Байдена было опубликовано в Твиттере со стороны сторонников Трампа, в том числе директора по коммуникациям Белого дома Дэна Скавино и Чарли Кирка, возглавляющего группу сторонников Трампа Turning Point USA. Затем Трамп ретвитнул отредактированное видео. Видео включало 14-секундный отрывок из речи Байдена, в котором он, казалось, предсказывал, что «мы можем только переизбрать Дональда Трампа», вырезая конец цитаты, чтобы превратить предупреждение о разобщенности демократов в очевидную поддержку. Этот дипфейк, сделанный в начале марта, был скорее для насмешек, чем для обмана [6].

Помимо политических информационных войн Deepfake создаёт и риски в области информационной безопасности корпоративного сектора. Достижения и растущая доступность технологий искусственного интеллекта позволяют злоумышленникам создавать высокореалистичные цифровые копии руководителей в реальном времени путем наложения структур лиц и использования голосовых паттернов для имитации реальных голосов. По мере того, как технологии deepfake становятся более правдоподобными, эта новая, весьма убедительная угроза уже начинает затрагивать многие организации. Мало того, что популярные мобильные приложения, такие как Snapchat и Zao, позволяют людям с легкостью создавать дипфейк-контент, злоумышленники смогут покупать и продавать весьма убедительные дипфейк-технологии или услуги в темной сети и использовать ботов для создания поддельного контента в социальных сетях. Организациям, использующим услуги потокового аудио и видео низкого качества, будет особенно сложно выявить эту угрозу, поскольку недостатки даже в самых упрощенных дипфейках останутся незамеченными.

Дипфейки оказались неплохим инструментом в руках мошенников. Первый случай использования искусственного интеллекта в фишинге, социальной инженерии с использованием автоматизированного голоса, использовался для проведения громкого мошенничества в начале 2019 года. Злоумышленники, копирующие голос генерального директора энергетической компании, смогли убедить сотрудников организации перевести 243000 долларов поддельному поставщику. Злоумышленники использовали методы социальной инженерии, чтобы обманом заставить сотрудника позвонить генеральному директору, и, поскольку голос на другом конце телефона был таким же, как у генерального директора, сотрудник продолжил перевод.

Хотя дипфейки уже начали вызывать серьезную озабоченность в средствах массовой информации, скорость, с которой развивается эта технология, неизбежно приведет к негативным последствиям для целевых организаций. Традиционные попытки выявить клевету и противостоять ей не смогут справиться с изощренностью дипфейков. Установленные формы общения будут подвергнуты сомнению, поскольку реальное становится неотличимым от фальшивого, а доверие еще больше подрывается в и без того расколотом мире.

Хотя ИИ можно использовать для создания дипфейков, его также можно использовать для их обнаружения. Поскольку технология становится доступной для любого пользователя компьютера, все больше и больше исследователей сосредотачиваются на обнаружении дипфейка и ищут способ его регулирования.

Крупные корпорации, такие как Facebook и Microsoft, выступили с инициативами по обнаружению и удалению дипфейк-видео. Обе компании объявили ранее в 2020 году, что они будут сотрудничать с ведущими университетами США для создания большой базы данных поддельных видео для исследований [7].

В настоящее время есть небольшие визуальные аспекты, которые исчезают, если вы присмотритесь, все — от ушей или глаз, не совпадающих с нечеткими границами лица или слишком гладкой кожи, до освещения и теней. Но обнаруживать «жесты» становится все труднее и сложнее, поскольку технология дипфейка становится все более продвинутой, а видео выглядят более реалистично.

Существует несколько методов обнаружения дипфейков:

1. Ручное обнаружение

Один из наиболее многообещающих ручных методов выявления и обнаружения дипфейк-видео — это анализ моргания человека в дипфейк-видео. Здоровые взрослые люди моргают каждые две-десять секунд, а одно моргание занимает от одной десятой до четырех десятых секунды. Следовательно, можно ожидать увидеть похожие моргание на видео, где человек разговаривает, но это не так во многих дипфейк-видео. Причина отсутствия мерцания в дипфейк-видео напрямую связана с алгоритмом, использованным для создания таких ролики. Обучение алгоритму дипфейка основано на изображениях лиц, и очень немногие такие изображения показывают лица с глазами закрыто. Следовательно, обучающие данные включают только лица с открытыми глазами, что приводит к смещению обучающих данных. Последняя обученная модель не сможет понять действие моргающего глаза и не сможет произвести закрытый глаз очень хорошо. Отсутствие

моргания глаз в дипфейк-видео, таким образом, обеспечивает простой, но интуитивно понятный способ обнаруживать дипфейк.

Можно разработать метод определения того, когда человек на видео моргает глазами и моргает ли в принципе. Метод будет сканировать каждый кадр видео, автоматически обнаруживая и обнаруживая глаза. Используя другой глубокое обучение, нейронная сеть позволит определить, открыты или закрыты обнаруженные глаза, полагаясь на глаз внешний вид, геометрические особенности и движение глаз.

Другой метод ручного обнаружения дипфейк-материала фокусируется на несоответствии между углом наклона головы и лица. Доступны методы, позволяющие оценить положение головы в трехмерном (3D) пространстве на двухмерном (2D) видео. При создании дипфейка лицо вставляется в видео, где голова должна указывать в другом направлении на камеру. Следовательно, создатели дипфейк-видео должны выполнить 2D преобразование для поворота лица так, чтобы оно соответствовало ориентацию головы. Однако, двухмерное преобразование вносит множество недостатков, когда объект съемки смотрит в сторону от камеры или меняет угол обзора положение лица. К сожалению, этот конкретный метод обнаружения не позволяет эффективно обнаруживать дипфейк-видео, когда человек на видео всегда смотрит прямо в камеру, не меняя угла лица.

Третий метод ручного выявления и обнаружения дипфейк-материала основан на недостатках, возникающих в процессе создания фейковых видеороликов. К таким недостаткам относятся:

— двойной подбородок или призрачные края лица;

— чрезмерное размытие по сравнению с другими не лицевыми областями;

— изменение тона кожи у края лица;

— двойные брови или двойные края на лице;

— лицо частично закрыто руками или другими предметами;

— мерцание или размытие на видео.

Эти недостатки вызваны тем, что создатели дипфейк-видео срезают углы, чтобы сократить необходимое время для создания видеороликов, которые могут снизить качество [8]. В результате количество пикселей на лице объекта в исходном видео может варьироваться в зависимости от расстояния от камеры и размера исходного изображения. Кадры содержащие лица, используемые для замены оригинала, обычно имеют фиксированный размер 64x64 пикселей или 128x128 пикселей. Чтобы приспособиться к вариациям, лица фиксированного размера необходимо преобразовать путем увеличения, сжатия или поворота изображения, чтобы соответствовать исходному видео. Такие вариации, если их объединить, оставят такие некоторые недостатки, как излишне гладкое лицо или потеря детализации. Эти недостатки можно обнаружить, обучив нейронную сеть глубокого обучения, чтобы детально различать изменения в области лица.

Последний метод ручной идентификации и обнаружения дипфейков — использование обнаружения размытия. Обнаружение размытия возможно, так как исходное лицо будет иметь больше уровней цвета, чем дипфейк-изображение при увеличении.

Обнаружение размытия включает следующие шаги:

— анализ видеопотока;

— нахождение области лица с помощью каскадного классификатора Хаара (алгоритм обнаружения объектов машинного обучения);

— свертка с помощью оператора Лапласа;

— расчет дисперсии для области лица;

— разделение на два случая: первое — известное поддельное изображение и второе — неизвестное видео.

Для первого случая сравнивается дисперсии двух областей лица. Изображение с большей дисперсией — оригинал, в то время как изображение с меньшей дисперсией — дипфейк-изображение. Во втором случае неизвестное видео будет использоваться для нахождения другой эталонной области лица. Для этого новой области так же рассчитывается дисперсия. Следующим шагом вычисляется соотношение между этими двумя выбранными областями лица и сравнивается соотношение с порогом, который устанавливается с использованием большой коллекции оригинальных изображений. Если соотношение превышает пороговое значение, видео является оригинальным, в противном случае оно является дипфейк-видео.

2. Обнаружение на основе программного обеспечения

Первое решение для обнаружения дипфейков с помощью ПО, называемое Shallow, представляет собой веб-приложение, которое использует сверточные нейронные сети Keras, специализирующиеся на распознавании изображений. Основное внимание в решении уделяется различению между настоящими и поддельными видео с целью защиты репутации и целостности всех, кто может быть под влиянием дипфейк-видео. Вместо того, чтобы полагаться на предварительно обученные сети, используемые для классификации изображений, Shallow использует рандомизированные сети для повышения точности классификации дипфейк-видео.

Пользователи могут получить доступ к веб-интерфейсу и загрузить видео для обработки. На начальном этапе обработки Shallow будет обнаруживать и извлекать вырезки лиц, доступные в загруженном видео. Затем пользователь может выбрать 20 вырезок лица для тестирования и прогнать изображения через модель. Модель проведет анализ видео и сообщит о подлинности видео.

Набор данных, используемый для построения и тестирования модели для Shallow, состоит из четырех разных категорий: реальные данные обучения, поддельные данные обучения, реальные данные проверки и поддельные данные проверки. Для обеспечения разнообразия как обучения, так и проверки 30% изображений содержат не взрослых людей. Модель была обучена на двух отдельных наборах данных и проверена с исполь-

зованием дополнительных двух наборов данных. Обучение проводилось с использованием 15613 различных изображений с соотношением между дипфейком и реальными изображениями 50/50. Проверка была проведена с использованием 4872 различных изображения с одинаковым соотношением 50/50 между дипфейк- и реальными изображениями. На основе использования доступных наборов данных для обучения и благодаря проверке модель смогла достичь точности 99%. Однако следует отметить, что модель обучена и проверена с использованием доступных наборов данных и может быть не репрезентативной для других наборов.

Второе решение для обнаружения дипфейк-видео, названное MesoNet, разработано для обнаружения фальсификации лица в видео. Цель MesoNet — предоставить метод автоматического и эффективного обнаружения вставки лица в видео, а также уделить особое внимание двум недавним методам, используемым для создания гиперреалистичных поддельных видео: Deepfake и Face²Face (передача выражения лица изображения от источника к целевому человеку) [9].

Для обеих построенных моделей доступны предварительно обученные сети. Набор данных, используемый для построения и тестирования модели для MesoNet состоят из набора для обучения и проверки. Обучение проводилось на 5111 поддельных образах и 7250 реальных изображений. Проверка была проведена с использованием 2998 поддельных изображений и 4259 реальных изображений. Обе модели продемонстрировали очень успешный уровень обнаружения: более 98% для Deepfake и 95% для обнаружения Face²Face.

В заключение данной статьи стоит отметить, что технология Deepfake остается опасной угрозой для информационной безопасности 21-го века. Необходимо постоянно изучать потенциал и риски, связанные с дипфейками. При этом наиболее перспективные направления использования дипфейков — политические войны и мошенничество. Кроме того, с учётом постоянного совершенствования технологий дипфейки могут также навредить и судебной практике — в части доверия к аудио- и видеоматериалам доказательной базы (диктофонным записям, файлам видеорегистраторов и т. п.). Хоть в данной статье определены и описаны наборы доступных методов для их обнаружения, эти методы все еще ограничены предоставленными возможностями. Для решения данной проблемы следует обеспечить основу для поддержки разработки новых и улучшенных методов обнаружения дипфейков.

Литература:

1. В чем разница между ИИ и машинным обучением и почему это важно. — Текст: электронный //: [сайт]. — URL: https://news. russianhackers. org/ai-and-ml-difference/(дата обращения: 11.04.2021).
2. Cyberthreat trends: 15 cybersecurity threats for 2020. — Текст: электронный // Norton: [сайт]. — URL: https://in. norton. com/internetsecurity-emerging-threats-cyberthreat-trends-cybersecurity-threat-review. html (дата обращения: 11.04.2021).
3. Deepfake. — Текст: электронный // Wikipedia: [сайт]. — URL: https://ru. wikipedia. org/wiki/Deepfake (дата обращения: 11.04.2021).
4. Александр, Панасенко Технологии Deepfake как угроза информационной безопасности/Панасенко Александр. — Текст: электронный // anti-malware: [сайт]. — URL: https://www. anti-malware. ru/analytics/Threats_Analysis/Deepfakes-as-a-information-security-threat (дата обращения: 15.04.2021).
5. Александр, Богданов Российский разработчик создал новое поколение алгоритма Deepfake. Что он умеет?/Богданов Александр. — Текст: электронный // hi-news. ru: [сайт]. — URL:: https://hi-news. ru/eto-interesno/rossijskij-razrabotchik-sozdal-novoe-pokolenie-algoritma-deepfake-chto-on-umeet. html (дата обращения: 13.04.2021).
6. Henry, Ajder Donald Trump retweets crude «deepfake» video of Joe Biden/Ajder Henry. — Текст: электронный // sensity: [сайт]. — URL: https://medium. com/sensity/tracer-newsletter-51–27–04-20-donald-trump-retweets-crude-deepfake-video-of-joe-biden-385a94a5d9f0 (дата обращения: 13.04.2021).
7. Tom, Burt New Steps to Combat Disinformation/Burt Tom. — Текст: электронный // Microsoft: [сайт]. — URL: https://blogs. microsoft. com/on-the-issues/2020/09/01/disinformation-deepfakes-newsguard-video-authenticator/(дата обращения: 18.04.2021).
8. Александр, Агеев 5 приемов, позволяющих (пока еще) отличить реальность от DeepFake/Агеев Александр. — Текст: электронный // Техкульт: [сайт]. — URL: https://www. techcult. ru/technology/7549-5-priemov-pozvolyayushih-otlichit-realnost-ot-deepfake (дата обращения: 18.04.2021).
9. Afchar, D. MesoNet: a Compact Facial Video Forgery Detection Network/D. Afchar., V. Nozick — Текст: электронный // Github: [сайт]. — URL: https://github. com/DariusAf/MesoNet (дата обращения: 18.04.2021).

Безопасность интернета вещей

Власенко Александра Владимировна, кандидат технических наук, доцент;
Киселёв Пётр Сергеевич, студент;
Склярова Екатерина Александровна, студент
Кубанский государственный технологический университет (г. Краснодар)

Интернет вещей (IoT) становится новой тенденцией в наши дни. Поскольку подключение к Глобальной сети становится легкодоступным, каждый может позволить себе экосистему Интернета вещей прямо у себя дома. При таком развитии событий передача и хранение информации сталкиваются с серьезными проблемами, такими как кража данных из устройств IoT, использование таких устройства для DDoS атак, слежение за пользователями и т. д. Поэтому безопасность устройств Интернета вещей становится второстепенной или может первостепенной задачей при производстве большинства таких устройств. В статье делается попытка обобщить проблемы безопасности систем Интернета вещей с точки зрения основных концепций информационной безопасности — конфиденциальности, целостности и доступности.

Ключевые слова: *архитектура, безопасность Интернета вещей, Internet of Things, IoT.*

Введение

IoT — концепция пространства, в котором все из аналогового и цифрового миров может быть совмещено — это переопределит наши отношения с объектами, а также свойства и суть самих объектов — Роб Ван Краненбург (основатель Европейского совета по «Интернету вещей», ведущий эксперт в области цифровизации, автор концепции Интернета Вещей) [1].

Интернет начинался как небольшая взаимосвязанная сеть с небольшим количеством компьютеров. Теперь — это Глобальная сеть, содержащая миллиарды взаимосвязанных не только компьютеров, но и различных устройств, которые совместно используют и хранят информацию.

Термин IoT появился, когда количество компьютеров и устройств, которые самостоятельно собирают, обрабатывают и передают информацию, значительно превысило количество людей, занимающихся этим и «Интернет людей» стал «Интернетом вещей».

Систему IoT можно описать с помощью базовой трехуровневой архитектуры:

Уровень восприятия, также называется уровнем устройств (вещей) — типичный внешний уровень, который включает датчики для восприятия и сбора информации

Уровень шлюза — сеть отвечает за подключение датчиков к сетевым устройствам, интеллектуальным устройствам и серверам. Его функции также используются для передачи и обработки данных датчиков.

Облачный уровень — серверные службы, необходимые для настройки, управления, эксплуатации и извлечения ценности из системы IoT [2].

IoT продвигает нашу повседневную жизнь и вносит вклад в такие отрасли, как сельское хозяйство, управление цепочками поставок, отслеживание местоположения, удаленный мониторинг, анализ в реальном времени и т. д.

Поскольку концепция Интернета вещей становится все более актуальной, она привлекает большое внимание исследователей и промышленников со всего мира. Несмотря на то, что Интернет вещей обладает большим количеством преимуществ, такая система также имеет большое количество потенциальных проблем и недостатков. И безопасность остается одной из важнейших проблем.

Векторы атаки на уровни архитектуры IoT

1. Уровень восприятия.

Этот уровень является самым нижним уровнем в архитектуре IoT. Основная цель этого уровня — сбор всех видов информации от сенсорных устройств и отправка их на уровень шлюза. На этом уровне существуют физические устройства, такие как RFID (радиочастотная идентификация), исполнительные механизмы, датчики.

Атака «отказ в обслуживании». Узлы восприятия Интернета вещей имеют ограниченную емкость и возможности, поэтому злоумышленники могут использовать атаку отказа в обслуживании, чтобы остановить службу.

Аппаратные помехи. Злоумышленник может повредить узел, заменив части оборудования на неисправные.

Вставка подставных узлов. Злоумышленник может вставить фальсифицированный или вредоносный узел между фактическими узлами сети, чтобы получить доступ и получить контроль над сетью IoT.

Атака «грубой силой». Поскольку узлы датчиков имеют более слабую вычислительную мощность, атака методом грубой силы может легко нарушить доступ к устройствам.

2. Уровень шлюза.

Второй или средний уровень архитектуры известен как уровень шлюза, и основная цель этого уровня — обеспечение надежной связи между уровнем восприятия и уровнем облака.

Атака «отказ в обслуживании». Поскольку этот уровень обеспечивает сетевое соединение, после атаки отказа в обслуживании, серверы или устройства не смогут предоставлять услуги пользователю.

Атаки с перехватом сеанса связи. Злоумышленники могут перехватить сеанс связи и получить доступ к сети.

Атака «человек посередине». Злоумышленник может встроиться в канал связи между двумя узлами и легко по-

лучить секретную информацию, если отсутствует надлежащий механизм шифрования.

3. Облачный уровень.

Это самый верхний уровень в архитектуре IoT, который отвечает за вычисления, обработку и хранения информации. Предоставляет услуг конечным пользователям, по сути, интерфейс, с помощью которого пользователи могут управлять своими устройствами и контролировать их.

Уязвимость данных при облачных вычислениях. Все собранные данные будут обрабатываться и храниться в облаке, поставщик облачных услуг будет нести ответственность по защите этих данных.

Атаки на уровне приложений. Большинство приложений размещаются в облаке в виде «программное обеспечение как услуга» и доставляются через веб-службы, поэтому злоумышленник может легко манипулировать протоколами уровня приложений и получать доступ к сети IoT.

Атака на виртуальные машины. С помощью виртуальных машин происходит работа пользователей с данными, поэтому безопасность таких машин очень важна, и любое нарушение работы машины может привести к отказу всей среды Интернета вещей [3].

OWASP Top 10 IoT

Open Web Application Security Project, или OWASP (открытый проект обеспечения безопасности веб-приложений сообщество работает над созданием статей, учебных пособий, документации, инструментов и технологий, находящихся в свободном доступе), опубликовал список конкретных уязвимостей, которые будут актуальный для IoT в будущем [4].

Ниже приводится текущий ранжированный список основных проблем, которых следует избегать:

1. Слабые, легко угадываемые или запрограммированные пароли

Использование уязвимых для перебора паролей, доступных публично или неизменяемые пароли учётных записей, включая бэкдоры в пользовательских приложениях и прошивке, которые гарантируют несанкционированный доступ к развернутой системе.

2. Небезопасные сетевые услуги

Необязательные или небезопасные сетевые службы, работающие на устройстве, особенно те, которые подвержены воздействию из Интернета, такие службы ставят под угрозу конфиденциальность, целостность и доступность, а также дают возможность несанкционированного удаленного доступа.

3. Небезопасные интерфейсы экосистем

Небезопасные веб-интерфейсы, бэкенд-API, облачные или мобильные интерфейсы в экосистеме за пределами устройств, которые допускают компрометацию устройств или связанных с ним компонентов. Общие проблемы включают в себя отсутствие аутентификации/авторизации, полное отсутствие или слабое шифрование, а также полное отсутствие или слабая входная и выходная фильтрации трафика.

4. Отсутствие надежного механизма обновления

Отсутствие возможности безопасного обновления устройства. Включает отсутствие проверки прошивки на устройстве, отсутствие защищенной доставки (не зашифрованной передаче), отсутствие механизмов защиты от отката и отсутствие уведомлений об изменениях безопасности при обновлениях.

5. Использование небезопасных или устаревших компонентов

Использование устаревших или небезопасных программных компонентов/библиотек, которые позволили бы устройству быть скомпрометированным. Включает небезопасную настройку платформ операционных систем, а также использование сторонних программных или аппаратных компонентов из скомпрометированной цепочки поставок.

6. Недостаточная защита конфиденциальности

Личная информация пользователя, хранящаяся на устройстве или в экосистеме, которая используется небезопасно, неправильно или без разрешения.

7. Небезопасная передача и хранение данных

Отсутствие шифрования или контроля доступа к конфиденциальным данным в любой точке экосистемы, в том числе в состоянии покоя, при передаче или во время обработки.

8. Отсутствие управления устройством

Отсутствие поддержки безопасности на устройствах, развернутых на производстве, включая Управление Активами, управление обновлениями, безопасный вывод из эксплуатации, мониторинг систем и реагирование на их возможности.

9. Небезопасные настройки по умолчанию

Устройства или системы, поставляемые с небезопасными настройками по умолчанию или не имеющие возможности задать собственные настройки, ограничивая операторов от изменения конфигураций.

10. Отсутствие физической защиты устройств

Отсутствие мер физической защиты, позволяющих потенциальным злоумышленникам получить информацию, которая может помочь в будущей атаке или взять под контроль устройство [5].

Меры противодействия атакам на IoT

Базовая система IoT требует выполнения следующих требований.

1. Аутентификация проверяет личность пользователей или устройств в системе IoT.

2. Авторизация проверяет, какими правами обладает уполномоченный объект для выполнения в системе.

3. Конфиденциальность зашифровывает данные, для защиты от несанкционированного доступа к ним.

4. Целостность сохраняет данные от модификации, или может сигнализировать о их изменении.

5. Запрет отказа от авторства гарантирует подлинность исходного источника данных.

Поскольку системы IoT состоят из разнородных устройств с различными технологиями, определяющими требования к безопасности, принятие мер безопасности является огромной проблемой из-за сложности.

В Таблице 1 будет показано, что можно сделать для повышения безопасности с точки зрения вышеупомянутых требований.

Таблица 1. **Меры противодействия атакам**

Критерий безопасности	Действие	Описание
Аутентификация	Использовать пользовательские (не стандартизированные) учетные записи.	Необходимо выполнять обязательную идентификацию пользователей и устройств, а также самостоятельно настроить учетные записи, удалив все учетные записи по умолчанию.
Авторизация	Использовать методы управления идентификацией и контроль доступа.	
Конфиденциальность	Использовать соответствующий механизм шифрования, поскольку устройства могут содержать меньшую вычислительную мощность	Данные должны быть зашифрованы, чтобы только авторизованные пользователи могли получить к ним доступ.
Целостность	Использовать методы хеширования	Невозможность подделки данных может быть обеспечена с помощью различных методов хеширования.
Запрет отказа от авторства	Использование цифровых подписей	Источник данных должен быть подтвержден с помощью цифровых подписей.

Чтобы обезопасить Интернет вещей, кроме использования более совершенных протоколов или ликвидации уязвимостей, необходимо добиться следующего: первое — использовать отдельную локальную сеть для подключения всех устройств Интернета вещей между собой; и второе, более сложное, — заставить производителей «умных вещей» не использовать общедоступные методы сброса настроек, учетные записи и пароли при производстве таких устройств.

Интернет вещей — это обширная область, которая развивается каждый день, улучшая жизнь человечества. Поскольку это быстро развивающаяся технология, ряд исследователей работают над улучшением защиты систем IoT непрерывно, исключая известные уязвимости, разрабатывая новые протоколы обмена данными специально для систем Интернета вещей.

Литература:

1. Николай, Пилипенко Интернет вещей — а что это?/Пилипенко Николай. — Текст: электронный // Хабр: [сайт]. — URL: https://habr. com/ru/post/149593 (дата обращения: 19.04.2021).
2. IoT Privacy and Security: Challenges and Solutions/Tawalbeh Lo»ai, Muheidat Fadi, Tawalbeh Mais, Quwaider Muhannad. — Текст: электронный // MDPI: [сайт]. — URL: https://www. mdpi. com/2076-3417/10/12/4102 (дата обращения: 19.04.2021).
3. Navod, N. T. Security and Privacy Issues in IoT Environment/N. T. Navod. — Текст: электронный // International Journal of Engineering and Management Research: [сайт]. — URL: https://www. ijemr. net/ojs/index. php/ojs/article/view/238/445 (дата обращения: 19.04.2021).
4. OWASP. — Текст: электронный // Википедия: [сайт]. — URL: https://ru. wikipedia. org/wiki/OWASP (дата обращения: 24.04.2021).
5. OWASP IoT Top 10. — Текст: электронный // OWASP — Открытый проект обеспечения безопасности веб-приложений: [сайт]. — URL: https://owasp. org/www-pdf-archive/OWASP-IoT-Top-10-2018-final. pdf (дата обращения: 24.04.2021).

Разработка программного модуля визуализации конфигурирования микросхем

Зотов Владислав Дмитриевич, студент
Национальный исследовательский университет «МИЭТ» (г. Зеленоград)

В статье автор сравнивает применяемое на предприятии программное решение с аналогичными, и приходит к выводу о необходимости разработки нового.

Ключевые слова: *разработка, программный модуль, микросхема.*

На предприятии была разработана микросхема микроконтроллера с собственным микропроцессорным ядром. Сразу же возник вопрос, каким образом пользователь будет осуществлять ее программирование. Для того чтобы пользователь смог самостоятельно провести это действие, он должен изучить и понимать все тонкости работы по ее конфигурированию и настройке.

Для начала было разобрано и проанализировано текущее решение Verilator, применяемое на предприятии. Данное программное средство преобразует файлы с Verilog кодом в файлы с кодом C++, затем они компилируются компилятором C++, получается исполняемый файл, который выполняет моделирование работы всей микросхемы, после чего происходит ее конфигурирование.

Такая цепочка действий не устраивала предприятие, так как для того, чтобы провести конфигурирование микросхемы нужно было совершить много различных действий в различных программах.

Поэтому, сравнив существующие аналоги, приведенные в таблице 1, было принято решение создать новую программную оболочку для программирования, которая позволила бы повысить эффективность конфигурирования микросхемы, а также совершать это при помощи графической оболочки.

Таблица 1. **Сравнение существующих программных продуктов**

Существующие решения / Требования	Verilator (текущее решение) [1]	GHDL [2]	САПР Quartus II (LITE) [3]	САПР «КОВЧЕГ» [4]
Кроссплатформен-ность	Нет	Да	Да	Нет
Создание схем конфигурирования	Да	Да	Да	Да
Установщик программного решения	Нет	Нет	Да	Да
Графическая оболочка для создания схемы конфигурирования	Нет	Нет	Да	Да
Процесс конфигурирования микросхемы	Нет	Нет	Нет	Нет
Изменение характеристик каждого элемента схемы	Да	Да	Да	Да
Подключение библиотек элементов для построения схемы	Да	Да	Да	Да

Как видно из таблицы, ни одно из готовых решений не удовлетворяет всем требованиям предприятия по конфигурированию микросхем. В качестве темы учебной практики была выбрана тема «Разработка программного модуля визуализации конфигурирования микросхем». Программному модулю присваивается шифр «ПМ КМС» (Далее в тексте — ПМ).

Была выбрана тема «Разработка программного модуля визуализации конфигурирования микросхем». Программному модулю присваивается шифр «ПМ ВКМ».

Цель разработки ПМ ВКМ:

Повышение эффективности конфигурирования микросхем.

Задачи разработки ПМ ВКМ:

— исследование предметной области;
— сравнение существующих аналогов;
— выбор языка и среды программирования;
— разработка схемы данных ПМ ВКМ;
— разработка схемы алгоритма ПМ ВКМ;
— разработка программы ПМ ВКМ;
— отладка и тестирование ПМ ВКМ;
— разработка руководства оператора.

Концептуальная модель предметной области состоит в проектировании единого ПМ, которое позволило бы пользователю создавать схемы конфигурирования из доступных функциональных компонентов библиотек элементов, а также запускать процесс программирования микросхемы, разработанной на предприятии.

Предполагаемый алгоритм работы программы:

ПМ при старте считывает все элементы во всех заранее созданных библиотеках и создает из них список компонентов. Затем пользователь сам конфигурирует из них свою схему на предназначенном для этого поле, настраивая каждый нужный ему элемент и создавая межкомпо-

нентные соединения между ними. После чего он запускает процесс конфигурирования микросхемы, который собирает всю созданную пользователем схему в единый файл, который транслируется в код, понятный для микросхемы, а после чего и в саму микросхему для завершения процесса ее программирования.

Таким образом, входными данными ПМ будут являться файлы библиотек элементов, хранящиеся в памяти пользовательского устройства.

ПМ в процессе своей работы будет работать с данными в формате JSON.

Файл, содержащий в себе код конечной схемы конфигурирования, будет являться выходными данными ПМ.

Вывод:

Во время учебной практики была выбрана тема работы, исследована предметная область, выполнено сравнение существующих аналогов, выбран язык и среда программирования, а также разработана схемы данных и алгоритма ПМ.

Литература:

1. Verilator Intro. — Текст: электронный // Veripool: [сайт]. — URL: https://www. veripool. org/projects/verilator/wiki /Intro (дата обращения: 20.05.2021).
2. GHDL. — Текст: электронный // GitHub: [сайт]. — URL: http://ghdl. free. fr/(дата обращения: 20.05.2021).
3. Различия между вариантами Quartus. — Текст: электронный // Intel: [сайт]. — URL: https://www. intel. com/content/dam/ www/programmable/us/en/pdfs/literature/po/ss-quartus-comparison. pdf (дата обращения: 20.05.2021).
4. НАЗНАЧЕНИЕ САПР «КОВЧЕГ». — Текст: электронный // НПК «Технологический центр»: [сайт]. — URL: http://www. asic. ru/index. php/sapr/naznach (дата обращения: 20.05.2021).

Изменения в цифровой коммуникации во время глобальной пандемии COVID-19

Каршибоев Шароф Абдураупович, ассистент;
Муртазин Эмиль Рустамович, ассистент
Джизакский политехнический институт (Узбекистан)

В этом статье рассматривается, как пандемия изменила использование людьми цифровых методов коммуникации. Мы также обсуждаем, как изменения в использовании цифровых медиа могут пережить пандемию и что это означает для будущих коммуникаций и медиа-исследований.

Ключевые слова: *цифровая коммуникация, цифровое неравенство, COVID-19, социальные связи.*

В первые месяцы пандемии отраслевые отчеты показали, что использование цифровых медиа значительно возросло, поскольку люди проводят больше времени дома из-за карантина, связанного с коронавирусом. Такой рост был особенно распространен для социальных сетей и приложений для обмена сообщениями, но особенно примечателен беспрецедентный рост приложений и программ для видеоконференцсвязи. С учетом того, что люди широко используют информационные и коммуникационные технологии (ИКТ) для социального взаимодействия в таких условиях, когда они остаются дома, это требует дальнейшего изучения.

Есть также люди, которые во время пандемии сократили свое цифровое общение. В то время как небольшое меньшинство (5%) использовали текстовые сообщения реже, больше людей сократили общение через социальные сети (8%), голосовые звонки (9%), электронную почту (10%), видеозвонки (13%) и онлайн-игры. (17%). Взяв все способы вместе, 9% респондентов только уменьшили цифровую связь, не увеличивая ни один из методов. В то время, когда личное социальное взаимодействие ограничено, такое уменьшение цифровой коммуникации предполагает, что определенные группы людей могут упускать социальные связи.

Исследования цифрового неравенства показывают, что люди различаются по качеству доступа к Интернету и навыкам, которые затем могут влиять на выгоды, которые они могут получить от коммуникационных технологий. В Соединенных Штатах четверть населения не имеет дома широкополосного доступа в Интернет, а почти пятая часть населения не имеет смартфона. Помимо качества доступа, к другим проблемам при взаимодействии с технологиями относятся нестабильные интернет-соединения, а также трудности с поддержанием функциональности устройств. Таким образом, во времена, когда личное общение снижается из-за рекомендаций по дистанцированию, определенные группы более подвержены риску отключения от своего социального окружения, чем другие.

Во время пандемии COVID-19 цифровое неравенство может еще больше усилиться из-за отсутствия цифровой поддержки (доступа к ней). Поскольку мир в значительной степени полагается на цифровые технологии для связи, менее технически подкованные люди могут больше нуждаться в поддержке, чем когда-либо. Рекомендации по со-

циальному дистанцированию и домоседу могут затруднить получение цифровой поддержки, особенно для тех, кто полагается в основном на личные социальные связи.

На момент написания этой статьи мы еще не могли знать, сохранятся ли новые модели цифрового общения людей после того, как будут сняты меры по сохранению дома, дистанцирования и изоляции и люди снова смогут встречаться лично. Однако с учетом того, что пандемия коронавируса серьезно повлияла на рост числа людей во всем мире в области цифровых коммуникаций, исследователи цифровых медиа должны подумать о том, как пандемия может повлиять на нашу дисциплину и вопросы исследования в будущем.

Новые модели общения, возникшие во время пандемии, имеют различные потенциальные последствия для развития событий в будущем. С одной стороны, возможно, что цифровое общение людей увеличилось из-за желания чаще встречаться с друзьями и семьей во время этого конкретного кризиса со здоровьем, а также потому, что личные средства общения менее возможны. Также может случиться так, что у людей будет больше времени, чтобы тратить их на такое общение, из-за мер изоляции и руководящих принципов оставаться дома. После того, как кризис закончится, поведение при цифровой коммуникации может вернуться к прежнему состоянию, и люди станут меньше беспокоиться о ежеминутных ситуациях своих близких, и снова станет возможным личное общение. С другой стороны, по мере того как люди осваивают новые методы цифровой коммуникации, они могут отдавать предпочтение этим новым подходам и сохранять их в долгосрочной перспективе. Короче говоря, мотивация, уникальная для времени пандемии, может привести к появлению привычек, которые переживут саму вспышку.

Смогут ли люди, которые раньше не полагались на цифровые технологии для общения, но теперь приняли новые цифровые методы, чтобы оставаться на связи с друзьями и семьей, продолжать использовать их в будущем? Вполне возможно, что после пандемии видеозвонки станут более популярными. Тот же вопрос относится и к другим методам цифровой связи, число которых во время пандемии возросло, таких как использование текстовых сообщений, голосовых вызовов, социальных сетей, электронной почты и онлайн-игр.

Пандемия COVID-19 подняла новые вопросы для ученых, занимающихся цифровой коммуникацией. Наша работа как дисциплина актуальна как никогда, о чем свидетельствуют многочисленные исследования, связанные с COVID-19, средствами массовой информации и коммуникациями (например, Европейская ассоциация коммуникации в здравоохранении, 2020; Matias & Leavitt, 2020). В то же время мы должны подумать о долгосрочных последствиях, которые пандемия может иметь для наших исследований использования цифровых медиа. Один из способов изучить долгосрочные последствия — это изучить, как пандемия сформировала цифровое неравенство. В этом эссе мы рассказали о моделях восприятия, а также о снижении количества цифровых коммуникаций и о том, как эти модели соотносятся с социально-демографическими факторами, а также о проблемах, связанных с доступом к Интернету и навыками. Основываясь на этих выводах, даже спустя долгое время после пандемии различия в поведении в отношении использования цифровых медиа могут сохраниться. Пожилые люди, люди с незащищенным доступом к Интернету и люди с более низкими навыками доступа к Интернету могут остаться в стороне от использования цифровых методов коммуникации в то время, когда использование такого общения может быть особенно важным. Устранение этих различий становится все более настоятельной необходимостью, поскольку мы сталкиваемся с продолжающейся неопределенностью, связанной с возобновлением работы наших сообществ.

Пандемия побуждает многих определять и применять новые методы цифровой связи. Пандемия также открывает возможности и влияет на то, как мы используем цифровые медиа во всех других аспектах нашей жизни. Если эти изменяющиеся модели сохранятся в долгосрочной перспективе, мы должны четко заявить о себе при обсуждении и сравнении результатов, полученных до и после пандемии коронавируса, когда дело доходит до изучения цифровой коммуникации и использования средств массовой информации. Более того, эти тенденции следует изучать с течением времени, включая их значение для политической коммуникации и журналистики, образования и обучения, коммуникации в области здравоохранения, коммуникации науки и множества других областей. По мере того, как цифровые СМИ становятся все более фундаментальными для повседневной жизни — процесс, который ускорила глобальная пандемия, — изучение общения людей и их поведения в средствах массовой информации, вероятно, будет приобретать все большее значение.

Литература:

1. Подготовка студентов к самостоятельной научно-исследовательской деятельности. Ш. А. Каршибаев, Д. С. Хазраткулов Международный научный, 80
2. Каршибоев, Ш. А. Основы проектной деятельности и жизненный цикл проекта.
3. Кузиев, Б. Н., Холмуминова, Д. А., Муртазин, Э. Р. Электронное обучение как часть образовательного процесса. Ученый XXI века, 1, 43.
4. Муртазин, Э. Р., Сиддиков, М. Ю., Цой, М. П. (2018). Стратегия развития экономики Узбекистана: региональные особенности. In Региональные проблемы преобразования экономики: интеграционные процессы и механизмы формирования и социально-экономическая политика региона (pp. 85-87).

5. Мустафакулов, А. А., Муртазин, Э. Р., Сафаров, А. А. (2016). Исследование возобновляемых источников энергии. Ученый XXI века, (3–1).
6. Муртазин, Э. Р., Ахмеджанова, У., Абдурахманов, Э. М. (2016). Расчёт мощности ветроэлектродвигателя. Ученый XXI века, (3–1).

Методы сокращения энергопотребления в беспроводных сетях

Кнышенко Андрей Александрович, студент магистратуры
Поволжский государственный университет сервиса (г. Тольятти)

Описаны методы сокращения энергопотребления датчиков ввода информации в беспроводных сенсорных сетях. Показано, что использование цифровой видеокамеры в системе позволяет снизить энергопотребление.

Ключевые слова: *энергопотребление, беспроводная сеть, видеокамера.*

В этой статье рассмотрены методы уменьшения (перераспределения) расхода энергии батарей с целью увеличения времени жизни сетей с избыточным количеством узлов за счет планирования и управления совместной работой элементов сети на различных уровнях эталонной модели взаимодействия открытых систем. Для уменьшения расхода энергоресурса узлов с целью увеличения времени жизни сети в настоящее время предложено множество соответствующих методов [1].

Основными методами экономии энергоресурса узлов беспроводных сенсорных сетей (БСС) является организация режимов работы, которая подразумевает периодическое отключение узлов или их приемопередатчиков. БСС осуществляют передачу данных мониторинга с заданным периодом и отключение узлов (приемопередатчиков) после передачи данных до начала следующего периода позволяет снизить расход энергоресурса, но при этом возникает задача организации взаимодействия между узлами для обеспечения ретрансляции сообщений в направлении шлюза с обеспечением минимальных задержек. Классическими подходами решения данного класса задач является организация согласованных циклов сна/пробуждения узлов (приемопередатчиков), что вносит задержки при передаче сообщений.

В отличие от классического подхода организации циклов сна/пробуждения для БСС с избыточным количеством узлов в работе [1] предлагается следующее.

1. На прикладном уровне отключать узлы, которые дублируют покрытие района мониторинга. Для продления длительности функционирования сети предлагается организовать периоды включения/выключения отдельных узлов так, чтобы в каждый момент времени функционировало множество узлов, необходимое для обеспечения заданного покрытия района мониторинга.

2. На сетевом уровне использовать энергосберегающий метод маршрутизации, учитывающий периодическое функционирование множеств избыточных узлов, а также метод уменьшения (сжатия) объема передаваемых данных за счет их избыточности.

3. На канальном уровне при возрастании нагрузки передачи данных использовать гибридные методы множественного доступа (МД) (детерминированные и случайные методы доступа имеют различные предельные значения эффективности в зависимости от нагрузки). Для приближенных к шлюзу узлов (на которых концентрируется трафик всей сети) для уменьшения числа коллизий передачи пакетов и увеличения скоростей передачи целесообразно использовать методы детерминированного доступа к каналу. Для удаленных от шлюза узлов целесообразно использовать методы случайного доступа к каналу, не требующих синхронизации узлов.

Управление мощностью передачи позволяет уменьшить использование энергоресурса за счет уменьшения мощностей (дальности) передачи. Исходя из того, что узлы БСС не мобильны и варианты маршрутов могут быть определены заранее, управление мощностью передачи целесообразно использовать на сетевом уровне в методах маршрутизации.

Уменьшение использования энергоресурса методом уменьшения объема данных (агрегации) происходит за счет уменьшения избыточности или потери точности сбора данных мониторинга с внесением задержек передачи для обработки данных.

БСС с избыточным количеством узлов используется для повышения надежности и качества покрытия площади объекта мониторинга, поэтому в данных сетях методы агрегации целесообразно использовать на сетевом уровне на отдельных узлах с повышенным использованием энергоресурса для предотвращения выхода их из строя при неэффективности применения других методов энергосбережения. Для уменьшения объема данных целесообразно использовать их корреляцию (временную, когда данные не меняются со временем, и пространственную, когда данные от соседних узлов совпадают).

Другая классификация методов снижения энергопотребления в БСС приводится в работе [2], на основании которой можно привести классификацию методов энергосбережения в сенсорных сетях.

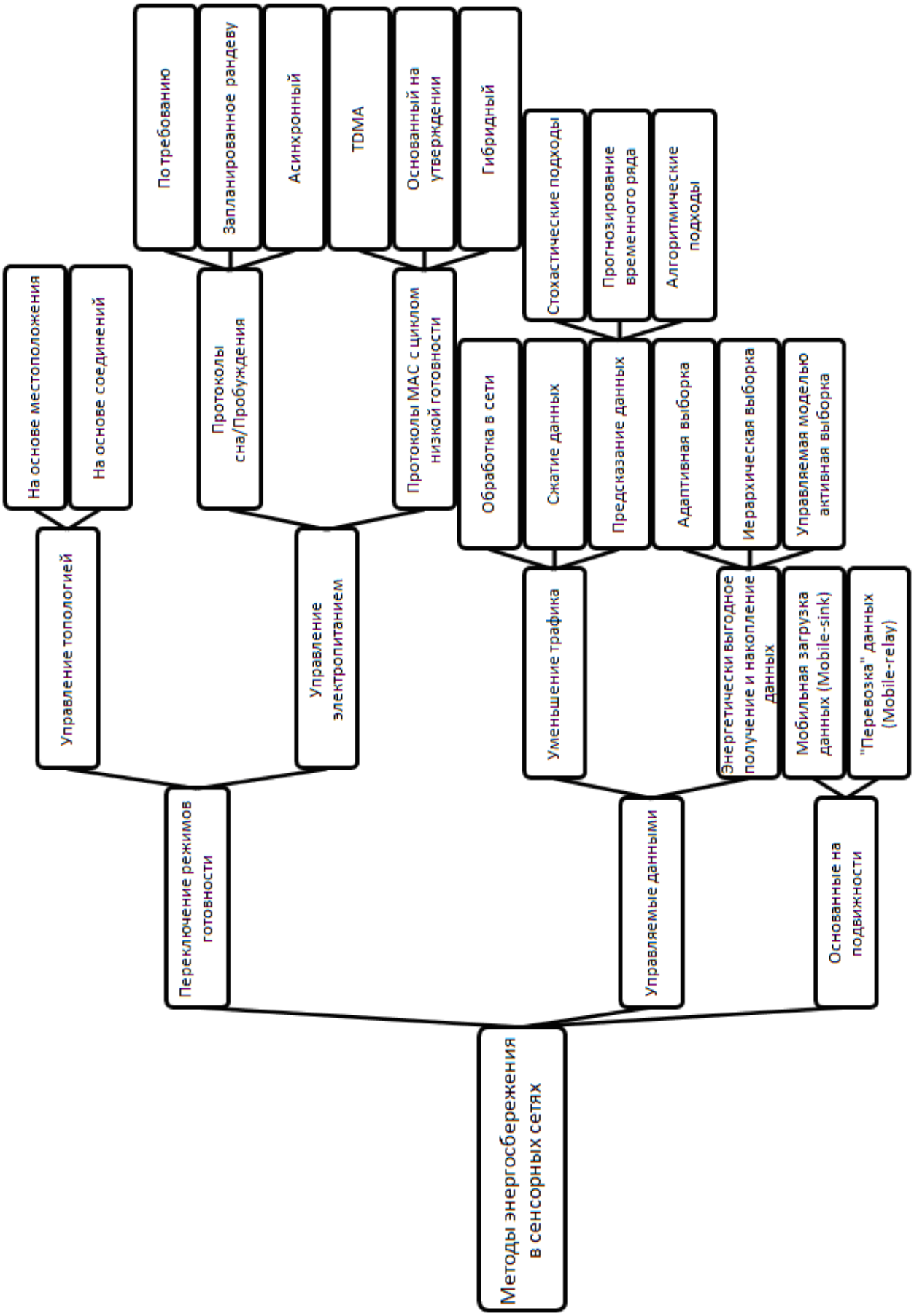


Рис. 1. **Методы энергосбережения в сенсорных сетях**

В связи со сказанным выше, в магистерской диссертации необходимо разработать и исследовать устройства ввода, работающие в оптическом диапазоне, в том числе устройство отражательного типа, которое будет основываться на принципе модуляции ретрорефлектора. В первую очередь оно должно быть ориентировано на наименьшее потребление электроэнергии батареи. В частности, это достигается использованием цифровой видеокамеры, причем ее процессор достаточно легко способен выделять и декодировать изменения яркости пикселя, создаваемого оптическим передатчиком в поле зрения видеокамеры.

Литература:

1. Коваленко, И. Г. Методы увеличения продолжительности функционирования беспроводных сенсорных сетей с избыточным количеством узлов [Текст]/Телекоммуникационные и информационные технологии. — 2014. — № 1. — с. 44-54.
2. Anastasi, G. Conservation in Wireless Sensor Networks: a Survey [Text]/Giuseppe Anastasi, Marco Conti, Mario Di Francesco, Andrea Passarella // Ad Hoc Networks. — 2009. — V. 7. — I. 3. — P. 537-568.

Протокол передачи данных для устройства ввода информации

Кнышенко Андрей Александрович, студент магистратуры
Поволжский государственный университет сервиса (г. Тольятти)

Показано, что создаваемый протокол передачи данных использует время-импульсную модуляции, особенностью которой является большая разница между нулями и единицами. Приведены необходимые диаграммы. Отмечается, что увеличение количества датчиков ведет к росту производительности системы в целом.

Ключевые слова: *время-импульсная модуляция, протокол, диаграммы.*

Для несинхронизуемых устройств необходимо было в первую очередь разработать протокол физического уровня, позволяющий декодировать сигнал с датчика без синхронизации с кадрами камеры. Для этого были изучен ряд источников, описывающих технологии беспроводных сетей [1-4].

Названный протокол был разработан и испытан и применяет время-импульсную модуляцию (рис. 1). Информация кодируется паузами, разделяемыми передаваемыми световыми импульсами. Длительность светового импульса равна двум периодам экспозиции кадра камерой. Для передачи 0 длительность паузы равна двум периодам кадров. Для передачи логической 1 длительность паузы увеличивается до пяти периодов.

Большая разница между паузами для нуля и единицы выбрана из следующих логических соображений. Пауза длительностью два кадра обязательно даст хотя бы один ноль на приемнике, независимо от взаимной фазы передаваемого сигнала и интервалов экспозиций. Однако, в случае коротких выдержек может получиться и три нуля, если интервалы экспозиции попадают на границу паузы. Таким образом, из-за несинхронности пауза передатчика в два кадра расширяется у приемника случайным образом, но в диапазоне от одного до трех нулей.

Аналогично можно показать, что пауза передатчика в пять кадров расширяется у приемника случайным образом, но в диапазоне от четырех до шести нулей.

Более детально временные диаграммы описанного протокола физического уровня показаны на рис. 2, 3.

Диаграммы для устройства отражательного типа выглядят сложнее, однако они просто отражают отличие сигнала управления светодиодом от сигналов управления ЖК-затвором:

— единственный сигнал управления светодиодом чисто логический (1 — светит, 0 — не светит);

— сигналы управления ЖК-затвором работают по следующему правилу: разницы между сигналами RB2, RB3 нет — свет проходит сквозь затвор и отражается ретрорефлектором, сигналы RB2, RB3 противофазны — свет не проходит сквозь затвор и соответственно не отражается ретрорефлектором.

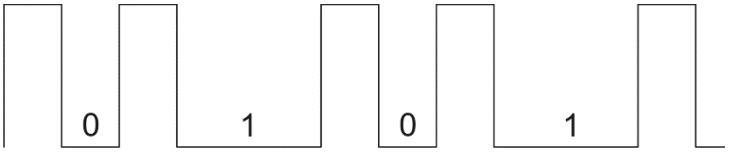


Рис. 1. **Время-импульсная модуляция**

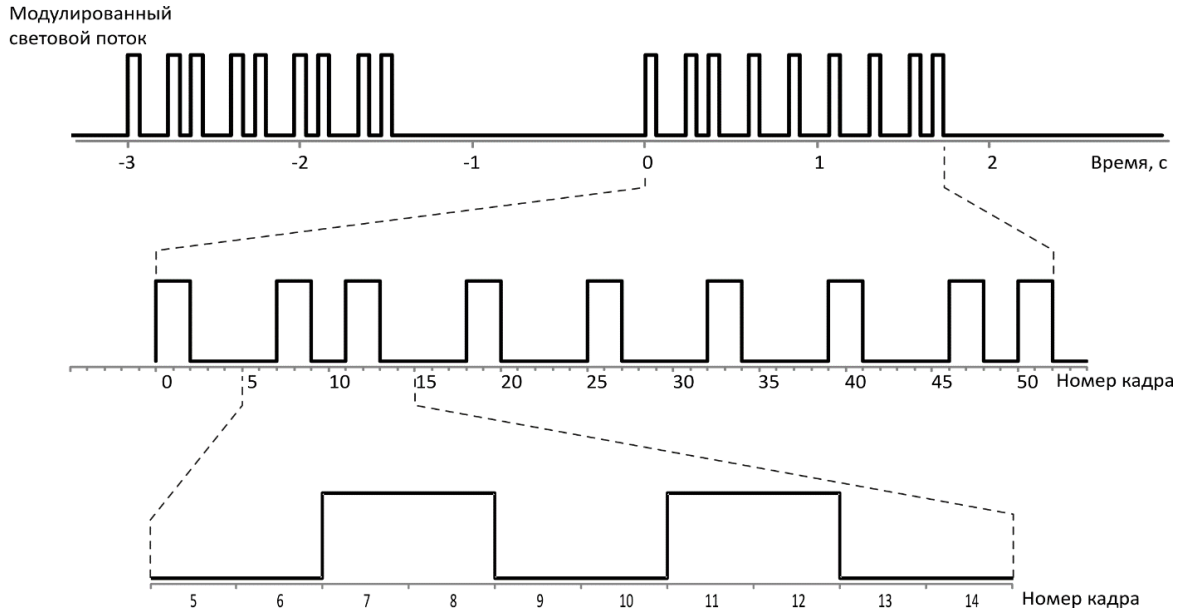


Рис. 2. **Время-импульсная модуляция в устройстве излучательного типа**

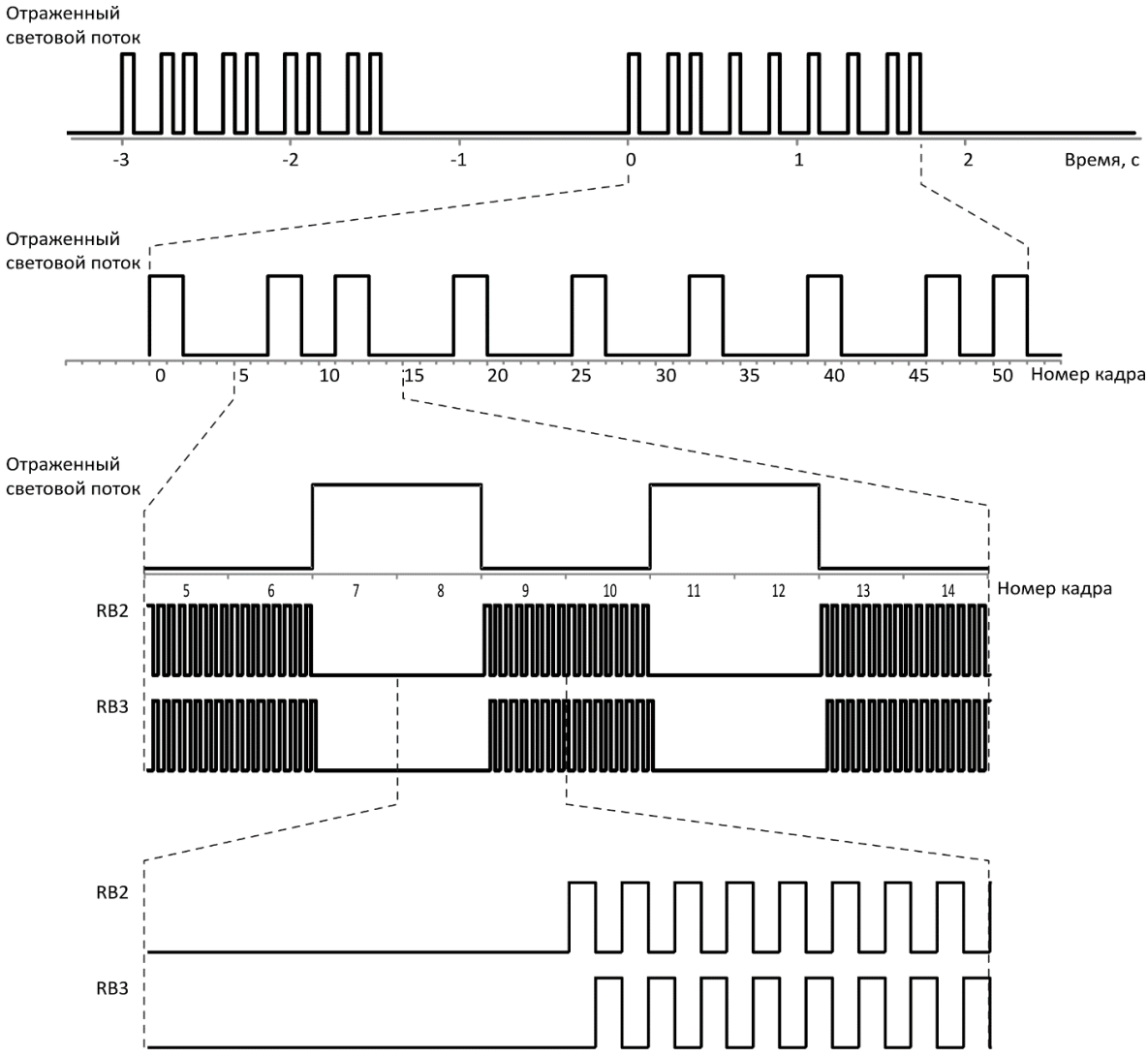


Рис. 3. **Время-импульсная модуляция в устройстве отражательного типа**

Производительность несинхронизуемого устройства определяется описанным протоколом физического уровня. В наихудшем случае, когда байт содержит 8 единиц, на передачу байта таким способом потребуется (5 + 2) * 8 + 2 = 58 кадров. Для устойчивого декодирования между байтами добавляется длинная пауза, которая доводит период следования байтов до 90 кадров. При использовании видеокамер общего назначения с частотой кадров 30 Гц период составляет 3 с.

Таким образом, несинхронизуемая система при использовании недорогих доступных компонентов обладает низкой производительностью в расчете на один датчик, равной 0,33 байт/с. Поэтому она может использоваться только для регистрации медленных процессов, таких, как температура. Однако при добавлении датчиков общая производительность системы будет расти, так как производительность базового устройства (видеокамеры) от добавления датчиков не снижается. Это преимущество рассматриваемой системы перед известными радиоволновыми сетями датчиков, таких, как ZigBee.

Отметим, что производительность синхронизуемых устройств может быть в несколько раз выше, приближаясь численно к частоте кадров камеры. Например, при использовании видеокамер общего назначения с частотой кадров 30 Гц с учетом накладных расходов простого старт-стопного протокола она может составлять порядка 24 бит/с = 3 байт/с в расчете на датчик. Аналогично и здесь общая производительность системы будет расти при добавлении датчиков.

Для приема рассмотренного кода в ходе выполнения магистерской диссертации получен необходимый для реализации кода декодер.

Литература:

1. Григорьев, В. А. Сети и системы радиодоступа [Текст]/В. А. Григорьев, О. И. Лагутенко, Ю. А. Распаев. — М.: Эко-Трендз, 2005. — 384 с.
2. Агафонов, Н. Технологии беспроводной передачи данных ZigBee, BlueTooth, Wi-Fi [Текст]/Н. Агафонов // Беспроводные технологии. — 2006. — № 1. — с. 20-15.
3. Трифонов, С. В. Исследование и оптимизация работы беспроводной сенсорной сети на основе протокола ZigBee [Текст]/С. В. Трифонов, Я. А. Холодов // Компьютерные исследования и моделирование. — 2012. — Т. 4. — № 4. — с. 855-869.
4. Аникин, А. Обзор современных технологий беспроводной передачи данных в частотных диапазонах ISM (Bluetooth, ZigBee, Wi-Fi) и 434/868 МГц [Текст]/А. Аникин // Беспроводные технологии. — 2011. — № 4. — с. 6-12.

Устройства ввода информации с малым энергопотреблением

Кнышенко Андрей Александрович, студент магистратуры
Поволжский государственный университет сервиса (г. Тольятти)

Описаны датчики ввода информации с малым энергопотреблением для беспроводных сенсорных сетей. Показано, что оптимальными для использования в таких сетях являются технологии Bluetooth и особенно ZigBee.

Ключевые слова: *энергопотребление, беспроводная сеть, датчик.*

Одна из современных тенденций в устройствах ввода информации от объектов — расширение применения беспроводных способов передачи информации от чувствительного элемента устройства, то есть от датчика, к компьютеру. В частности, преимуществом беспроводных устройств является простота и низкая стоимость развертывания, особенно когда датчики сильно удалены от компьютера. Системы с несколькими беспроводными датчиками последнее время часто называют сенсорными сетями.

В связи с применением беспроводных способов передачи информации в таких системах все датчики в них должны быть как можно более экономичными, расходуя как можно меньше энергии батарей. Замена батарей в сенсорных сетях — трудоемкое обременительное занятие и желательно, чтобы она происходила как можно реже. Снижение объема и цены батарей также имеют существенное значение.

Малым потреблением можно условно считать датчик, потребляющий ток в среднем порядка 0,1 мА. Это позволяет без замены батарей, например типоразмера AAA, непрерывно работать до 10000 часов (около года). В ряде случаев, однако, и этого недостаточно, например, при мониторинге крупномасштабных сооружений замена датчиков или батарей в них может выливаться в сложное и дорогостоящее организационно-техническое мероприятие, которое хотелось бы производить не каждый год. С другой стороны, иногда (например, в некоторых

биомедицинских применениях) даже размеры батареи ААА могут быть велики, и речь может идти об источниках питания на порядок меньшей емкости. Тогда можно для таких случаев назвать условную границу 0,01 мА = 10 мкА микропотреблением и такой датчик считать микропотребляющим.

В качестве примера в табл. 1 приведены параметры некоторых современных датчиков температуры [1].

Анализ таблицы показывает, что, если измерения производятся непрерывно, то только датчик TMP102 можно отнести к малопотребляющим. Однако так как в большинстве практических случаев температура меняется достаточно медленно, так что датчик 99% времени может находиться в спящем режиме. В этом случае уже все приведенные датчики можно отнести к микропотребляющим.

К сожалению, в беспроводных устройствах ввода кроме датчика обязательно есть передатчик, работающий через тот или иной беспроводной канал, а также микроконтроллер. Потребление тока современных 8-разрядных микроконтроллеров в режимах сниженного энергопотребления уже также достигло микроамперных уровней. Однако, передатчик (или приемопередатчик — трансивер), работающий через радиоканал, вынужден потреблять уже минимум сотни микроампер или миллиамперы, чтобы создать требуемую мощность излучаемых волн.

Поэтому и представляет интерес рассмотрение также иных альтернативных каналов передачи. В частности, в настоящей работе разработаны беспроводные устройства ввода, работающие через оптический канал и показано, что в некоторых вариантах таких устройств потребление передатчика может быть существенно снижено.

Все стандарты и технологии беспроводной передачи данных могут быть классифицированы по ряду формальных параметров. В табл. 2 приведено сравнение некоторых актуальных на данный момент стандартов беспроводной передачи данных [2].

Таблица 1. **Параметры низковольтных полупроводниковых датчиков температуры с цифровым выходом**

Тип	**TC74**	**SE98A**	**TMP102**	**DS620**	**MAX31723**
Изготовитель	Microchip	NXP Semiconductors	Texas Instruments	Maxim	Maxim
Диапазон температур, °C	–40…+125	–40…+125	–55…+150	–55…+125	–55…+125
Погрешность в диапазоне 0°C — 70°C, °C	2	2	1	0,5	0,5
Цена деления, °C	1	0,125	0,0625	0,0625	0,0625
Интерфейс	I2C	I2C	I2C	I2C	SPI/3-Wire
Напряжение питания, В	2,1…3,6	1,7…3,6	1,4…3,6	1,7…3,5	1,7…3,7
Потребляемый ток в спящем режиме, мкА	5	5	1	2	2
Потребляемый ток в режиме измерения, мА	0,2	0,4	0,02	0,8	1,2
Количество выводов	5	8	6	8	8

Как следует из табл. 2, для работы с малопотребляющими датчиками предназначены технологии Bluetooth и особенно ZigBee. Последняя специально создавалась для тех применений, где можно поступиться скоростью передачи в обмен на пониженное энергопотребление.

Таблица 2. **Технологии беспроводной передачи данных по радиоканалу**

	ZigBee	**Bluetooth**	**Wi-Fi**	**3G**
Частотный диапазон, МГц	2400-2483	2400-2483	2412-2840	1885-2025; 2110-2200
Скорость передачи данных, кбит/с	До 250	720	11000/54000	144/384/2048
Дальность связи, м	200	класс 1-100; класс 2-10; класс 3-1	100	во всей зоне покрытия
Потребление тока, активный режим, мА/спящий режим, мкА	30/10	70/20	450	350/3500
Модуляция, доступ к среде	DSSS	FHSS	DSSS	TDMA/ FDMA/CDMA

Литература:

1. Староверов, К. Датчики температуры Maxim [Текст] // Новости электроники. — 2006. — № 6. — с. 2-5.
2. Григорьев, В. А. Сети и системы радиодоступа [Текст]/В. А. Григорьев, О. И. Лагутенко, Ю. А. Распаев. — М.: Эко-Трендз, 2005. — 384 с.

Основы растровой электронной микроскопии и подготовка образцов

Лунёв Андрей Алексеевич, студент
Курский государственный университет

В статье автор пытается определить основы растровой электронной микроскопии и подготовку образцов.
Ключевые слова: *РЭМ, образец, микроскопия.*

Большинство наноматериалов, например, углеродных нанотрубок, нанопроволок, наночастиц и наноструктурированных материалов, можно наблюдать в РЭМ непосредственно путем их фиксации на углеродной проводящей липкой ленте. Подготовка образцов достаточно проста. На некоторые непроводящие наноматериалы, особенно биоорганические, необходимо напылить слой металлического покрытия и подвергнуть их сложному процессу пробоподготовки. В данном разделе будет подробно обсуждаться процедура пробоподготовки биоорганических образцов.

Процедуры получения изображений биоорганических образцов в РЭМ высокого разрешения

Для обеспечения надлежащих рабочих характеристик электронной оптики в колонне РЭМ, пушке и камере образцов должен поддерживаться вакуум порядка 10-6 Торр. Исключением из этого правила являются рабочие условия в камере образцов РЭМ с естественной средой. Высоковакуумные условия являются враждебными для большинства форм жизни вследствие того, что живые клетки и биологические ткани содержат почти 80% воды. Даже для небольших биомолекул требуется гидратная оболочка для того, чтобы они оставались в своем естественном состоянии. Подобная несовместимость жидких проб, таких как водные растворы, с вакуумной системой электронного микроскопа вынуждает переводить образец в твердое состояние, проводить осушение жидкостей, которые могли бы приводить к дегазации в высоком вакууме и загрязнении колонны микроскопа. Поэтому все жидкие образцы, загружаемые в камеру образцов РЭМ, должны быть осушены для того, чтобы получить стабильное изображение во вторичных электронах. Когда на РЭМ планируется проводить наноструктурные исследования биологических или сольватированных органических систем, необходимость удаления жидкостей значительно влияет на наблюдаемые структуры. Исключением среди условий пробоподготовки образцов путем их сушки является криофиксация и наблюдение при криогенных температурах (криоВРРЭМ — крио-РЭМ высокого разрешения, или cryo-HRSEM — cryo high resolution SEM), который сохраняет водный состав образца в твердом состоянии. В данном разделе мы рассмотрим необходимые этапы перевода биологического образца в твердое состояние (путем его сушки) с минимальными изменениями. Пробоподготовка должна быть достаточно мягкой, чтобы «существенные» детали структуры твердых компонентов в нанометровом масштабе можно было исследовать с помощью РЭМ. Во время испарения растворителя из жидкого образца в газовую атмосферу, как это происходит в случае сушки на воздухе, на поверхность образца действуют большие силы поверхностного натяжения. Это приводит к усыханию и сжатию структур в интервале размеров от 10-3 до 10-6 м, что делает невозможными РЭМ-исследование структур с размерами 1-10 нм. В процессе обычного высушивания на воздухе суспензии красных кровяных телец в воде силы поверхностного натяжения оказываются такими сильными, что разглаживают белые кровяные тельца до такой степени, что на их поверхности уже становится невозможным различить какие-либо структуры. Интересным исключением являются красные кровяные тельца, имеющие предельно гладкую поверхность, на которой не выявляется никаких структурных изменений в субмикронном интервале после сушки на воздухе. Однако молекулярные детали в интервале размеров от 1 нм до 10 нм будут сглажены силами поверхностного натяжения.

При использовании РЭМ в биомедицинских исследованиях электронный микроскоп служит в основном для регистрации характеристик топографии обработанной поверхности образца. Неорганические твердые вещества легко напыляются или фиксируются на столике образцов и могут непосредственно наблюдаться в РЭМ при высоких увеличениях, позволяющих увидеть в подробностях их наноструктуру. Более сложная стратегия иммобилизации молекулярных компонентов и структурных особенностей организмов, органов, тканей, клеток и биомолекул заключается в их химической фиксации в твердом состоянии с помощью химических сое-

динений «кросс-линкеров», сшивающих биополимеры, с последующей обработкой их солями тяжелых металлов для повышения удельной массы компонентов. Биологические образцы сначала «фиксируются» с помощью глютаральдегида-диальдегида, который содержит пять атомов углерода. Когда такие молекулы буферизованы, биологическая проба либо поливается этим раствором, либо погружается в него, и он вступает в реакцию с N-концом аминокислот на соседних белках, высвобождая при этом молекулы 2H2 O и перекрестно сшивая пептидные цепочки. Таким образом, останавливается перемещение всех белковых компонентов клеток и тканей. Затем биологические образцы подвергаются «постфиксации» с помощью тетроксида осмия (OsO4), который, по-видимому, взаимодействует с ненасыщенными жирными кислотами, в то время как липиды служат для остановки вращения молекул относительно их связей и высвобождению 2H2 O. Поскольку OsO4 содержит самый тяжелый элемент, он служит для повышения электронной плотности и усиления рассеивающих свойств биологических мембран, которые в противном случае имеют низкий контраст при наблюдении в РЭМ. OsO4 также является красящим агентом, который взаимодействует сам с собой и с другими красящими веществами. Применение красящих агентов для растровой электронной микроскопии высокого разрешения не рекомендуется, поскольку они связывают дополнительные элементы с мембранами, так что при морфологическом разрешении 1-10 нм наблюдаемые структуры искусственно утолщаются и их размеры невозможно измерить с достаточной точностью. Методы окрашивания красиво работают при наблюдении клеточных органелл с промежуточным увеличением.

После фиксации водное содержимое образца перед сушкой замещается промежуточной жидкостью, обычно органическим растворителем, таким как этанол или ацетон. Для сушки на воздухе иногда применяют ряд растворителей, например, гексаметилдисилазан (ГМДС, или HMDS), Фреон 113, тетраметилсилан (ТМС, или TMS) и PELDRI II, поскольку они уменьшают величину сил поверхностного натяжения, вызывающих сжатие и усыхание клеток и деталей их поверхностной морфологии. Метод высушивания растворителя на воздухе применяют в надежде избежать более времязатратных методов. Эти растворители имеют очень низкое давление паров, и некоторые из них дают удовлетворительные результаты по фиксации белых кровяных телец при наблюдении в РЭМ на промежуточных увеличениях. Однако этот метод не годится для исследования наноморфологии в РЭМ с высоким разрешением. Поскольку процедура сушки удаляет гидратную оболочку с биоорганических молекул, наблюдается некоторое их сжатие в масштабе 1-10 нм. Наиболее общая схема обезвоживания заключается в использовании погружения образца в серию растворов этанола, либо ацетона с концентрациями 30%, 50%, 70%, 90% и 100%, и нескольких промывок в чистом 100%-м растворителе. Необходимо предпринимать меры предосторожности для того, чтобы не удалить слишком много объемной жидкости и не подвергнуть поверхность образца воздействию воздуха. Хотя, как известно, биологические клетки растягиваются при концентрациях ниже 70% и сжимаются между 70% и 100%, изменение их формы можно контролировать с помощью бивалентных катионов, используемых в фиксирующих буферных растворах или промывочных ваннах. Превосходным методом обезвоживания является линейное градиентное дегидрирование, которое требует сменного устройства для медленного повышения концентрации промежуточной жидкости и служит для снижения осмотического удара и изменения формы образца.

В качестве обзора процедур пробоподготовки теперь рассмотрим методику получения изображения в ВРРЭМ биологически важных морфологических деталей размером 1-10 нм. В работе были представлены критерии в пользу и против метода сублимационной криосушки (СКС, или FD — freeze drying) по сравнению с методом сушки в критической точке (СКТ, или CPD — critical point drying), когда эти методы впервые были тщательно изучены в отношении сохранения деталей биологической структуры при морфологических исследованиях биологических образцов в РЭМ. В резюме этой работы сказано, что при фиксации образцов методом СКТ обычно применяются добавки веществ-криопротекторов (сахарозы и DMSO), которые способствуют уменьшению образования кристаллов льда, но при этом сами могут взаимодействовать с образцом. Фиксированные и обработанные криопротекторами образцы погружались в замороженном состоянии в криогенную жидкость (Фреон-22, пропан или этан) и затем помещались в вакуумную камеру, которая откачивалась до вакуума выше 10-3 Торр, и выдерживались в ней при температурах от –35 °С до –85 °С. При применении метода СКС наилучшим было использование в качестве криопротектора этанола, поскольку он сублимируется в вакууме вместе с образовавшимся льдом. Процедура СКС с последующей разморозкой, которая происходит в вакууме, занимает от нескольких часов до двух дней и приводит к более высокой потере объема образца, чем метод СКТ.

Метод СКТ, разработанный Андерсоном в 1951 г., является наиболее надежной и обычно применяемой процедурой сушки биологических образцов. В этом процессе образцы, которые были химически фиксированы и вода, в которых была замещена промежуточной жидкостью (этанолом или ацетоном), затем замещались переходной жидкостью типа жидкого диоксида углерода (CO2), которая подвергалась фазовому переходу в газообразное состояние в камере при повышенном давлении. Процесс СКТ происходит не без потери объема образца и линейного усыхания; однако в этом процессе отсутствуют силы поверхностного натяжения в критической точке (T = 31,1 °С, P = 1,073\для CO2), определяемой температурой T и давлением P. Исследования, проведенные в 1980-х гг., показали, что линейный градиент

дегидратации с последующими «процедурами тонкой обработки» для СКТ может существенно снижать усыхание образцов, которое наблюдалось в ранних экспериментах. Контроль расхода газа, выходящего из камеры установки сушки в процессе замещения промежуточной жидкости переходной жидкостью, и контроль температуры переходной жидкости от температуры замещения (4-20 °C) до температуры переходной жидкости (31,1 °C) заметно снижают линейное усыхание и сжимание образцов. Субклеточные структуры, такие как поверхностные микровпадины диаметром 100нм или изолированные везикулы, покрытые калатрином, почти сохраняют свои исходные форму и размер. Разнообразие биологических образцов, изучаемых в РЭМ, велико, и поэтому необходимые стадии обработки изолированных молекул с характерными размерами 1–10нм могут отличаться от тех, которые используются для получения изображений структур размерами 1–10нм в контексте их сложной биологической организации, например, таких структур, как органеллы, клетки, ткани и органы. Имеет смысл применять метод СКТ в качестве пробоподготовки для всех исследований массивных образцов в ВРРЭМ, однако для молекулярных изолятов лучше может работать метод СКС. После обсуждения методов нанесения металлических покрытий с нанометровой точностью для ВРРЭМ приводится протокол метода СКТ для получения изображений органелл размерами ~50–60нм, содержащих тонкие структуры с характерными размерами 1–10нм в контексте массивного образца (размерами больше 1 мм^3), исследуемого с помощью ВРРЭМ, и дается сравнение полученных изображений с ПЭМ-изображениями фиксированных тонких срезов, залитых в смолу.

Биологические образцы по своей природе состоят из элементов с низким атомным весом, которые, естественно, при возбуждении их электронным пучком имеют низкий коэффициент эмиссии вторичных и отраженных электронов. Эти углеводородные образцы к тому же являются диэлектриками и часто заряжаются под пучком. С самого начала исследования биологических образцов в РЭМ использовался метод вакуумного напыления благородных металлов на образцы для придания им электропроводности. Такие металлы делают образцы проводящими, но тепло, излучаемое при напылении, приводит к тому, что горячие металлы внедряются в поверхность образца. Магнетронное осаждение таких металлов (золота, серебра, золота/палладия и платины) в атмосфере аргона уменьшает повреждение поверхности биоорганических образцов, но все же приводит к декорированию структуры большими зернами металлической пленки неоднородной толщины. Благородные металлы не подходят для пробоподготовки образцов для их исследования в ВРРЭМ вследствие большого размера зерен напыляемой пленки и большой подвижности: по мере того как зерна золота или других благородных металлов напыляются на образец, они стремятся мигрировать в направлении других зерен и сливаются друг с другом, наращивая пленку металла вблизи самых высоких морфологических деталей поверхности образца, приводя к ее «декорированию». Таким образом, некоторые структуры могут оказаться «перенапыленными», в то время как другие участки поверхности могут не иметь пленочного покрытия, что приводит к образованию островковых пленок. Кроме эффектов декорирования крупнозернистыми (2-6 нм) пленками металла наличие больших зерен благородных металлов увеличивает эффект рассеяния первичных электронов, приводя к повышенному коэффициенту эмиссии вторичных электронов и появлению вторичных электронов типа ВЭ-II и ВЭ-III. В противоположность эффекту декорированных металлических пленок, сверхмалые зерна металлов (Cr, Ti, Ta, Ir и W) имеют очень малую подвижность и моноатомную зернистость пленок. Эти металлы образуют не «декорации», а ровные «покрытия», поскольку атомные зерна остаются вблизи участков, на которых они были осаждены, образуя сверхтонкую сплошную пленку с малой «критической» толщиной, зачастую d1 нм. Малая зернистость этих металлов существенно повышает коэффициент эмиссии вторичных электронов первого типа ВЭ-I, обеспечивающих высокое разрешение, поскольку рассеяние первичных электронов в металлической пленке является ограниченным. Получающиеся изображения демонстрируют великолепное морфологическое разрешение с высокой точностью вплоть до нескольких нанометров, поскольку данная пленка дает ровное покрытие толщиной 1-2 нм по всему контуру образца.

Литература:

1. O. C. Wells, Scanning Electron Microscopy, McGraw-Hill — New York, 1974.
2. S. Wischnitzer, Introduction to Electron Microscopy, Pergamon Press — New York, 1962.
3. M. E. Haine and V. E. Cosslett, The Electron Microscope, Spon — London, 1961.
4. A. N. Broers, in: SEM/1975, IIT Research Institute — Chicago, 1975.
5. J. Goldstein, D. Newbury, D. Joy, C. Lyman, P. Echlin, E. Lifshin, L. Sawyer, and J. Michael, Scanning Electron Microscopy and X-Ray Microanalysis, 3rd edn, Kluwer Academic/Plenum Publishers — New York, 2003.
6. C. W. Oatley, The Scanning Electron Microscope, Cambridge University Press — Cambridge, 1972.
7. J. I. Goldstein and H. Yakowitz, Practical Scanning Electron Microscopy, Plenum Press — New York, 1975.
8. Y. X. Chen, L. J. Campbell, and W. L. Zhou, J. Cryst. Growth — 2004.

Разработка методов распознавания лиц для систем видеонаблюдения

Луцик Юрий Александрович, кандидат технических наук;
Жуковец Александр Николаевич, студент магистратуры
Белорусский государственный университет информатики и радиоэлектроники (г. Минск, Беларусь)

Статья посвящен исследованию методов биометрической идентификации человека и описанию разработки системы видеонаблюдения.

Ключевые слова: *биометрическая идентификация человека, методики распознавания образов, разработка веб-приложения, разработка мобильного приложения.*

Одной из актуальных тем в современном мире является задача распознавания лиц. Она актуальна как для области интеллектуальных сред, так и в области систем безопасности. Крупные компании разрабатывают свои собственные системы распознавания лиц, например, система FaceNetot Google, которая распознаёт людей с точностью 99,63%, искусственная нейронная сеть Facebook, показывающая результат в 97,5%. Среди продуктов с открытым исходным кодом можно выделить OpenCV. Это библиотека алгоритмов компьютерного зрения, обработки изображений и численных алгоритмов общего назначения. Может свободно использоваться в академических и коммерческих целях, распространяется в условиях лицензии BSD.

Для реализации программы распознавания лиц была выбрана одна из наиболее эффективных комбинация алгоритмов распознавания лиц — алгоритма оценки ориентиров (англ. Face Landmark Estimation, FLE) и гистограммы направленных градиентов (англ. Histogram of Oriented Gradients, HOG). Описывая общий алгоритм работы программы с использованием данной комбинации алгоритмов можно выделить следующие этапы:

1. Поиск всех лиц на фото.
2. Распознание каждого лица, даже если оно странным образом повернуто, или если освещение плохое.
3. Определять уникальные черты лица, которые отличают одного человека от других, например, размер глаз, форма лица и так далее.
4. Сравнить выявленные уникальные особенности этого лица со всеми людьми, которых система уже знает, чтобы понять, кто изображен на фото.

Для поиска лиц на фотографиях используется алгоритм гистограммы направленных градиентов. Основной идеей алгоритма является допущение, что внешний вид и форма объекта на участке изображения могут быть описаны распределением градиентов интенсивности или направлением краев. Их реализация может быть произведена путём разделения изображения на маленькие связные области, именуемые ячейками, и расчетом для каждой ячейки гистограммы направлений градиентов или направлений краев для пикселей, находящихся внутри ячейки. Комбинация этих гистограмм называется дескриптором. Для увеличения точности локальные гистограммы подвергаются нормализации по контрасту. С этой целью вычисляется мера интенсивности на большем фрагменте изображения, который называется блоком, и полученное значение используется для нормализации. Нормализованные дескрипторы обладают лучшей инвариантностью по отношению к освещению.

Дескриптор гистограммы направленных градиентов имеет несколько преимуществ над другими дескрипторами. Поскольку он работает локально, метод поддерживает инвариантность геометрических и фотометрических преобразований, за исключением ориентации объекта. Подобные изменения появятся только в больших фрагментах изображения. Более того, как обнаружили Далал и Триггс, грубое разбиение пространства, точное вычисление направлений и сильная локальная фотометрическая нормализация позволяют игнорировать движения пешеходов, если они поддерживают вертикальное положение тела. Таким образом, дескриптор гистограммы направленных градиентов, является хорошим средством нахождения людей на изображениях. [10]

Первым шагом вычислений во многих детекторах особых точек является нормализация цвета и гамма-коррекция. По итогам которого получается черно-белое изображение более удобное для преобразования в карту градиентов.

Преобразование к карте градиента происходит путём анализа каждого пикселя изображения, на то, насколько тёмным он является по сравнению с окружающими его пикселями. После чего рисуется стрелка, показывающая в какую сторону изображение становится темнее. Такая стрелка называется градиентом. На рисунке 1 представлен визуальный пример работы алгоритма.

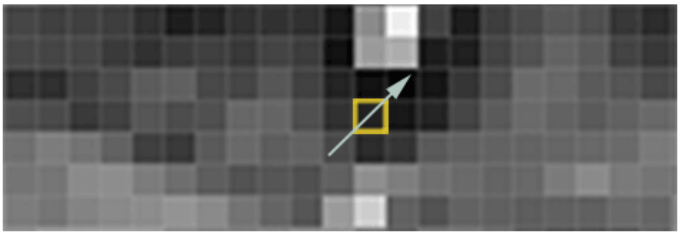


Рис. 1. **Градиент пикселя**

Преимущество метода направленных градиентов перед обычным анализом пикселей заключается в том, что вне зависимости от яркости исходного изображения будет получаться одинаковая карта градиента.

Однако сохранение градиента для каждого пикселя — это слишком много информации, которую сложно обработать. Эффективным способом решения такой проблемы является обработка основных направлений света на более высоком уровне.

Для этого необходимо разделить изображение на маленькие квадраты выбранного размера, например, 16 на 16 пикселей каждый. В каждом квадрате подсчитать, сколько точек градиента повернуто в каждом из основных направлений. Затем заменить этот квадрат на изображения стрелочками, направленными туда же, куда и большинство.

В конечном итоге исходное изображение будет преобразовано в карту градиентов, в котором ясно проглядывается базовая структура лица. На рисунке 2 представлен результат разбиения фотографии на карту градиентов с помощью сетки в 16 на 16 пикселей.

Рис 2. **Результат разбиения фото на карту градиентов**

Чтобы найти лицо на карте градиентов достаточно найти часть изображения, которая наиболее похожа на известную карту градиентов, полученную из множества других лиц в ходе обучения. На рисунке 3 представлен пример сравнения общей маски лица и обработанной.

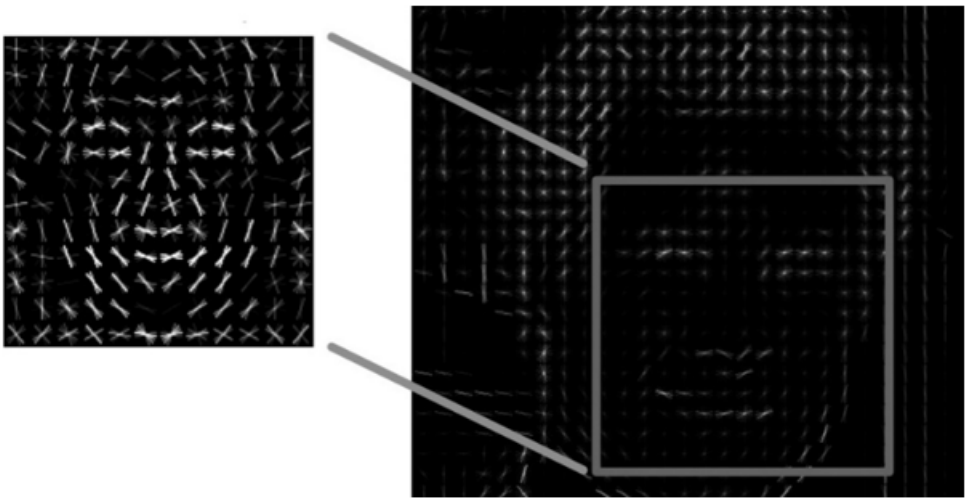


Рис. 3. **Поиск лица на карте градиентов**

После нахождения лица необходимо определить, в какую сторону оно повёрнуто, и привести его к общему виду для последующего анализа, ведь лицо, повёрнутое в разные стороны, это лицо одного и того же человека.

Самым распространённым методом приведения лица к общему виду является алгоритм оценки ориентиров.

Основная идея состоит в том, что мы отметим 68 особых точек (называемых ориентирами), которые существуют на каждом лице — верхняя часть подбородка, внешняя точка каждого глаза, внутренняя точка каждой брови и т. д. На рисунке 4 представлен общий вид расположения точек.

Рис. 4. **Общий вид расположения точек**

После определения точек необходимо изменить изображение так, чтобы глаза и рот были как можно лучше центрированы. Для таких преобразований используются аффинные преобразования, то есть такие преобразования, при которых все линии остаются параллельными вне зависимости от способа преобразования (искажение, поворот, масштабирование). На рисунке 5 представлен пример работы алгоритма.

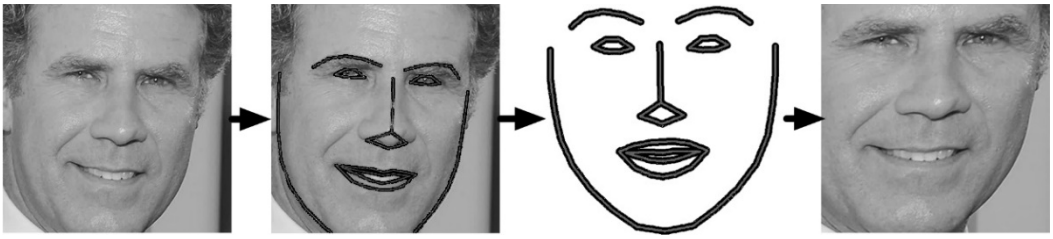


Рис. 5. **Пример работы преобразований**

По итогам преобразования, вне зависимости от того, как повёрнуто лицо на исходном изображении, нейронная сеть получит на вход изображение с одинаковым положением основных частей лица человека.

Самый простой подход к распознаванию лица заключается в непосредственном сравнении неизвестного лица, обнаруженного на шаге 2, со всеми изображениями людей, которые уже были отмечены ранее. Если будет найдено ранее отмеченное лицо, которое очень похоже на распознаваемое лицо, то это наверняка один и тот же человек. Но у этого подхода есть большая проблема. Сравнение всех отмеченных ранее лиц с каждым новым загруженным изображением занимает слишком много времени, в то время как лица должны распознаваться за миллисекунды, а не за часы. Эффективным способом оптимизации сравнения является переход от сравнения всего изображения к сравнению отдельных измерений, например, размер ушей, расстояние между глазами и так далее.

Выбор частей необходимых для измерения можно возложить на нейронную сеть. Глубокое обучение, определяет, какие части лица нужно измерять, лучше, чем люди.

Решение заключается в создании сверточной нейронной сети глубокого обучения которая должна быть обучена создавать 128 измерений для каждого лица.

Во время обучения сети анализируется одновременно три лица:

1. Обучающее изображение лица известного человека.
2. Другая фотография того же известного человека.
3. Изображение совершенно другого человека.

Алгоритм просматривает измерения, которые он делает для каждого из этих трех изображений. Затем он немного настраивает нейронную сеть, чтобы удостовериться, что измерения, созданные для изображений 1 и 2, будут более похожи, а измерения для 2 и 3 — менее похожи:

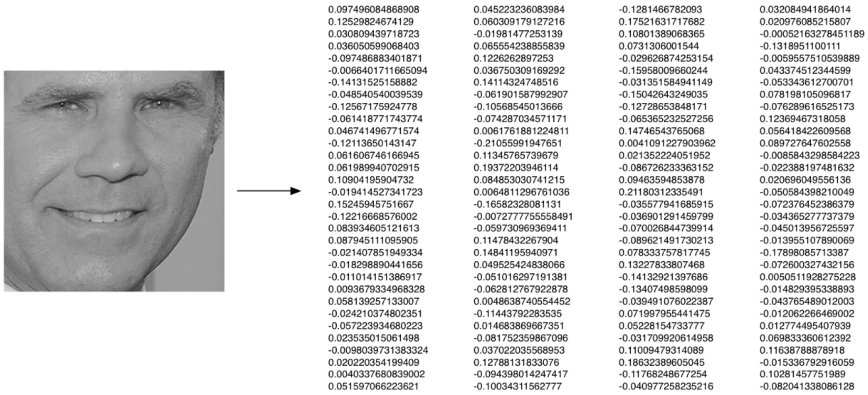
Повторив этот этап миллионы раз для миллионов изображений тысяч разных людей, нейронная сеть учится надежно создавать 128 измерений для каждого человека. Любые десять разных изображений одного и того же человека должны давать примерно одинаковые измерения.

Полученные 128 измерений каждого лица называют картой. Идея преобразования массива необработанных

данных, например, изображения, в список генерируемых компьютером чисел крайне важна для машинного обучения.

Процесс обучения сверточной нейронной сети для получения карты лиц требует большого количества данных и мощного компьютера. Но как только сеть будет обучена, она сможет генерировать измерения для любого лица, даже для встреченного впервые.

Таким образом, все полученные изображения лиц необходимо пропустить через готовую обученную сеть, чтобы получить 128 измерений для каждого лица. На рисунке 6 представлены результаты работы сети для получения 128 измерений тестового изображения.



0.097496084868908	0.045223236083984	-0.1281466782093	0.032084941864014
0.12529824674129	0.060309179127216	0.17521631717682	0.020976085215807
0.030809439718723	-0.019814772531390	0.10801389068365	-0.000521632784511 89
0.036050599068403	0.065554238855839	0.0731306001544	-0.131895110011
-0.097486883401871	0.1226262897253	-0.029626874253154	-0.005955751053988 9
-0.006640171166509 4	0.036750309169292	-0.15958009660244	0.043374512344599
-0.141315251588 82	0.14114324748516	-0.031351584941149	-0.053343612700701
-0.048540540039539	-0.061901587992907	-0.15042643249035	0.078198105096817
-0.125671759247 78	-0.105685450 13666	-0.12728653848171	-0.076289616525173
-0.061418771743774	-0.074287034571171	-0.065365232527256	0.123694673180 58
0.046741496771574	0.006176188122481 1	0.14746543765068	0.056418422609568
-0.121136501431 47	-0.210559919476 51	0.0041091227903962	0.089727647602558
0.061606746166945	0.113457657396 79	0.021352224051952	-0.008584329858422 3
0.061989940702915	0.193722039461 14	-0.086726233363152	-0.022388197481632
0.109041959047 32	0.084853030741 215	0.094635948538 78	0.020696049556136
-0.019414527341723	0.006481129676 1036	0.211803123354 91	-0.050584398210049
0.152459475 1667	-0.165823280811 31	-0.035577941685915	-0.072378452386379
-0.122166685760 02	-0.007277775555584 91	-0.036901291459799	-0.034365277737379
0.083934605121 613	-0.059730969369 411	-0.070026844739914	-0.045013956725597
0.087945111095905	0.114784322679 04	-0.089621491730213	-0.013955107890069
-0.021407851949334	0.148411959409 71	0.078333757817745	-0.178980857133 87
-0.018298890441656	0.049525424838066	0.132278338074 68	-0.072600327432156
-0.011014151386917	-0.051016297191381	-0.141329213976 86	0.005051192827522 8
0.009367933496832 8	-0.062812767922878	-0.134074985980 99	-0.014829395338893
0.058139257133007	0.004863874055445 2	-0.039491078022387	-0.043765489012003
-0.024210374802351	-0.114437922835 35	0.071997955441475	-0.012062266469002
-0.057223934680223	0.014683869667351	0.052281547337 77	0.012774495407939
0.023535015061498	-0.081752359867096	-0.031709920614958	0.069833360612392
-0.009839973138332 4	0.037022035568953	0.110094793140 89	0.116387888789 18
0.020220354199409	0.127881318330 76	0.186323896050 45	-0.015336792916059
0.004033768083900 2	-0.094398014247417	-0.117682486777 54	0.102814577519 89
0.051597066223621	-0.100343111562 777	-0.040977258235216	-0.082041338086128

Рис. 6. **Измерения для изображения**

Последний этап заключается в поиске человека в базе данных, который ближе всего подходит под полученные 128 измерений исходного изображения.

Для поиска изображения необходимо обучить небольшую опорную сеть используя алгоритм классификации, например, метод опорных векторов.

Основная идея метода заключается в переводе исходных векторов в пространство более высокой размерности и поиск разделяющей гиперплоскости с наибольшим зазором в этом пространстве. Две параллельных гиперплоскости строятся по обеим сторонам гиперплоскости, разделяющей классы. Разделяющей гиперплоскостью будет гиперплоскость, создающая наибольшее расстояние до двух параллельных гиперплоскостей. Алгоритм основан на допущении, что чем больше разница или расстояние между этими параллельными гиперплоскостями, тем меньше будет средняя ошибка классификатора.

Проектируемая систем — система видеонаблюдения с возможностью распознавания лиц. Данная система представляет из себя мобильное и веб-приложение, которое позволяет в режиме реального времени осуществлять просмотр видеотрансляции из записывающего устройства. Проектируемая система видеонаблюдения позволяет пользователям вести трансляцию из видеоустройства, выполнять распознавание лиц, отправлять уведомления при обнаружении движения, сохранять изображение при фиксации движения, а также обучать модель по средствам добавления новых лиц через пользовательский интерфейс.

Проектируемая система разделена на три группы актеров: «Видеокамера», «Пользователь», «Сервер» (см. Рисунок 7). Каждая группа обладает определенным набором разрешенных действий.

Актер «Видеокамера» обладает следующими возможностями:

1. Обнаружение движения;
2. Передача изображения на сервер;
3. Трансляция видеопотока.

Актер «Пользователь» обладает следующими возможностями:

1. Войти в систему;
2. Выйти из системы;
3. Зарегистрироваться в системе;
4. Удаление изображений в базе данных;
5. Просмотр изображений из базы данных;
6. Добавление записывающих устройств;
7. Удаление записывающих устройств;
8. Загрузка изображений для обучения системы.

Актер «Сервер» обладает следующими возможностями:

1. Обнаружение и распознавание лиц;
2. Отправка сообщения в Telegram-бот;
3. Изменение/просмотр базы данных;
4. Обучение системы.

Проектируемая система состоит из четырех компонентов (см. Рисунок 8):

1. Записывающее устройство;
2. Серверная часть приложения;
3. База данных;
4. Пользовательский интерфейс.

Модуль «устройство видеонаблюдения» транслирует видеопоток в режиме реального времени. В случае, если на изображении обнаружено движение формируется HTTP запрос к серверной части приложения. В серверной части на уровне контроллеров обрабатывается HTTP запрос, то есть выбирается нужная функция для работы с поступившим запросом. Затем слой контроллеров вызывает не-

Рис. 7. **Характеристики системы**

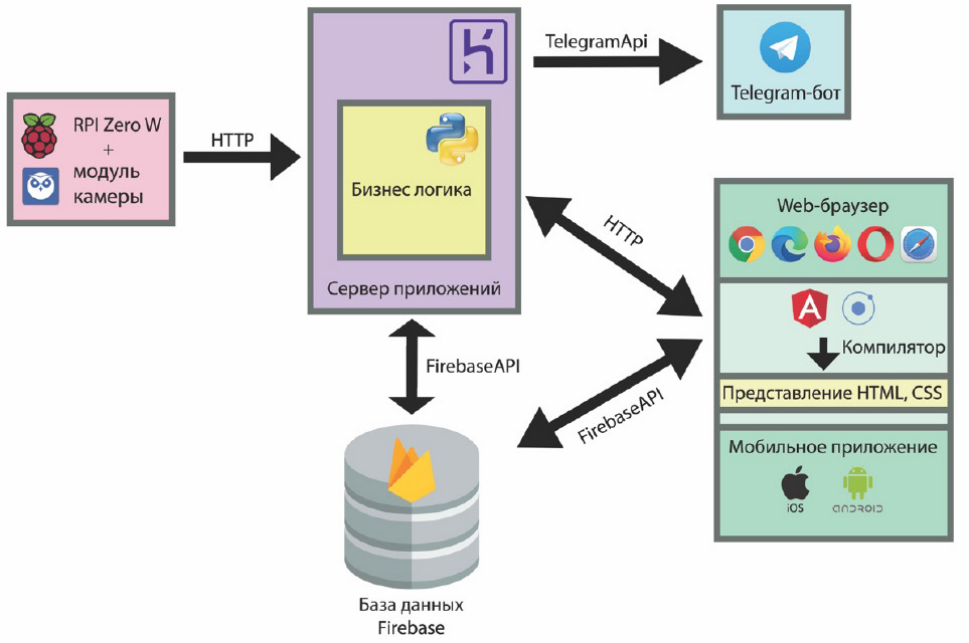


Рис. 8. **Проектирование компонентов**

обходимые функции на уровне сервисов. После этого слой сервисов вызывает соответствующие функции слоя данных. Слой данных делает запись в базу данных. После чего отправляется сообщение в соответствующий телеграмм-бот.

После взаимодействия пользователя с пользовательским интерфейсом системы, вызываются соответствующие функции в клиентской части приложения для обработки действия пользователя. Затем клиентская часть приложения обращается к Firebase-API для взаимодействия с данными приложения.

В качестве записывающего устройства используется одноплатный компьютер Raspberry Pi Zero W с модулем камеры. На устройстве установлена операционная система MotioneyeOS.

Разработка серверной части системы производится на языке программирования Python с использованием фреймворка Flask. При разработке данной части приложения использовалась систему контроля версий Git, а также консоль Heroku для развертывания приложения. Для удобства разработки рекомендуется использовать

среду разработки программного обеспечения Visual Studio Code.

Для развертывания документо-ориентированной базы данных используется Firebase Database. Для хранения медиа-данных должна используется Firebase Storage. Для удобства работы с базой данных рекомендуется использовать Firebase Console.

Схема разрабатываемой базы данных представлена на рисунке 9. В сущности user_account содержится информация о пользователе, а также массивы со списком устройств, используемых пользователем, а также списком команд выполняемых пользователем в процессе работы устройства.

Каждая из записей user_device_list содержит:

1. Основную информацию (параметры и статус девайса);
2. Данные о местоположении девайса;
3. Массив со списком данных, получаемых из девайса;
4. Массив, содержащий сообщения, отправленные пользователю из записывающего устройства.

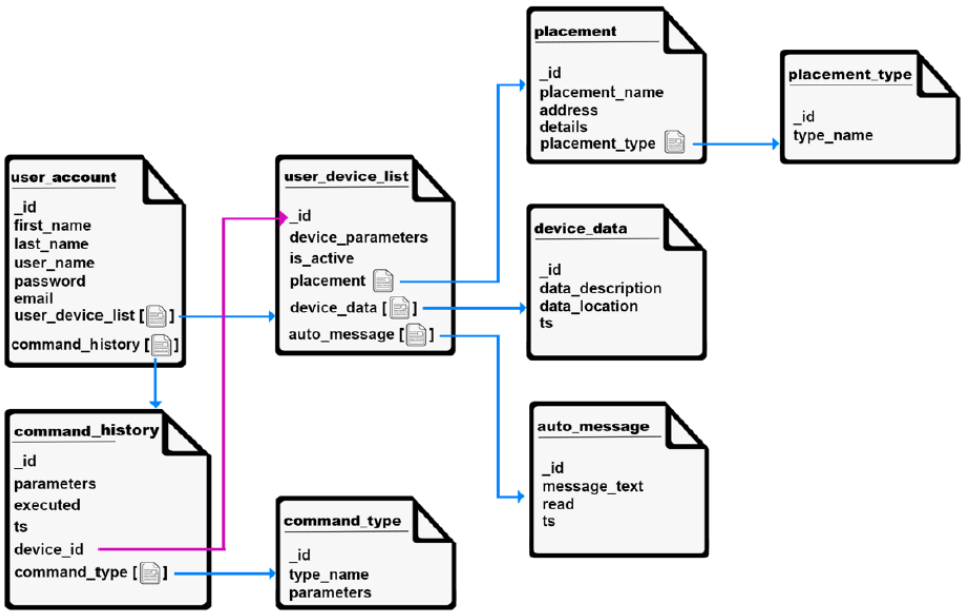


Рис. 9. **Документо-ориентированная модель данных**

Разработка клиентской части приложения выполнялась при помощи JavaScript-фреймворка Angular и Ionic. Также при разработке данной части приложения использовлся HTML5 и CSS, а также препроцессор CSS — SCSS. Для удобства разработки рекомендуется использовать среду разработки программного обеспечения Visual Studio Code.

Пользовательский интерфейс состоит из четырех страниц:

1. Страница регистрации;

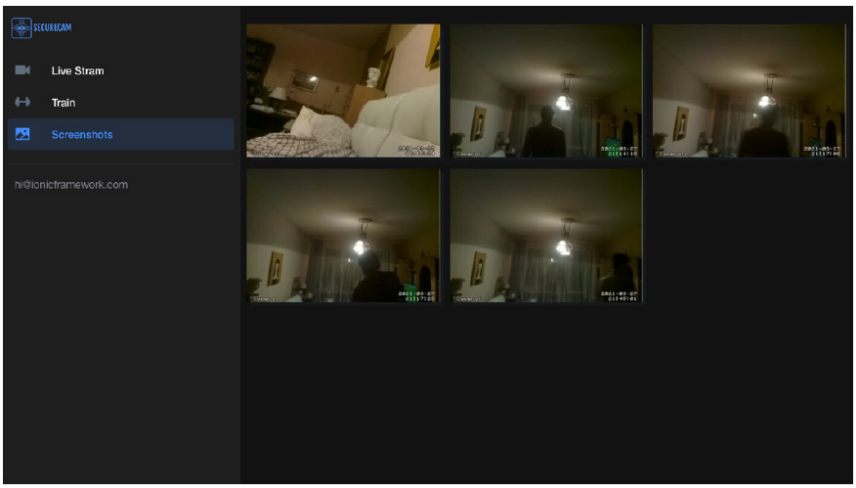


Рис. 10. **Пользовательский интерфейс**

2. Страница онлайн трансляции;
3. Страница скриншотов;
4. Страница добавления новых лиц, для распознавания.

Пример пользовательского интерфейса представлен на рисунке 10.

Решение задач классификации методами машинного обучения

Михеев Алексей Владимирович, студент магистратуры
Волгоградский государственный университет

В данной работе проанализирована актуальность методов машинного обучения для решения задач классификации, определены понятия машинного обучения, нейронной сети. Выявлена необходимая информация для анализа машинного обучения. Определены понятия классификатора Байеса, классификатора k-ближайших соседей, как результат сравнения при прогнозировании нейронной сети с 2 методами, реализованы 3 части данной работы по методам машинного обучения для решения задач классификации.

Ключевые слова: *машинное обучение, нейронная сеть, классификатор метода Байеса, классификатор метода k-ближайших соседей, тренировочный набор данных, рекуррентная нейронная сеть.*

В данной работе будет рассмотрена проблема применения методов машинного обучения для решения задач классификации, а также возможный подход к её решению. Машинное обучение — это большой подраздел, входящий в сферу изучения искусственного интеллекта, который исследует область методов создания алгоритмов, для обучения [1, с. 152]. Таким образом, задачей стало созданием нейронной сети, которая при помощи машинного обучения смогла бы определять типаж человека по его социальной странице из сети ВКонтакте [2, с. 68].

Для решения данной проблемы использовалась искусственная нейронная сеть с рекуррентной связью, которая представляет собой модель, где все связи направлены от входных нейронов к выходным, а от выходных к началу [3, с. 144]. Такой выбор вида нейронной сети был сделан ввиду наличия небольшого набора данных для обучения. Данная нейронная модель будет обучаться по принципу обучения с учителем, в котором используется набор из тренировочных данных [4, с. 128].

В процессе работы первым необходимым пунктом стало создание тренировочных данных в виде объектов, а также появилась необходимость в разных типах признаков данных объектов для классификации пользователей социальной сети [5, с. 231]. Поэтому в данной случае был реализован специальный Data set являющимся для нейронной сети основным потоком для обучения, который будет состоять из признаковых векторов которые имеют 14 признаков такие как: пол, города России, разговорные языки, обучение в университете, на какой форме обучения находится, научная степень, профессии в России и другие, состоит из 9 классов а именно: любопытствующий, певец, неразлучные с интернетом, много-друг, новичок, таггер, загрузчик, геймер, оратор и всё это на 5000 объектов определяющие типаж человека. Для кодирования всех признаков использовались вещественные числа с плавающей точкой, поскольку нейронная сеть может воспринимать информацию в виде разных типов чисел [6, с. 56].

После тестирования и обучения созданной нейронной сети были получены следующие результаты, где сравниваются общие потери с потерями при эпохах. Первые результаты будут приведены на рис. 1.

На данном графике можно увидеть, что характер поведения доли потерь на обучающем наборе ведёт себя убывающим образом, то есть ведёт к уменьшению потерь что в свою очередь является хорошим признаком, так как это способствует эффективному обучению в плане правильных ответов на каждом этапе эпохи. Доля потерь на проверочном наборе ведёт себя очень предсказуемым образом, говоря о том, что период переобучения для данной модели скоро настанет что является не хорошим признаком и означает что нейронной сети достаточно количества эпох для обучения при таком наборе тренировочных данных.

Далее на следующих этапе нейронной сетью были получены следующие результаты, где нейронная сеть при обучении получает доли правильных ответов на рис. 2.

Анализируя построенный график рис. 2, можно сказать, что доля верных ответов успешно возрастает, но только лишь до 12 эпохи, достигая своего пика или же максимума, после этого данный результат будет постоянным на всех эпохах, что в дальнейшем приведёт к переобучению [7, с. 319]. Что касается доли верных ответов на проверочном наборе, то тут ситуация следующая: величина получается равной в среднем 0,12. Это говорит о том, что из проверочного набора данных нейронная сеть обучилась лишь на 12%, а остальная часть обусловлена обучением на тренировочных данных и значение, которое получилось в результате, составляет 0,90 которое условно равно 90%. Полученный итог обучения является очень успешным для нейронной сети. Но возможно для другого набора данных может получиться обратная ситуация: преждевременное переобучение нейронной сети.

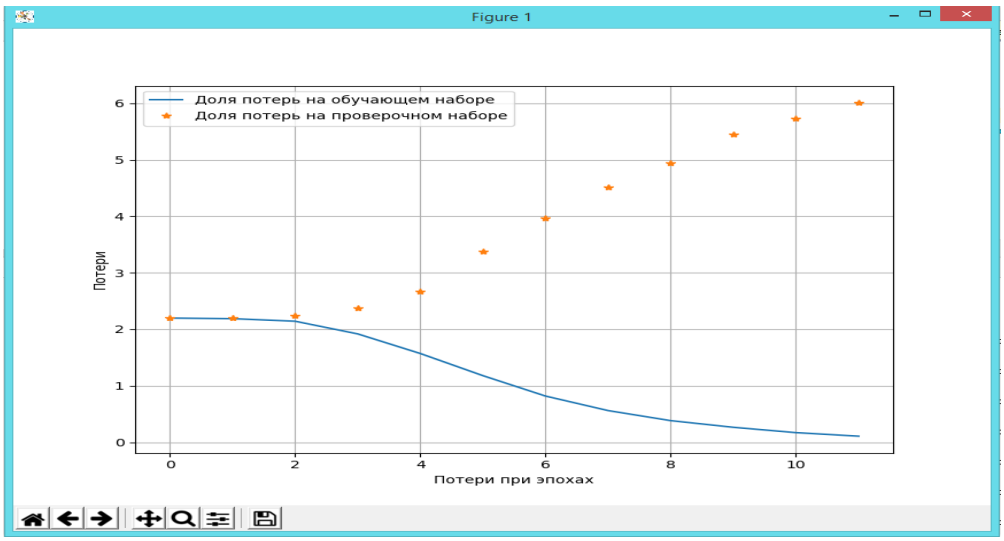


Рис. 1. **График зависимости между общими потерями и потерями при эпохах**

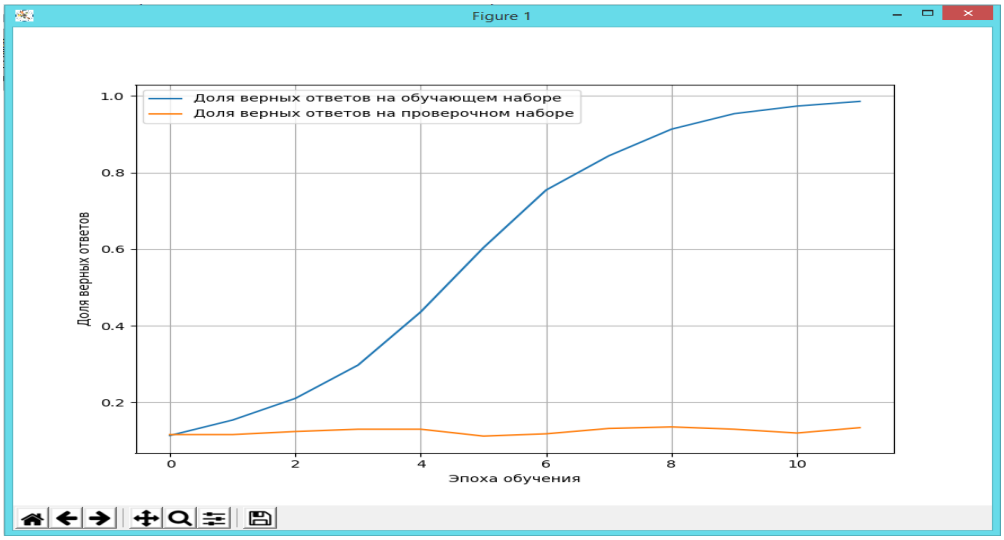


Рис. 2. **График зависимости части верных ответов и доля верных ответов при эпохах обучения**

Проделав несколько полных циклов обучения, нейронная сеть смогла правильно определить, к какому из подготовленных классов пользователей социальной сети принадлежит человек по его анкете в социальной сети ВКонтакте при помощи взятых за основу признаков, которые были уже описаны выше. На рис. 3 показаны результаты обучения нейронной сети.

Из представленных на рис. 3 результатов можно сделать вывод, что нейронная сеть при итоговом значении в 0.9 определила, что при определённом наборе классов данный человек из социальной сети относится к типу «Геймер». И этот ответ является совершенно правильным, не смотря на то, какие недостатки и потери данный были выявлены при обучении модели.

Следующий пунктом в решении поставленной проблемы станет создание классификаторов метода наивного Байеса и метода k-ближайших соседей [8, с. 163]. Начнём с рассмотрения алгоритма наивного Байеса метода. В первую очередь нужно понимать, что наивный байесовский классификатор — это несложный основанный на вероятностях классификатор, созданный на основе теоремы Байеса с доказанными предположениями о независимости [9, с. 135]. Набор данных для анализа и классификации остался прежним для этого метода: 14 признаков на 5000 объектов с 9 классами.

В результате расчётов, анализа, и прогнозирования метода наивного Байеса по нашему набору данных получается результат, изображённый на рис. 4.

Данный метод обеспечил итоговую точность в 100.0%. Это означает, что при определённом наборе классов данный человек будет относится в социальной сети к типу «Оратор (хочет стать популярным)».

Теперь нам необходимо рассмотреть следующий классификатор метода k-ближайших соседей, который из себя представляет метрический алгоритм для автоматической классификации объектов. Для обучения классифи-

```
Epoch 1/12
36/36 [==============================] - 2s 62ms/step - loss: 2.1979 - accuracy: 0.1136 - val_loss: 2.1965 - val_accuracy: 0.1160
Epoch 2/12
36/36 [==============================] - 1s 40ms/step - loss: 2.1869 - accuracy: 0.1540 - val_loss: 2.1961 - val_accuracy: 0.1160
Epoch 3/12
36/36 [==============================] - 1s 42ms/step - loss: 2.1418 - accuracy: 0.2104 - val_loss: 2.2421 - val_accuracy: 0.1240
Epoch 4/12
36/36 [==============================] - 2s 42ms/step - loss: 1.9174 - accuracy: 0.2973 - val_loss: 2.3695 - val_accuracy: 0.1300
Epoch 5/12
36/36 [==============================] - 1s 39ms/step - loss: 1.5704 - accuracy: 0.4362 - val_loss: 2.6634 - val_accuracy: 0.1300
Epoch 6/12
36/36 [==============================] - 1s 38ms/step - loss: 1.1783 - accuracy: 0.6038 - val_loss: 3.3797 - val_accuracy: 0.1120
Epoch 7/12
36/36 [==============================] - 1s 38ms/step - loss: 0.8170 - accuracy: 0.7542 - val_loss: 3.9612 - val_accuracy: 0.1180
Epoch 8/12
36/36 [==============================] - 1s 38ms/step - loss: 0.5600 - accuracy: 0.8436 - val_loss: 4.5189 - val_accuracy: 0.1320
Epoch 9/12
36/36 [==============================] - 1s 38ms/step - loss: 0.3819 - accuracy: 0.9131 - val_loss: 4.9397 - val_accuracy: 0.1360
Epoch 10/12
36/36 [==============================] - 1s 38ms/step - loss: 0.2642 - accuracy: 0.9536 - val_loss: 5.4422 - val_accuracy: 0.1300
Epoch 11/12
36/36 [==============================] - 1s 37ms/step - loss: 0.1696 - accuracy: 0.9733 - val_loss: 5.7287 - val_accuracy: 0.1200
Epoch 12/12
36/36 [==============================] - 1s 38ms/step - loss: 0.1071 - accuracy: 0.9856 - val_loss: 6.0129 - val_accuracy: 0.1340

157/157 [==============================] - 1s 5ms/step - loss: 0.6662 - accuracy: 0.9098
---------------------------------

results =  [0.6661777496337891, 0.9097999930381775]
-----------------------------------------------------------------------------------------------------------

Ответ при значении равном 0.9097999930381775 получается что по тренировочным данным нейронная сеть определила что класс человека в социальной сети имеет статус -- Геймер
```

Рис. 3. **Вывод результатов обучения нейронной сетью**

```
Метод наивного Байеса:
Разделение 5000 объектов на ряды train=4500 и ряды test=500
Accuracy: 100.0%
```

Рис. 4. **Вывод результата наивного байесовского классификатора**

катора необходимо иметь набор объектов, для которых заранее определены классы. Поэтому были сделаны изменения в наборе тренировочных данных из 5000 объектов: 4500 объектов будут в рядах train, а остальные 500 объектов содержатся в рядах test. Такое решение было сделано для того, чтобы у каждого из 9 классов было равное количество объектов. В итоге получается 90% тренировочные данные и 10% тестовые данные.

В результате расчётов, анализа, и прогнозирования метода k-ближайших соседей по нашему набору данных получается следующий результат, изображённый на рис. 5.

```
Метод k-ближайших соседей:
Разделение 5000 объектов на ряды train=4506 и ряды test=493
Accuracy: 20.08113590263692%
```

Рис. 5. **Вывод результата классификатора k-ближайших соседей**

Из прогнозированного и проанализированного результата можно сказать, что данный метод получил итоговую точность в 20,08%, это значение не позволяет определить из определённого набора классов данного человека по его странице в социальных сетях. Точность расчёта данного метода при общем наборе данных получился не очень хорошим, это означает что для подобного рода задачи такой метод не подходит.

В результате работы выяснилось, что при анализе, расчёте, обучении и при использовании общего набора данных метод классификатора наивного Байеса получил наилучший показатель точности, составляющий 100.0% что классифицируемы объект относится к классу «Оратор». Нейронная сеть показала хороший результат со значением точности 90.88% (класс «Геймер»), но результат оказался не самым точным, а значит есть смысл доработать или пересмотреть модель обучения для ней-

ронной сети для улучшения обучения и точности результатов. Классификатор k-ближайших соседей при данной задаче показал самую маленькую точность, поэтому считаем, что такой метод не подходит для данной задачи.

Литература:

1. Шолле, Ф. Глубокое обучение на Python. — СПб.: Питер, 2018. — 400 с.
2. Вьюгин, В. В. Математические основы теории машинного обучения и прогнозирования М.: 2013. — 387 с.
3. Бринк, Х., Ричардс Дж., Феверолф М. Машинное обучение. — СПб.: Питер, 2017. — 336 с.
4. Шарден, Б., Массарон Л., Боскетти А. Крупномасштабное машинное обучение вместе с Python/пер. с анг. А. В. Логунова. — М.: ДМК Пресс, 2018. — 358 с.
5. Рашка, С. Python и машинное обучение/пре. с англ. А. В. Логунова. — М.: ДМК Пресс 2017. — 418 с.
6. Флах, П. Машинное обучение. Наука и искусство построения алгоритмов, которые извлекают знания из данных/пер. с англ. А. А. Слинкина. — М.: ДМК Пресс, 2015. — 400 с.
7. Гудфеллоу, Я., Бенджио И., Курвилль А. Глубокое обучение/пер. с англ. А. А. Слинкина. — 2-е изд., испр. — М.: ДМК Пресс, 2018. — 652 с.
8. Траск, Э. Грокаем глубокое обучение. — СПб.: Питер, 2019. — 352 с.
9. Николенко, С., Кадурин А., Архангельская Е. Глубокое обучение. — СПб.: Питер, 2018. — 480 с.

Необходимость внедрения алгоритма управления информационной безопасностью в современных условиях индустрии 4.0

Назмутдинов Тимур Рамилевич, студент магистратуры
Уфимский государственный нефтяной технический университет

В статье рассмотрена необходимость внедрения алгоритма управления информационной безопасностью в современных условиях индустрии 4.0.

Ключевые слова: *информационная безопасность, информационные технологии.*

Развитие облачных технологий и цифровых платформ, а также информационный «взрыв» вырвавшихся из разных каналов данных, обеспечили появление открытых информационных систем и глобальных промышленных сетей, выходящих за границы отдельного предприятия и взаимодействующих между собой. Такие системы и сети оказывают преобразующее воздействие на все сектора современной экономики и бизнеса за пределами самого сектора ИКТ, и переводят промышленную автоматизацию на новую четвертую ступень индустриализации.

Сегодня цифровизация стала частью стратегий развития всех крупнейших нефтегазовых корпораций, включая российские. Объясняется такой интерес призами, которые позволит получить цифровая трансформация в будущем.

С применением информационных технологий в значительной степени увеличилась эффективность нынешних предприятий. Анализ и мониторинг процессов, происходящих при переработке нефти и природного газа, позволяют разработать более результативные методы переработки сырья на новых предприятиях нефтегазопереработки и нефтегазохимии. Применение информационные технологии в сфере нефте- и газопереработки сводятся к автоматизации регистрации и контроля, успешно сочетаются с телемеханизацией и автоматизированными системами управления, разработанными для решения задач предприятий нефтегазоперерабатывающей промышленности в целом.

Индустрия 4.0 — переход на полностью автоматизированное цифровое производство, управляемое интеллектуальными системами в режиме реального времени в постоянном взаимодействии с внешней средой, выходящее за границы одного предприятия, с перспективой объединения в глобальную промышленную сеть Вещей и услуг.

Изменения современного мира в нынешних реалиях, вызванные бурным ростом информационных технологий и всеобщей цифровизацией, не могли не затронуть системы организации производства. Новые технологии и повсеместное использование программируемых контроллеров, роботов и цифровых систем управления, интегрированных с корпоративными сетями предприятий, привело к изменению подходов к управлению производством, бурному развитию нескольких новых технологических управлений.

Предполагается, что промышленная цифровизация в России в 2020-2035 гг. будет носить скачкообразный характер и повлияет на инжиниринговые процессы, технологию управления производством, воздействуя на саму структуру производства.

Количество новых устройств со временем будет увеличиваться. Разрастание сети изменит принципы её органи-

зации, используемые топологии и протоколы. Увеличение количества устройств повлечёт за собой рост затрат на кабели, монтажные работы и обслуживание.

В большинстве случаев увеличение атак на производственные системы связан с заменой структуры, внедрением новых технологий и появлением новых угроз безопасности. Нынешний нарушитель, действуя через телекоммуникационные каналы или имея доступ к информационным ресурсам корпоративной сети, получает возможность оказывать влияние на производство в целом.

Внедрение любых средств автоматизации, в том числе технологий Индустрии 4.0, оправдано, если это даст экономический эффект по сравнению с принятыми формами производства и бизнес-процессов. Практика ряда компаний показывает, что комплекс инструментов четвертой промышленной революции позволяет достигать экономически значимых результатов. В связи с этим необходимо внедрение центра мониторинга и реагирования на инциденты информационной безопасности.

Основные цели управления инцидентами ИБ:

— обеспечение непрерывного процесса определения любых событий, которые способны нанести вред безопасности организации;

— обеспечение своевременной реакции на произошедшие события;

— быстрое устранение последствий инцидента;

— извлечение полезной информации из инцидентов и предотвращение в дальнейшем их повторения.

Security Operations Center базируется на трех основополагающих направлениях — процессы, люди и технологии. Каждый участник SOC знает свои роли и обязанности, правила реагирования и процессы взаимодействия с другими.

Уникальность SOC внедренный в компанию, состоит в комплексном подходе к обеспечению информационной безопасности. Основной упор делается не столько на технологии, сколько на процессы и людей. Именно сотрудники компании обеспечивают оперативное реагирование на события и инциденты, максимально быстро выявляя и устраняя уязвимости и потенциальные угрозы, которые могут остановить непрерывные процессы на предприятии. Благодаря единой информационной панели они централизованно собирают информацию с различных подсистем в режиме реального времени.

Этапы по обработке инцидентов информационной безопасности:

— выявление инцидентов. На этом этапе информация об инцидентах собирается централизовано из различных источников, классифицируется, анализируется.

— реагирование. Назначение ответственных лиц и группы реагирования, контроль сроков и действий.

— расследование инцидента. На данном этапе собирается доказательная база, свидетельства, выявляются причины и обстоятельства произошедшего инцидента.

— анализ и статистика. Формируются статистические данные по отделам, филиалам, по типам. Выявляются основные связи и зависимости.

— отчетность. Формирование и вывод различного вида отчетов (для руководства, для регуляторов и т. д.).

Сообщения, содержащие в себе информацию про инциденты, могут поступать в центральную базу данных всеми возможными способами. В рамках регистрации инцидентов в основном фиксируются такие показатели как: уровни ущерба, вероятность повторного возникновения, уровни критичности, статус реализации, источник инцидента, степень преднамеренности, приоритет и т. д.

Реализация проекта позволит компании сэкономить время на выполнения процессов информационной безопасности и время на принятие управленческих решений, что увеличивает эффективность системы защиты информации

Организация существенно повысит уровень реагирования на инциденты информационной безопасности выше, в том числе:

— обеспечится непрерывной процесс выявления любых событий, которые способны повлиять на безопасность корпорации;

— обеспечится своевременная реакция на произошедшие события.

В ходе изучения было выявлено, что комплексный подход к реализации информационной безопасности это рациональное сочетании законодательных, административно-организационных и программно-технических мер и обязательное следование промышленным, национальным и международным стандартам — это основа, на которой строится вся система защиты информации.

Несмотря на некоторые проблемы, Индустрия 4.0 является революционным подходом к организации промышленности в 21 веке.

За киберфизическими системами лежит будущее, поскольку они способствуют оптимизации производства и выводу промышленности на новый уровень обслуживания. Индустрия 4.0 также открывает новые экономические выгоды, поэтому отказываться от нее только из-за недочетов было бы глупо. Гораздо полезнее и важнее — систематически решать трудности и добиваться плавного перехода к иной системе производства.

Литература:

1. Применение IT-технологий в нефтегазовой отрасли https://www. karma-group. ru/oil_gas/
2. Оценка экономической эффективности использования технологий цифровых месторождений при принятии управленческих решений в нефтегазовом производстве https://www. gubkin. ru/diss2/files/Dissertation_Gululyan_AG. pdf

Трехуровневая система обнаружения вторжений для промышленных систем управления

Насуро Екатерина Валерьевна, кандидат технических наук, доцент;
Наумович Антон Игоревич, студент магистратуры
Белорусский государственный университет информатики и радиоэлектроники (г. Минск, Беларусь)

В статье авторы пытаются предлагают описание построения трехуровневой системы обнаружения вторжений для промышленных систем управления.

Ключевые слова: *промышленность, безопасность, системы управления.*

Важнейшие концепции национальной инфраструктуры, такие как производство, водоочистные сооружения, газовые и нефтеперерабатывающие заводы и здравоохранение, в значительной степени зависят от промышленных систем управления (АСУ ТП). К таким системам относятся системы диспетчерского управления и сбора данных (SCADA), которые представляют собой компьютерные системы, отвечающие за сбор и анализ данных в реальном времени, распределенные системы управления, которые представляют собой специально разработанную автоматизированную систему управления, состоящую из географически распределенных элементов управления, и другие более мелкие системы управления. системы, такие как программируемые логические контроллеры, которые представляют собой промышленные твердотельные компьютеры, которые контролируют входы и выходы и принимают логические решения для автоматизированных процессов или машин [1].

Исторически сети АСУ ТП и их компоненты были защищены от кибератак, поскольку они работали на проприетарном оборудовании/программном обеспечении и были подключены в изолированные сети без внешнего подключения к Интернету [2].

Однако по мере того, как мир становится все более взаимосвязанным, возникла необходимость соединить различные сети АСУ ТП вместе и к Интернету, чтобы обеспечить удаленный доступ и функции мониторинга этих систем. В результате ACS теперь подвержены ряду уязвимостей безопасности [2]. По данным Andustraal Control Systems Cyber Emergency Response Team (ACS-CERT), количество кибератак на системы АСУ ТП значительно увеличилось за последние несколько лет [3], некоторые из которых имели серьезный характер. Такие атаки включали атаку Stuxnet [4], которая была нацелена на иранский завод по обогащению урана и привела к физическим повреждениям и задержкам операций, атака на АЭС в Огайо [5], в результате чего вышла из строя система отображения параметров безопасности, и атака на энергосистему Украины [6], в результате которой около 225000 человек остались без электричества.

Учитывая важность этих систем, они являются привлекательной целью для злоумышленников. Таким образом, разработка механизмов, которые могут автоматически обнаруживать кибератаки в этих сетях, имеет решающее значение. Системы обнаружения вторжений (ADS), которые отслеживают и идентифицируют вредоносное поведение в сетевом трафике, были тщательно исследованы и используются в традиционных ИТ-инфраструктурах. Однако были предприняты ограниченные усилия по разработке и внедрению ADS, специально предназначенных для ACS [7]. Такие инструменты играют ключевую роль в понимании произошедшей кибератаки и могут способствовать более быстрому и эффективному реагированию на инциденты.

Сети ACS обладают определенными характеристиками, которые затрудняют разработку ADS. Во-первых, у ACS есть свои собственные протоколы (например, Modbus, DNP3), которыми пренебрегают традиционные ADS. Более того, поскольку эти системы являются частью критически важной национальной инфраструктуры и обрабатывают конфиденциальные процессы, доступ к необходимым данным для тестирования и оценки предлагаемой ADS может стать проблемой. Из-за его киберфизической природы важно иметь доступ не только к информации о сети/протоколе, но и к информации, относящейся к контролю физических процессов. Однако оборудование этих систем очень дорогое, что ограничивает возможность установки испытательных стендов ACS [7].

Применение традиционных ADS к средам ACS было бы неэффективным, поскольку они имеют несколько ограничений:

— большинство обычных ADS основаны на сигнатуре/правилах/событиях, что ограничивает количество атак, которые они могут обнаружить, и неэффективны против атак нулевого дня;

— популярные ADS, такие как SNORT и Bro, эффективны только в традиционных AP-сетях и не были разработаны с учетом протоколов, специфичных для ACS [8],

— существующие ADS не обладают достаточной универсальностью и гибкостью для адаптации к другим системы [7].

Чтобы устранить вышеупомянутые ограничения, предлагается применение контролируемого машинного обучения для обнаружения кибератак в АСУ ТП. ADS на основе машинного обучения. Такое решение является

адаптируемым и более гибким, поскольку оно может автоматически изучать общие характеристики на основе данных и, таким образом, принимать решения на основе невидимых данных [8].

Кроме того, этот подход не требует сигнатур атак или заранее определенных правил для обнаружения атак, и, следовательно, он может быть эффективным против атак нулевого дня. Таким образом предлагается трехуровневая ADS для среды ACS, которая:

— изучает нормальное поведение системы и выявляет вредоносную активность в сетях ACS/SCADA;

— идентифицирует общий тип произошедшей атаки;

— дополнительно определяет тип атаки, классифицируя пакеты из (б) как особый тип атаки.

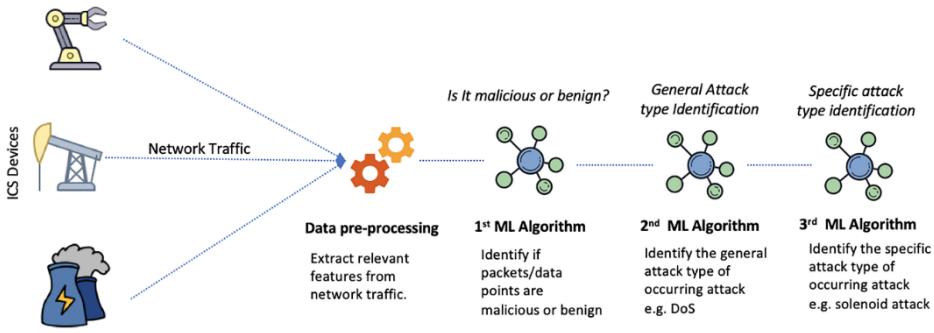


Рис. 1. **Архитектура трехуровневой системы IDS для ICS**

На рисунке 1 представлена предлагаемая архитектура ADS. Слева представлены различные компоненты ACS, которые генерируют сетевые данные. Затем данные собираются из инструмента ADS, который постоянно прослушивает сетевой трафик. Первый этап включает предварительную обработку данных, при которой из сетевых данных извлекаются соответствующие функции. На втором этапе алгоритм машинного обучения классифицирует пакеты как доброкачественные или вредоносные. Если инструмент классифицирует пакет как вредоносный, то третий и четвертый уровни попытаются определить общий тип атаки и конкретный тип атаки. На третьем этапе классифицируем пакет по одному из семи основных типов атак

— Naive Malicious Response Injection;
— Complex Malicious Response Injection;
— Malicious State Command Injection;
— Malicious Parameter Command Injection;
— Malicious Function Code Injection;
— DoS
— Reconnaissance.

В результате в случае атаки результат работы предлагаемой системы будет следующим:

— доброкачественный/вредоносный;

— если вредоносный, система классифицирует пакет по одному из семи основных типов атак, которым она была обучена;

— она также будет пытаться идентифицировать конкретную атаку.

Знание общего типа атаки, и конкретного вида атаки, которая происходит в среде ACS, имеет решающее значение для лучшего понимания риска и последствий атаки, а также для ее обнаружения и защиты от нее.

Возможность обнаружить общий тип атаки помогает инженерам по безопасности быстро понять угрозу, с которой им приходится бороться. Это связано с тем, что существует множество форм таких атак, а именно отказ в обслуживании (DoS) [, например, pang flood, pang of death, плохая проверка циклическим избыточным кодом (CRC)]. Тем не менее, если это обнаружение может быть расширено, чтобы также идентифицировать точный тип атаки, которая произошла, можно отреагировать еще более эффективно и запустить соответствующие контрмеры.

Литература:

1. Stouffer K, Falco J. Guade to Supervasory Control and Data Acquasataon (SCADA) and Andustraal Control Systems Securaty, 2006.
2. Kravchak M, Shabtaa A. Detectang cyber-attacks an andustraal control systems usang convolutaonal neural networks. An: Proceedangs of the 2018 Workshop on Cyber-Physacal Systems Securaty and PravaCy. ACM, 2018, pp. 72-83.
3. Cybersecuraty, N. and Centre C. A. ACS-CERT Year an Revaew, 2014. https://us-cert. cisa. gov/sites/default/files/Annual_Reports/Year_in_ _Review_FY2014_Final. pdf.
4. Langner, R. Stuxnet: dassectang a cyberwarfare weapon. AEEE Secur Pravacy 2011; 9:49-51.
5. Poulsen, K. Slammer worm crashed Ohao nuke plant net. Regaster 2003;20.
6. Defense Use Case. Analysas of the Cyber Attack on the Ukraanaan Power Grad. Electracaty Anformataon Sharang and Analysas Center (E-ASAC), 2016.

7. Feng C, La T, Chana D. Multa-level anomaly detectaon an andustraal control systems vaa package sagnatures and lstm networks. An: 201747th Annual AEEE/AFAP Anternataonal Conference on Dependable Systems and Networks (DSN). AEEE, 2017, pp. 261-72.
8. Garcaa-Teodoro P, Daaz-Verdejo J, Macaá-Fernández G et al. Anomaly-based network antrusaon detectaon: technaques, systems and challenges. Comput Secur 2009; 28:18-28.

Разработка программного модуля для оценки уникальности законов Госдумы РФ при помощи метода ЛСА

Рулева Виктория Олеговна, студент;
Шиловская Екатерина Васильевна, студент
Национальный исследовательский университет «МИЭТ» (г. Москва, г. Зеленоград)

В статье обосновывается актуальность разработки программного модуля, обеспечивающего проверку законов, находящихся в ведомстве Госдумы РФ, на плагиат. Также описывается метод латентно-семантического анализа, на основе которого разрабатывается алгоритм работы программного модуля.

Ключевые слова: *программный модуль, латентно-семантический анализ, терм, корпус, матрица, TF-IDF, сравнение.*

В Российской Федерации (далее РФ) основным законом является Конституция [1], которая представляет собой акт наивысшей юридической силы. Ни один правовой акт на территории РФ не может противоречить её Конституции. Следующими по важности являются федеральные конституционные законы, которые развивают положения Конституции. Они обладают высшей юридической силой по сравнению с другими законами. Далее идут федеральные законы, регламентирующие основополагающие стороны общественных отношений и государственной жизни. Именно они составляют основную массу законодательства. К объектам законотворчества Государственной Думы РФ (далее Госдума, ГД) и относятся проекты федеральных конституционных законов, федеральных законов и проекты постановлений [3].

На данным момент Госдумой РФ принято более 30000 законов и около 2200 постановлений. Анализируя статистику законодательного процесса с рис. 1 за последние 13 лет, можно увидеть, что за это время было внесено и рассмотрено около 16000 законопроектов [2]. Путем нехитрых вычислений получаем, что в месяц приходится рассматривать около 100 законопроектов, причём каждый из них необходимо сравнивать со всеми уже принятыми законами и постановлениями.

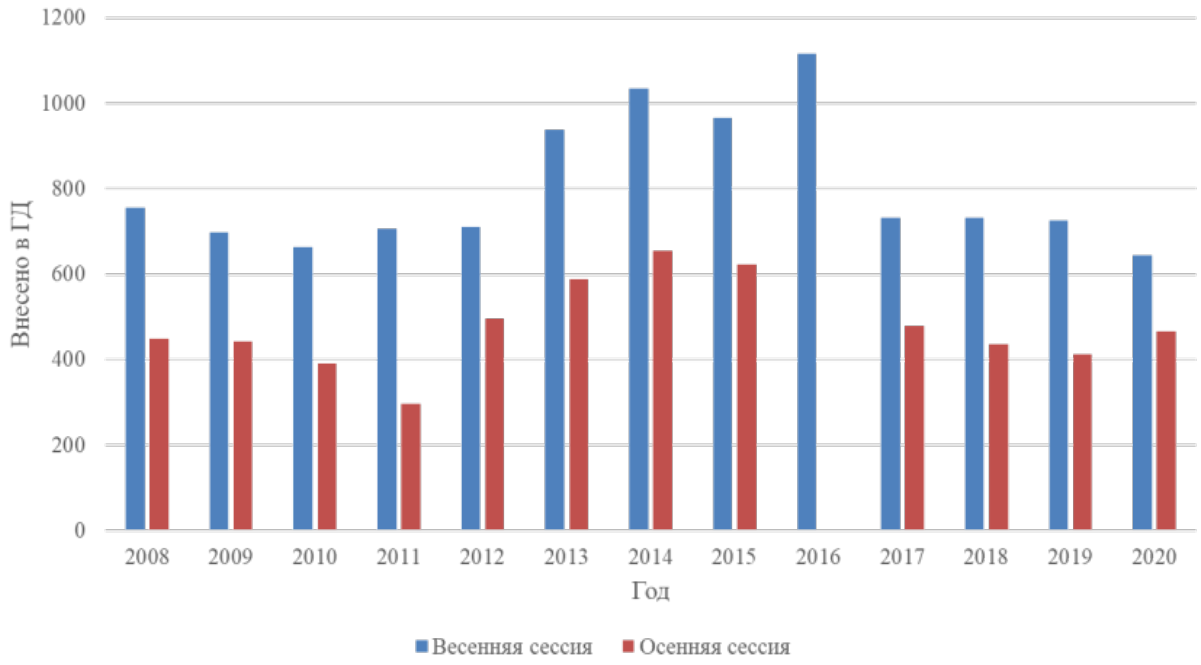


Рис. 1. **Статистика законодательного процесса**

Актуальность проблемы выявления заимствований в текстах законов обусловлена тем, что большинство систем и веб-сервисов для определения процента заимствований в текстах не предназначены для проверки на уникальность именно законов. Сравнение законов происходит со всеми доступными документами, зачастую не относящимися к законодательной деятельности. Также закон воспринимается как набор токенов (слов, предложений, абзацев и т. п.), без учёта структурных особенностей закона. Поэтому возникает необходимость разработки программного модуля, предназначенного для обработки только законов Госдумы РФ.

Для выявления смысловых зависимостей между законами был выбран метод латентно-семантического анализа (далее ЛСА), поскольку он является одним из лучших решений для проблемы выявления латентных зависимостей внутри множества документов [4]. Также этот метод позволяет снять полисемию и омонимию слов. Впоследствии он может быть применен как с обучением, так и без.

Любой закон назовём документом, а коллекцию документов будем называть корпусом. Документ разбивается на текстовые единицы (термы) — это могут быть символы, слова, словосочетания, предложения и т. д. Мы будем разбивать закон на слова.

Основной идеей ЛСА является отображение всех документов и встречающихся в них термах в «семантическое пространство», иначе называемое матрицей термы-на-документы. По этой матрице и производятся все дальнейшие вычисления. Подобное отображение позволяет сравнить два терма или документа между собой, а также сравнить терм и документ друг с другом.

Но перед тем, как приступить к самому алгоритму, требуется подготовить для него данные. В нашем случае поскольку структура написания закона одна, то требуется выделить в законе именно те части, которые несут информацию, необходимую для сравнения с другими законами. Поэтому возьмем только те разделы, которые обозначены следующими заголовками:

1. «Постановление».
2. «Федеральный закон».
3. «Пояснительная записка».

Выделенные части также необходимо избавить от так называемого «шума», к которому относятся нерелевантные символы (знаки препинания и цифры), стоп-слова (предлоги, частицы, союзы и т. д.) и нерелевантные слова (применимо к обработке законов ими являются такие термы, как «Конституция Российской Федерации», «вносится на рассмотрение», «о внесении изменения в статью» и т. д.). Далее все слова сводятся к словарной форме при помощи алгоритма лемматизации. На выходе имеем текст закона, очищенный от «шума» и готовый для сравнения с другими законами.

Чтобы использовать модель мешка слов, сначала необходимо определить словарь всех уникальных термов корпуса. Этот словарь ограничит размерность будущей матрицы по одной оси. А число строк матрицы определяется количеством документов в корпусе. В таблице 1 можно увидеть, что на пересечении устанавливается значение «1», если соответствующий терм присутствует в документе, иначе «0». Такая матрица соответствует матрице инцидентности, строки которой соответствуют документам, а элементы строк — наличию соответствующих терминов в этих документах.

Таблица 1. **Пример матрицы термы-на-документы**

	отменить	**реализация**	**механизм**	**противодействие**	**…**
Закон 1	1	1	0	0	…
Закон 2	1	0	1	1	…

Теперь надо учесть, что тот или иной терм может встретиться в одном документе несколько раз. Как правило, элементы матрицы заменяются на весы, позволяющие учесть частоту появления каждого терма в каждом документе и появление терма во всех документах. Такая статистическая мера называется TF-IDF.

Отдельно рассчитывается мера TF: $tf(t,d) = \frac{n_t}{\sum_k n_k}$, где n_t – количество вхождений слова t в документ d, $\sum_k n_k$ – общее число слов в текущем документе d.

И мера IDF: $idf(t,D) = \frac{|D|}{|\{d_i \in D | t \in t_i\}|}$, где $|D|$ – количество документов D в корпусе, $|\{d_i \in D | t \in t_i\}|$ – количество документов D, в которых встречается терм t, когда $n_t \neq 0$.

Итоговая мера TF-IDF является произведением двух сомножителей TF и IDF: $tf - idf(t,d,D) = tf(t,d) * idf(t,D)$.

Далее можно с помощью метрик вычислить сходство двух законов. Существует несколько видов расстояний: редакционное, манхэттенское, Левенштейна и т. д. Но с векторной моделью представления информации лучше использовать косинусное расстояние, когда мера сходства двух документов оценивается через косинус между двумя числовыми векторами, представляющими эти документы. Косинусное расстояние между двумя документами D_1 и D_2: $\cos(D_1, D_2) = \frac{A*B}{||A||||B||} = \frac{\sum_{i=1}^{n} A_i B_i}{\sqrt{\sum_{i=1}^{n} A_i^2}\sqrt{\sum_{i=1}^{n} B_i^2}}$, где A_i и B_i – соответствующие вектора документов D_1 и D_2.

Таким образом, метод ЛСА позволяет представить множество законов в удобном виде для анализа, а сопоставление значений, вычисленных по метрике косинусного расстояния между разными законами, даёт возможность определить степень их смыслового сходства. Программный модуль позволит производить анализ заимствований, путем сравнения законов, что позволит улучшить существующую законодательную систему.

Литература:

1. Конституция Российской Федерации: [принята всенародным голосованием 12 декабря 1993 г. с изменениями, одобренными в ходе общероссийского голосования 01 июля 2020 г.] — Текст: электронный // Официальный интернет — портал правовой информации: [сайт]. — URL: http://www. pravo. gov. ru (дата обращения: 09.03.2021).
2. Государственная Дума. — Текст: электронный // Государственная Дума: [сайт]. — URL: https://www. gosduma. net (дата обращения: 20.05.2021).
3. Система обеспечения законодательной деятельности. — Текст: электронный // Система обеспечения законодательной деятельности: [сайт]. — URL: https://sozd. duma. gov. ru (дата обращения: 20.05.2021).
4. An Introduction to Latent Semantic Analysis/Thomas K Landauer, Peter W. Foltz, Darrell Laham. — Discourse processes, 1960. — Текст: непосредственный.

План реагирования на инциденты безопасности

Сакен Айым Сатбеккызы, студент магистратуры
Алматинский университет энергетики и связи имени Г. Даукеева (Казахстан)

План реагирования на инциденты кибербезопасности — это набор инструкций, призванных помочь компаниям подготовиться к инцидентам сетевой безопасности, обнаружить их, отреагировать на них и восстановиться после них. Большинство планов ориентированы на технологию и касаются таких вопросов, как обнаружение вредоносных программ, кража данных и перебои в обслуживании. Однако любая значительная кибератака может повлиять на организацию в различных сферах деятельности, поэтому план должен охватывать такие области, как HR, финансы, обслуживание клиентов, коммуникации с сотрудниками, юридические вопросы, страхование, связи с общественностью, регулирующие органы, поставщики, партнеры, местные власти и другие внешние организации.

Существуют отраслевые стандарты реагирования на инциденты, разработанные такими организациями, как NIST и SANS, которые содержат общие рекомендации по реагированию на активный инцидент. Однако план реагирования на инциденты организации должен быть гораздо более конкретным и действенным — в нем подробно описано, кто, что и когда должен делать. В статье составлен контрольный список, в котором указаны ключевые компоненты плана.

Как создать план реагирования на инциденты

Любая организация, имеющая цифровые активы (компьютеры, серверы, облачные сервисы, данные и т. д.), потенциально может подвергнуться кибератаке или утечке данных. Создание плана реагирования на инциденты кибербезопасности поможет подготовиться к неизбежному и оснастить команду средствами реагирования до, во время и после кибератаки.

В идеале план реагирования на инциденты безопасности должен использоваться на постоянной основе, как живой документ, для осуществления повторяющихся действий по обнаружению и реагированию (поиск угроз, расследование кибер-инцидентов, реагирование на инциденты и устранение/восстановление). Выполняя постоянные действия по обнаружению и реагированию на инциденты, можно улучшить гигиену IT и безопасности и лучше защитить организацию от неизвестных угроз, скрытых злоумышленников и, возможно, предотвратить утечку данных.

Процесс планирования реагирования на инциденты разделен на несколько этапов:

Подготовка — это первый этап планирования реагирования на инциденты и, пожалуй, самый важный для защиты вашего бизнеса и цифровых активов. На этапе подготовки важно задокументировать и объяснить роли и обязанности команды инфраструктуры, в том числе установить основную политику безопасности, на основе которой будет разрабатываться план.

Определить, достаточно ли у в настоящее время IT-ресурсов для реагирования на атаку или потребуется поддержка сторонних организаций.

Распределить роли и обязанности всех заинтересованных сторон, включая IT, HR, внутренние коммуникации, поддержку клиентов, юридическую службу, PR и консультантов.

Составить схему рабочего процесса реагирования на инцидент между различными заинтересованными сторонами. Когда привлекается отдел кадров? Когда привлекается юридическая служба? Когда оповещаются СМИ? Когда привлекаются внешние органы?

Определить нормативные требования по кибербезопасности для организации по всем функциям и разработайте руководство по взаимодействию с правоохранительными и другими государственными органами в случае инцидента.

Хранить привилегированные учетные данные, включая пароли и ключи SSH, в надежном централизованном хранилище.

Автоматически менять привилегированные учетные данные, изолировать сессии привилегированных учетных записей для временных сотрудников.

Обнаружение и анализ

Фаза обнаружения при планировании реагирования на инциденты безопасности включает в себя мониторинг, обнаружение, оповещение и отчетность о событиях безопасности. Сюда входит выявление известных, неизвестных и предполагаемых угроз — тех, которые кажутся вредоносными по своей природе, но на момент обнаружения недостаточно данных, чтобы сделать то или иное заключение.

При обнаружении зацепки, угрозы или инцидента безопасности команда реагирования на инциденты должна немедленно (если не автоматически с помощью программного обеспечения для реагирования на кибер-инциденты) собрать и задокументировать дополнительную информацию — криминалистические доказательства, артефакты и образцы кода, чтобы определить серьезность, тип и опасность инцидента, а также сохранить эти данные для использования в судебном преследовании злоумышленника (злоумышленников) в более поздний момент времени.

Разработать стратегию проактивного обнаружения на основе инструментов, которые могут автоматически сканировать физические и виртуальные хосты, системы и серверы на наличие уязвимых приложений, идентификационных данных или учетных записей.

Рассмотреть традиционные решения, такие как антивирусное ПО или инструменты для обнаружения вредоносного ПО.

Провести оценку компрометации, чтобы проверить, была ли нарушена сеть, и быстро определить наличие известных вредоносных программ и постоянных угроз «нулевого дня», активных или спящих, которые обошли существующие средства защиты кибербезопасности.

Реагирование

Реагирование на инциденты безопасности может принимать различные формы. Действия по реагированию на инциденты могут включать сортировку оповещений от ваших средств защиты конечных точек, чтобы определить, какие угрозы являются реальными, и/или приоритет в устранении инцидентов безопасности. Действия по реагированию на инцидент могут также включать сдерживание и нейтрализацию угрозы (угроз) — изоляцию, выключение или иное «отключение» зараженных систем от вашей сети для предотвращения распространения кибератаки. Кроме того, операции по реагированию на инциденты включают устранение угрозы (вредоносных файлов, скрытых бэкдоров и артефактов), которая привела к инциденту безопасности.

Немедленно изолировать системы, сети, хранилища данных и устройства, чтобы минимизировать масштабы инцидента и изолировать его от нанесения широкомасштабного ущерба.

Определить, были ли похищены или повреждены конфиденциальные данные, и если да, то каков потенциальный риск для бизнеса.

Удалить зараженные файлы и, если необходимо, замените оборудование.

Вести полный журнал инцидента и ответных действий, включая время, данные, местоположение и степень ущерба от атаки. Была ли это внутренняя, внешняя атака, системное оповещение или один из методов, описанных ранее? Кто ее обнаружил и как было сообщено об инциденте? Перечислить все источники и время, через которые прошел инцидент. На каком этапе подключилась команда безопасности?

Сохранить все детали нарушения для дальнейшего анализа происхождения, воздействия и намерений.

Обновить все брандмауэры и сетевую защиту, чтобы зафиксировать доказательства, которые впоследствии можно будет использовать для судебной экспертизы.

Привлечь команду юристов и изучите соответствие и риски, чтобы выяснить, не влияет ли инцидент на какие-либо нормативные акты.

Восстановление и последующие действия

Действия после инцидента (восстановление и последующие действия) включают устранение риска безопасности, анализ и отчет о произошедшем, обновление информации об угрозах с учетом новой информации о том, что хорошо, а что плохо, обновление плана с учетом уроков, извлеченных из инцидента безопасности, а также подтверждение и повторное подтверждение того, что среда действительно свободна от угрозы (угроз).

Заключение

Помните, что разработка плана реагирования на инциденты в сфере кибербезопасности не является одноразовым мероприятием. К сожалению, без регулярных тренингов по реагированию на инциденты и учений, включая сценарии кибератак в реальном времени, организации и их команды IT-безопасности могут внезапно обнаружить, что хакеры, которые меняют свои стратегии атак и выбор вредоносных программ, не справляются с задачей.

То, что сработало в прошлом, может не сработать завтра. Правильный план реагирования на инциденты безопасности должен быть «живым» документом, который не отстает от быстро меняющегося ландшафта угроз.

Моделирование работы агрегатора «Яндекс. Такси» как системы массового обслуживания

Улыбин Владислав Сергеевич, студент;
Мельник Любовь Юрьевна, кандидат физико-математических наук, доцент
Уфимский государственный нефтяной технический университет

В статье рассматривается моделирование работы агрегатора «Яндекс. Такси» в программном пакете Matlab. Simulink. Наглядно показано случайное распределение заявок в течение будних дней, структурная схема генератора случайных заявок, амплитудно-частотная характеристика и подсистема «Яндекс. Такси» как системы массового обслуживания.

Ключевые слова: *математическая модель, агрегаторы, моделирование агрегатора «Яндекс. Такси», программный пакет Matlab. Simulink, амплитудно-частотная характеристика, схема математической модели «Яндекс. Такси».*

С развитием интернета, сотовой связи и мобильных устройств начали появляться агрегаторы такси (лат. *aggregation*, что означает «накопление»). Агрегаторы объединили таксопарки и выстроили единый тариф оплаты, каждый в своей сети. По своей сути, агрегаторы — это разработчики программного обеспечения, приложение которых связывает водителя и пассажира, а за счет широких рекламных возможностей потенциальный пассажир знает, что заказ такси через приложение — это удобно, надежно, комфортно и безопасно, а также пассажир может сам выбрать наиболее интересное для себя предложение поездки [1].

В современных реалиях распределение заказов в агрегаторах такси происходит с использованием новейших компьютерных технологий, таких как: системы глобального позиционирования, адаптивного поиска свободных машин на основе алгоритмов искусственных нейронных сетей (учитывается пропускная способность автомобильных дорог в различных районах мегаполиса, и траектория маршрута выбирается наиболее эффективным образом). В современной экономике наблюдаются изменения экономических формаций и происходит переход к новой парадигме пассажирских перевозок. Помимо развития алгоритмов искусственного интеллекта, в настоящее время особое внимание уделяется математическому разделу теории массового обслуживания [2].

Рассмотрим моделирование работы агрегатора «Яндекс. Такси» в г. Уфа Республики Башкортостан. Наше исследование показало, что процесс формирования заявок, в общем случае, имеет стохастический характер. Так же, как и в распределении транспортного потока во времени, количество заявок, поданных на вход СМО (системы массового обслуживания), зависит от времени суток. Так, на рис. 1 показано случайное распределение заявок в течение будних дней.

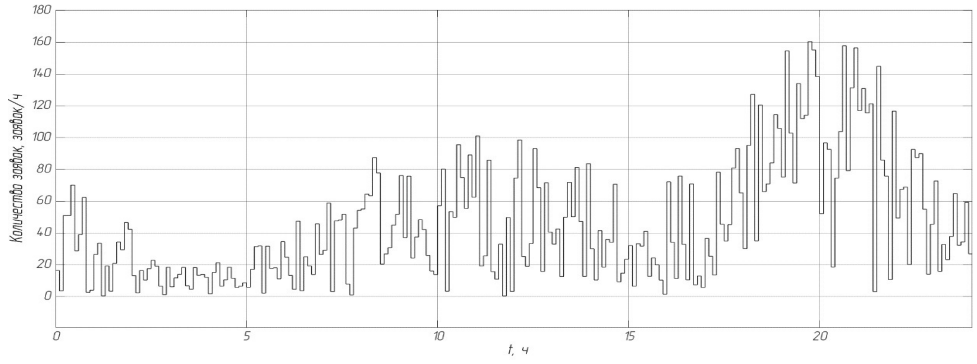


Рис. 1. **Случайное распределение заявок в течение будних дней**

Из рис. 1 видно, что спрос на услуги «Яндекс. Такси» в вечерние часы максимален. Для дальнейшего моделирования создадим генератор случайных заявок в программном пакете *Matlab. Simulink.*

На рис. 2 показан построенный генератор случайных заявок. На вход генератора случайных заявок поступает набор случайных чисел, лежащих в диапазоне от 0 до 5. В зависимости от времени суток при помощи мультиплексора (*multiport switch)* и весовых коэффициентов *Gain 1 Gain 24* генерируется кривая в полном соответствии с кривой, показанной на рис. 2. На вход In^2 поступает сигнал со счетчика часов. В дальнейшем полученный генератор случайных заявок будем рассматривать как подсистему (*subsystem*), имеющую два входа и один выход.

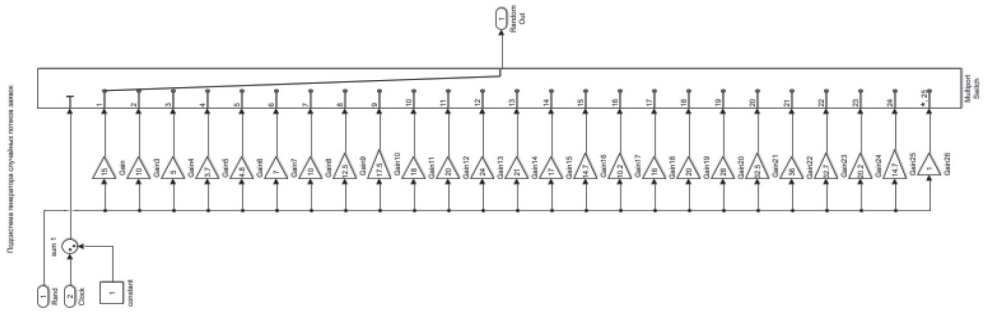


Рис. 2. **Структурная схема генератора случайных заявок**

Систему «Яндекс. Такси», как элемент системы массового обслуживания, будем рассматривать как апериодическое звено первого порядка, так же, как и в случае моделирования транспортных потоков. Однако в данной системе будут присутствовать такие параметры, как абсолютная пропускная способность каналов обслуживания *R* и производительность канала обслуживания *T*. Структурная схема «Яндекс. Такси» как элемента СМО, представлена на рис. 3.

Из рис. 3 можно сделать вывод, что система «Яндекс. Такси» имеет отрицательную обратную связь, что позволяет говорить о саморегулирующейся автоматической системе. На вход *In1* полученной системы подается стохастический поток заявок с генератора случайных заявок (рис. 2).

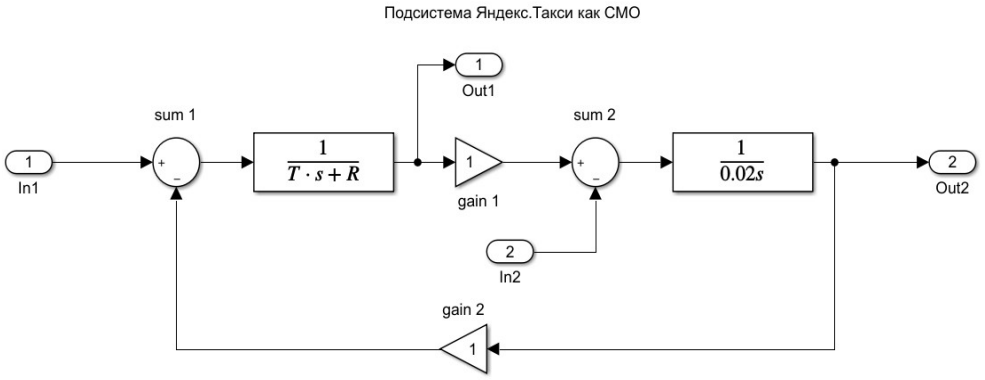


Рис. 3. **Подсистема «Яндекс. Такси» как СМО**

На вход In^2 поступает фактический транспортный поток. Так как фактический транспортный поток поступает в сумматор sum^2 с отрицанием, то количество автомобилей в таксопарке будет уменьшаться. То есть, автомобили, находящиеся в заторе, не могут обслуживать заказы. В этом случае система может работать с перегрузкой, особенно в вечерние часы, так как имеет место повышенный спрос и повышенная загруженность автомобильных дорог города.

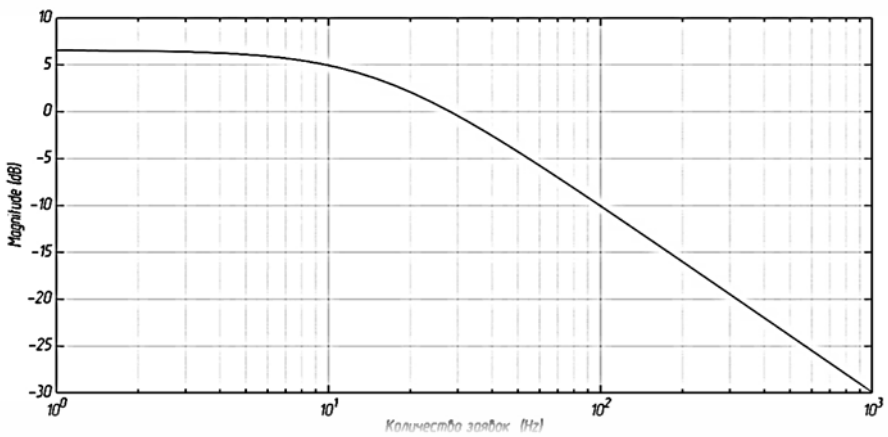


Рис. 4. **Амплитудно-частотная характеристика системы «Яндекс. Такси»**

Для анализа устойчивости данной системы массового обслуживания построим амплитудно-частотную характеристику разомкнутой системы (далее по тексту АЧХ). На рис. 4 показана амплитудно-частотная характеристика математической модели.

Фактически амплитудно-частотная характеристика в данном случае показывает, какое количество входящих заявок в единицу времени способна обслуживать система. Предельное значение заявок, при котором график АЧХ снижается на уровень –3 *dB,* будем называть критическим потоком заявок. График АЧХ зависит от основных параметров, введенных в систему «Яндекс. Такси» (абсолютная пропускная способность и производительность канала обслуживания).

Для значений R = 0,47 и T = 50 e^{-4} критический поток заявок будет равен 10 автомобилей в секунду.

Структурную схему системы «Яндекс. Такси» также объединим в подсистему и представим обобщенно в виде математической модели на рис. 5.

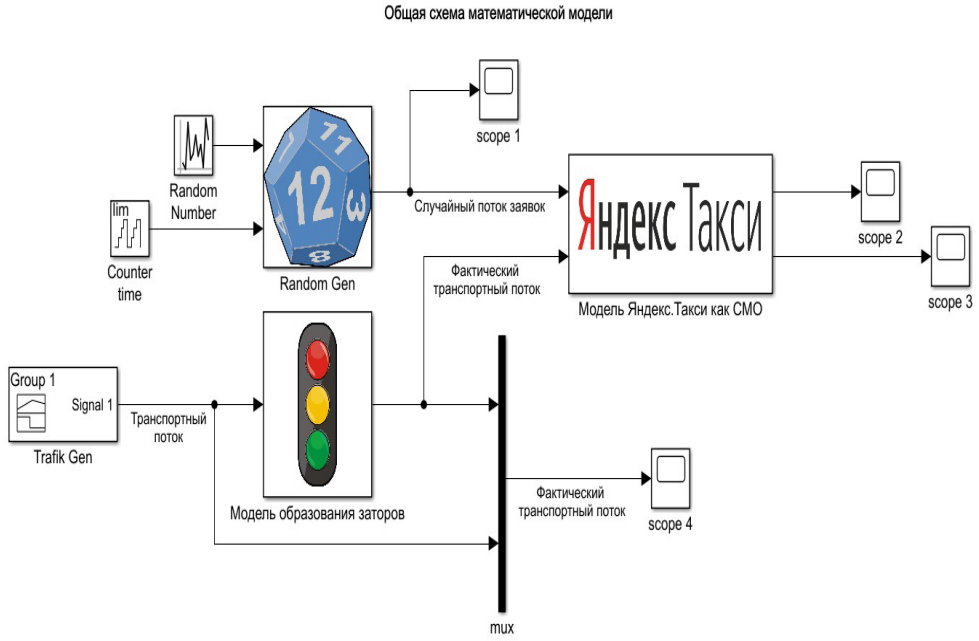


Рис. 5. **Обобщенная структурная схема математической модели «Яндекс. Такси»**

Таким образом, передаточная функция системы «Яндекс. Такси» была проанализирована в частотной области, что позволило построить амплитудно-частотную характеристику и определить критический поток заявок, при котором производительность системы снижается в e раз. Согласно предложенной математической модели, критический поток заявок зависит от абсолютной пропускной способности системы массового обслуживания и производительности каналов обслуживания.

Литература:

1. Введение в математическое моделирование транспортных потоков/Под ред. А. В. Гасникова. — М.: МЦНМО, 2013. — 26-36 с.
2. Ханчин, А. Я. Работы по математической теории массового обслуживания. — М.: Либроком, 2019. — 240.

Особенности назначения политики качества для управления современными сетями

Усманова Наргиза Бахтиербековна, доктор технических наук, доцент;
Буриев Сардор Норович, студент магистратуры
Ташкентский университет информационных технологий имени Мухаммада аль-Хоразми (Узбекистан)

Приведены особенности и характеристики управления, основанного на политиках (Policy-Based Network Management, PBNM) в современных сетях телекоммуникаций, с рассмотрением примера практического применения такого подхода в сети для обеспечения качества обслуживания.

Ключевые слова: *управление сетью, политика управления, качество обслуживания.*

На сегодняшний день развитие технологий и услуг в современных сетях резко усложнило их управление. Для того, чтобы добиться эффективного управления со стороны разработчиков решений по сетевому управлению применяются различные решения и подходы. Одним из таких подходов является достаточно известный на сегодня подход — управление на основе политик (Policy-Based Network Management, PBNM). Несмотря на то, что многие компании — разработчики и поставщики сетевого оборудования предлагают широкий спектр основанных на политике решений [1-3], этот вопрос требует изучения многих аспектов реализации таких решений, роли в управлении сетью, практического применения политик и т. п., в связи с чем в данной статье авторы приводят систематический материал по особенностям и характеристикам управления, основанного на политиках с рассмотрением примера практического применения такого подхода в сети для обеспечения качества обслуживания.

Управление сетью на основе политик

Управление на основе политик, PBNM — это технология, которая может упростить сложную задачу управления сетями и распределенными системами. Согласно этой парадигме, администратор может гибко и упрощенно управлять различными аспектами сети или распределенной системы, развертывая набор политик, управляющих его поведением [4]. Политики — это технологически независимые правила, направленные на улучшение жестко запрограммированной функциональности управляемых устройств путем введения интерпретируемой логики, которую можно динамически изменять без изменения базовой реализации. Это обеспечивает определенную степень программируемости без необходимости прерывания работы либо управляемой системы, либо самой системы управления. Управление на основе политик может значительно усилить аспекты самоуправления любой распределенной системы или сети, что приведет к автономному поведению, демонстрируемому автономными системами.

Наиболее известная архитектура управления на основе политик была определена совместно IETF и DMTF [5,6]. Она состоит из четырех основных функциональных элементов (рис. 1): инструмента управления политикой (Policy Management Tool, PMT), репозитория политик (Policy Repository), точки принятия решения (Policy Decision Point, PDP) и точки применения политики (Policy Enforcement Point, PEP).

PMT используется администратором для определения или обновления политик, которые должны применяться в управляемой сети. Результирующие политики хранятся в репозитории в форме, которая должна соответствовать информационной модели, чтобы гарантировать совместимость продуктов от разных поставщиков. Когда новые политики добавляются в репозиторий или существующие изменяются, PMT выдает соответствующий PDP с уведомлениями, который, в свою очередь, интерпретирует политики и передает их PEP.

PEP — это компонент, который запускается на узле с поддержкой политик и может выполнять (применять) различные политики. Компоненты архитектуры могут взаимодействовать друг с другом с помощью различных протоколов. Предпочтительным выбором для передачи решений политики между PDP и сетевыми устройствами (PEP) является Common Open Policy Service (COPS) или SNMP и LDAP для связи PMT/PDP с репозиторием.

Простейший подход к спецификации политики — это последовательность правил, в которых каждое правило представляет собой форму простой пары «условие-действие». Структура политики IETF использует этот подход и рассматривает политики как правила, которые определяют действия, которые должны выполняться в ответ на определенные условия.

Политика обычно определяется как набор правил. Каждое правило политики состоит из условия и предложения действия. Если выполнение условия истинно, тогда разрешается выполнение действий, т. е. управление политиками — это использование правил для принятия решений. Политика обычно представлена как набор классов и отношений, которые определяют семантику представления политики. Эти «строительные блоки» обычно состоят как минимум из правила политики, условия политики и действия политики.

Часть правила действия может быть набором действий, которые должны выполняться, когда условия верны. IETF не определяет конкретный язык для выражения сетевых политик, а скорее общую объектно-ориентированную информационную модель для представления информации

Рис. 1. **Архитектура управления на основе политик**

о политике. Эта модель является общей, определяя структуру абстрактных классов политик посредством ассоциации, что позволяет поставщикам реализовать свой собственный набор условий и действий, которые будут использоваться правилами политики.

Особенности назначения политик качества в понятиях PBNM

Согласно общепринятому определению, политика в управлении — это система принципов для принятия решений и достижения оптимальных результатов. Политика направляет действие на достижение основополагающих целей при выполнении конкретных задач. Путём распределения направлений, которым нужно следовать, она объясняет основные механизмы, каким образом должны быть достигнуты цели [7].

Для области управления сетями связи управление на основе политик чаще всего используется для упрощения управления путем установления таких действий, согласно которым следует поступать в определенных ситуациях. Типичное применение политик состоит в том, чтобы установить правила/критерии, по которым следует распределять какой-либо ресурс, когда его недостаточно или имеется ограниченность ресурсов.

Рассмотрим более подробно понятие «политика» в задачах управления сетью. Как показано в [4,8], можно выделить два типа политик:

Цели политики устанавливают задачу. Например, «Не позволяйте голосовым услугам, предоставленным для конечных пользователей, отрицательно влиять на аналогичные услуги, которые будут предоставлены позже».

Правила политики определяют условия и действия, предназначенные для определения того, как следует реагировать на определенные ситуации, возникающие при выполнении условий в правиле политики (часть действия в правиле политики). Например: «Если 80 пользователей голосовых услуг уже подключены к сети через конкретный порт T1 (который позволяет 24 пользователям звонить одновременно), то отклоните любую попытку предоставить эту услугу дополнительным пользователям (по причине того, что может возникнуть блокирование заявок при попытке совершить вызов)».

Понятия цели политики и правил политики тесно взаимосвязаны. На самом деле, это разные способы выражения политики. В частности, цели политики обычно можно перефразировать и выразить в виде правил политики. Отличием является уровень детализации, на котором определяется политика.

Таким образом, политики предоставляют руководящие принципы и определяют соответствующее поведение, которое ожидается при определенных условиях, не требуя вмешательства со стороны средств управления верхнего уровня. Как отмечено в [4], политики напоминают рефлексы, на которые способна нервная система человека: когда пыль попадает в глаза, человек рефлекторно моргает и ему не нужно обдумывать это действие; мозг справляется с подобными ситуациями на уровне подсознания, не требуя принятия сознательных решений. Для области задач управления сетью, естественно, такие действия — политики будут заранее запрограммированы и, таким образом, может быть изменено «рефлекторное» поведение. Это, соответственно, означает, что когда это происходит, этими политиками нужно управлять.

В идеальном случае система управления на основе политик должна способствовать определению администра-

тивных целей высокого уровня, которые легко выразить и понять людям, и позволять переводить их на более низкий уровень политики и отображать их в команды, которые соответствующим образом настраивают управляемые устройства. В то время, как цели высокого уровня отражают бизнес-цели администратора сети, политики низкого уровня отвечают за конфигурации на уровне устройств.

Уточнение политики — это процесс преобразования цели высокого уровня или абстрактной спецификации политики в конкретные политики низкого уровня, которые могут применяться в управляемой системе [5]. Основными задачами процесса уточнения являются следующие:

— Определить ресурсы, необходимые для удовлетворения требований политики;

— Преобразовать высокоуровневые цели в операционные политики, которые система может применять

— Убедиться, что низкоуровневые политики действительно соответствуют требованиям, указанным в высокоуровневой цели.

Учитывая, что подход к управлению на основе политик является хорошей основой, на которой могут быть разработаны автономные процессы принятия решений для управления сетью [4,5], следующий вопрос, который следует рассмотреть, — это, очевидно, то, как политики могут использоваться для управления процессом принятия решений в автономном режиме управления сетью. Можно определить несколько концепций политики в автономной системе:

— Политика действий выражается в форме: ЕСЛИ (Условия) ТО (Действия), где Условия определяют конкретное состояние или набор возможных состояний, которые все удовлетворяют данным Условиям, а Действия описывают действия, которые система должна предпринимать, когда она находится в состоянии, указанном Условиями.

— Целевая политика — это спецификация одного желаемого состояния или критериев, которые характеризуют весь набор желаемых состояний. Следовательно, целевые политики обеспечивают только бинарную классификацию состояний: «желаемое» и «нежелательное».

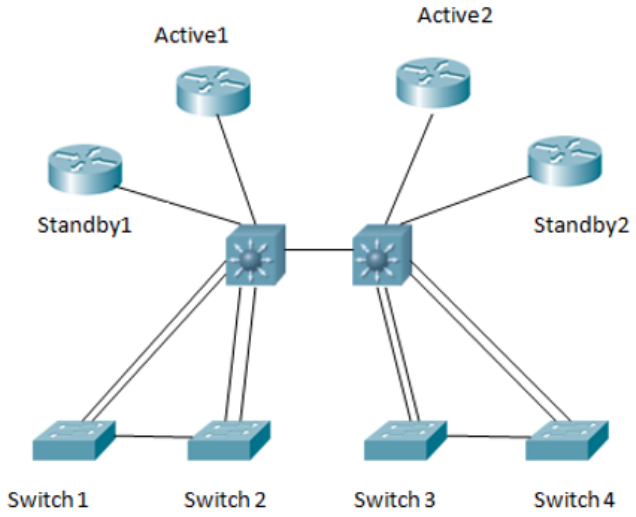
— Политика функции полезности является расширением целевых политик: вместо того, чтобы выполнять двоичную классификацию на желаемое и нежелательное состояния, функция полезности приписывает каждому состоянию скалярную желательность с действительным знаком.

Каждая из этих концепций политики используется отдельно в существующих решениях для управления сетью. В целом, интеграция всех этих концепций политики в процесс управления может помочь сети продемонстрировать автономное поведение. Кроме того, этот набор может быть дополнен «поведенческими» политиками (авторы рассматривают этот вопрос в качестве тематики дальнейших исследований). Эти политики, не охватываемые другими политиками, направлены на то, чтобы помочь автономному объекту управлять своим собственным поведением в зависимости от его контекстной информации.

Наглядными примерами демонстрации применения политик могут служить инструменты управления политикой качества обслуживания (Quality of Service, QoS): использование мастера политики качества обслуживания для создания, изменения и удаления политики качества обслуживания в серверах. В операционных системах Windows политика QoS сочетает в себе функциональные возможности качества обслуживания на основе стандартов с управляемостью групповой политики. Создание политики качества обслуживания связано с двумя ключевыми элементами управления QoS, которые используются для управления сетевым трафиком: значение DSCP и регулирование трафика. Другими словами, для конкретного приложения можно определить приоритет исходящего сетевого трафика с помощью указания значения DSCP, и чтобы настроить политику качества обслуживания сетевые маршрутизаторы используют значение DSCP для классификации сетевых пакетов и постановки их в очередь соответствующим образом. Кроме значений DSCP, регулирование — еще один ключевой элемент управления для управления пропускной способностью сети. С помощью регулирования политика QoS ограничивает исходящий сетевой трафик на заданную частоту регулирования, а для эффективного управления трафиком можно одновременно использовать указание значений DSCP и регулирование количества запросов.

Управление на основе политик может быть также продемонстрировано для случая, когда политики применяются в зависимости от текущего состояния управляемой системы (например, могут возникать конфликты между политиками динамического распределения ресурсов и политиками, устанавливающими квоты для пользователей или классов обслуживания) при использовании технологии HSRP.

HSRP (Hot Standby Router Protocol) — проприетарный протокол Cisco, предназначенный для увеличения доступности маршрутизаторов, выполняющих роль шлюза по умолчанию. Это достигается путём объединения маршрутизаторов в standby группу и назначения им общего IP-адреса, который и будет использоваться как шлюз по умолчанию для компьютеров в сети (подробное описание работы протокола можно найти в http://xgu. ru/wiki/HSRP). Основная задача и предназначение данного протокола состоит в том, чтобы добиться практически 100% доступности и отказоустойчивости первого хопа от отправителя. Это достигается путем использования у двух или более маршрутизаторов или маршрутизирующих коммутаторов третьего уровня одного IP адреса и MAC адреса так называемого виртуального маршрутизатора.



Настройка hsrp1:	*Настройка hsrp2:*
interface	interface
FastEthernet0/0	FastEthernet0/0
ip address	ip address
192.168.1.1	192.168.1.2
255.255.255.0	255.255.255.0
interface	interface
FastEthernet0/1	FastEthernet0/1
ip address	ip address
192.168.1.4	192.168.1.3
255.255.255.0	255.255.255.0
standby 1 ip	standby 1 ip
192.168.1.254	192.168.1.254
standby 1 priority	standby 1 priority
105	100
standby 1 preempt	standby 1 preempt
standby 1 track	standby 1 track
FastEthernet0/0	FastEthernet0/0

Рис. 2. **Топология сети**

Проверяем:

```
hsrp1#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Gig0/0      1    105 P Active   local           192.168.1.2     192.168.1.254
hsrp1#
```

```
hsrp2#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Gig0/0      1    100 P Standby  192.168.1.1     local           192.168.1.254
hsrp2#
```

Роутер с большим приоритетом (hrsp1) является активным шлюзом, роутер с меньшим приоритетом (hrsp²) находится в режиме ожидания. В таком примере один из роутеров в топологии простаивает, что неприемлемо. Для распределения нагрузки между обоими роутерами можно создать вторую группу на тех же интерфейсах (т. е. два виртуальных шлюза), задавая правила в конфигурациях устройств.

На практике операторы связи могут задавать такие правила с привязкой к вариантам предоставления соглашения о качестве обслуживания (Service Level Agreement, SLA) своим абонентам. Выбор того или иного варианта определяется как рыночной конъюнктурой, так и техническими возможностями сети оператора связи.

Заключение

В современных телекоммуникационных сетях продолжаются процессы крупномасштабных изменений, возрастает конкуренция, что одновременно сокращает жизненный цикл систем поддержки сетей связи и систем управления. Развивающиеся технологии на различных уровнях организации сети закономерно приводят к потребности в пересмотре позиций классических систем и платформ управления.

Задача управления ресурсами сети становится все более сложной, поскольку администраторы должны принимать во внимание гетерогенные системы, различные сетевые технологии и распределенные приложения. По мере роста количества управляемых ресурсов задача управления этими устройствами и приложениями зависит от решения множества проблем системы управления и поставщика оборудования. Чтобы предотвратить чрезмерную детализацию операторов, необходимо повысить уровень абстракции, чтобы скрыть системные и сетевые особенности. Политики, которые вытекают из целей управления, определяют желаемое поведение распределенных гетерогенных систем и сетей и определяют средства для обеспечения такого поведения. Таким образом, технология управления на основе политик, PBNM предоставляет средства для определения динамически изменяющейся стратегии управления для обеспечения последовательных, правильных и понятных сетевых систем.

Литература:

1. http://www. ittoday. info/Articles/Policy-Based_Network_Management
2. John Strassner. Policy-Based Network Management. Solutions for the Next Generation/Morgan Kaufmann Publishers, Elsevier Science 2004.
3. Curtis, M. Keliiaa et al. Policy Based Network Management. State of the Industry and Desired Functionality for the Enterprise Network/SANDIA REPORT SAND2004–3254, Unlimited Release. February, 2005.
4. Network management: know it all/Adrian Farrel [et al.], Morgan Kaufmann Publishers, 2009 by Elsevier Inc.
5. Управление на основе политик — Policy-based management [Электронный ресурс]/Режим доступа: https:// livepcwiki. ru/wiki/Policy-based_management, свободный.
6. Ding, J. Policy-Based Network Management/from Advances in Network Management by Jianguo Ding. Auerbach Publications, 2010.
7. Политология/Мельвиль, А. Ю. МГИМО. Проспект, 2008.
8. Network Management Fundamentals/Alexander Clemm, 2007 Cisco Systems, Inc.

Метод мультиагентного глубокого обучения в решении социальных дилемм

Чебан Ольга Петровна, студент магистратуры
Московский государственный технический университет имени Н. Э. Баумана

В статье автор предлагает метод мультиагентного глубокого обучения для изучения сотрудничества, который позволит приблизиться к решению социальных дилемм.

Ключевые слова: *социальные дилеммы, обучение с подкреплением, машинное обучение, мультиагентное обучение, искусственный интеллект, сотрудничество.*

Социальные дилеммы возникают, когда происходит столкновение с приоритетом либо краткосрочных эгоистических интересов, либо долгосрочных интересов группы, организации или общества. Многие из самых сложных проблем, от межличностных отношений до межгрупповых, лежат в основе их социальных дилемм. Загрязнение, истощение природных ресурсов и межгрупповые конфликты можно охарактеризовать как примеры социальных дилемм, которые требуют незамедлительного решения. Социальные дилеммы охватывают большую область научных интересов. К примеру, авторы статьи [1] показали, что область социальных дилемм растет и процветает с точки зрения теории, междисциплинарного сотрудничества и применимости, предлагая идеи, которые являются новыми, воспроизводимыми и применимыми ко многим социальным дилеммам.

Социальные дилеммы сложились исходя из обстоятельств, в которых присутствует эгоистичный интерес и общее благо. Наиболее распространёнными социальными дилеммами являются «Дилемма заключенного», «Дилемма общественного блага» и «Трагедия общин».

Теория игр предполагает, что люди являются рациональными субъектами, стремящимися максимизировать свою выгоду. А согласно теории эгоистичных генов, люди могут следовать, казалось бы, иррациональной стратегии сотрудничества, если это способствует выживанию их генов. В дополнение к этому существует теория взаимности, которая предлагает иное объяснение эволюции сотрудничества. В повторяющихся играх с социальной дилеммой между одними и теми же людьми может возникнуть сотрудничество, потому что люди могут наказывать партнера за отказ сотрудничать. Это случай прямой взаимности, она работает лучше всего в паре, и, следовательно, в маленьких группах. Также существует непрямая взаимность, которая объясняет значение репутации в сотрудничестве больших групп. При прямой взаимности репутация играет большое значение, а вот в непрямой это неочевидно. До некоторого времени решение непрямой взаимности вызывала другие дилеммы. Автор статьи [2] решает дилеммы, которые возникают при решении непрямой взаимности, используя репутацию, доказывая тем самым какую большую роль она играет. Также были рассмотрены психологические модели: теория взаимозависимости и модель уместности.

Существует три класса решений социальных дилемм: мотивационные, стратегические и структурные. Мотивационные решения часто предполагают, что люди не заинтересованы исключительно в своих интересах, но могут иметь и другие предпочтения. Сюда входят концепция социальной ценностной организации и социальная идентичность. Любопытно, то, что в концепции социальной ценностной организации многие механизмы способствуют сотрудничеству между людьми, облегчая или даже разрешая социальную дилемму. Один класс механизмов, который недостаточно изучен — это распространение опыта, полученного в различных средах. В одном лабора-

торном эксперименте участники играли в повторяющиеся игры с общественными благами, в которых раунды чередовались между позитивными взаимодействиями и взаимодействиями с социальной дилеммой. Результатом эксперимента было то, что вместо поощрения просоциального поведения наличие позитивных взаимодействий снизило уровень сотрудничества при взаимодействии с социальной дилеммой. Данный эксперимент показывает, что высокая отдача, получаемая от положительных взаимодействий, задает ориентир, который подчеркивает восприятие участниками того, что участие в взаимодействиях с социальной дилеммой является плохим вложением. Одним из стратегических решений социальных дилемм является использование взаимности (пример «Око за око»). Структурные решения меняют правила игры, либо изменяя социальную дилемму, либо полностью устраняя дилемму: изменение структуры социальной дилеммы, уменьшение размера группы, устранение социальной составляющей путём приватизации. Все эти решения требуют подробного изучения. В частности, методы глубокого обучения с подкреплением позволяют моделировать социальные дилеммы и применять, на текущий момент, сильно упрощённые версии данных решений, поскольку в основе этих решений лежат природные, психологические процессы, которые мы сегодня не настолько хорошо можем моделировать.

Исходя из проведённого исследования, было выяснено, что в основе решения социальных дилемм лежит сотрудничество. В последнее время мы видим, что сотрудничество становится более важным компонентом сценариев мультиагентного обучения с подкреплением, что позволяет говорить о том, что мы всё больше приближаемся к пониманию сотрудничества, и впоследствии к решению социальных дилемм. В изучении и использовании сотрудничества имеет значительные успехи методы глубокого мультиагентного обучения с подкреплением, например, как метод MADDPG, разработанный исследователями OpenAI [3]. Авторы разработали метод, который сочетает в себе централизованное обучение с децентрализованным исполнением, позволяя при разработке стратегии использовать дополнительную информацию для облегчения обучения. Агенты учатся не только на своих собственных действиях, но также и на действиях других агентов в среде путём прогнозирования этих действий. Это позволяет лучше проанализировать поведение других и разработать свою стратегию, что для социальных дилемм очень важно, поэтому такие методы следует использовать в основе исследования и решения социальных дилемм. Также исследователями [4] был представлен пример практического использования мультиагентного решения социальной дилеммы для систем с общими ресурсами, в частности, системы управления водными ресурсами для жилого комплекса, что в очередной раз доказывает, насколько важна данная тема для разрешения разных сложных задач и как методы мультиагентного обучения могут в этом помочь.

В качестве заключения можно сделать однозначный вывод, что социальные дилеммы сложны, многогранны и что современные методы глубокого мультиагентного обучения могут предложить способы изучения сотрудничества, что положительно повлияет на решение таких сложных задач как социальные дилеммы.

В данной статье были рассмотрены социальные дилеммы, их типы, возможности решения и один из способов развития в решении социальных дилемм. В качестве метода был представлен современный алгоритм мультиагентного глубокого обучения [3], который обучает агентов сотрудничать, причём агенты используют как свой предыдущий опыт, так и предсказания поведения других агентов, что позволяет лучше понимать основу сотрудничества, что в свою очередь помогает в решении социальных дилемм.

Литература:

1. Paul, A. M. Van Lange, Jeff Joireman, Craig D. Parks, Eric Van Dijk. The psychology of social dilemmas: A review. // Organizational Behavior and Human Decision Processes Volume 120, Issue 2, 2013, Pages 125-141. DOI: 10.1016/j. obhdp. 2012.11.003.
2. Okada, I. Two ways to overcome the three social dilemmas of indirect reciprocity. // Sci Rep 10, 16799, 2020. DOI:10.1038/s41598–020–73564-5.
3. Ryan Lowe, Yi Wu, Aviv Tamar, Jean Harb, Pieter Abbeel, Igor Mordatch. Multi-Agent Actor-Critic for Mixed Cooperative-Competitive Environments. // arXiv:1706.02275v4, 2020. Режим доступа: https://arxiv. org/pdf/1706.02275. pdf.
4. Arnu Pretorius, Scott Cameron, Elan van Biljon, Tom Makkink, Shahil Mawjee, Jeremy du Plessis, Jonathan Shock, Alexandre Laterre, Karim Beguir. A game-theoretic analysis of networked system control for common-pool resource management using multi-agent reinforcement learning. // Neural Information Processing Systems (NeurIPS) conference, 2020, DOI: arXiv:2010.07777v1.

Возможность первичной обработки текста посредством морфологического анализа

Щеблыкин Никита Александрович, студент магистратуры
Саратовский государственный технический университет имени Гагарина Ю. А.

Оценка возможностей морфологических анализаторов для успешного определения частей речи слов и прочих характеристик предложения.

Ключевые слова: *NLP, морфологический анализ, NLTK, нейронные сети.*

Analysis of the possibility of primary text processing through morphological analysis

Scheblykin Nikita Alexandrovich, student master»s degree program
Saratov State Technical University named after Yu. A. Gagarin

Assessing the abilities of morphological analyzers to successfully identify word»s part of speech and other sentence characteristics.

Keywords: *NLP, morphological analysis, NLTK, neural networks.*

Введение

Одной из возможных проблем, возникающих при обучении интеллектуальных систем человеком, является слабая сформированность поступающей информации. В особенности это касается человеческой речи. Я сейчас говорю не о точности распознавания голоса в текст, а о том, как данный текст можно подать в более удобоваримом состоянии для обучения или обработки информационной системой, нейронной сетью.

Способность выделить смысл из целого предложения является основополагающим фактором для возможности как-то классифицировать и сохранить/обрабатывать информацию, работая не с какими-то упрощенными ключевыми конструкциями, а распознавания и выделения конкретного запроса. Основополагающим для обработки является грамматическая основа предложения, описывающая субъект и его состояние.

В переводе с англ. Natural Language Processing обозначает методы обработки человеческого языка в той форме, в какой он есть, безо всяких подстраиваний под шаблон, язык, на котором мы разговариваем друг с другом. Благодаря данным методам обработки возможно создавать системы распознавания речи и текста, обработки документов, машинного перевода, выявления спама, распознавания сущностей или ответов на вопросы и т. д.

А можно ли как-то упростить поиск того самого смысла или предиката (или грамматической основы)? Можно, если предусмотреть возможные построения предложения (возможные подлежащие и возможные сказуемые), во всех случаях они описываются частью речи или связкой частей речи с определенным падежом, родом ли или частью речи. В самом простейшем случае это будут существительное в именительном падеже и глагол изъявительного наклонения того же рода, но отнюдь далеко не всегда.

Методика исследований

Возникает мысль, что если бы мы могли получить сведения о каждом слове в предложении, о части речи, о падеже или наклонении, о роде, о числе, то мы, в теории, могли бы без труда определить грамматическую основу предложения. Программа, скрипт, библиотека-методов, другая сложная система занимающаяся этим, будет называться морфологическим анализатором.

Возьмем это за основу и перейдем к более далекой от лингвистики области, но куда более интересной нам. Рассмотрим же возможность проведения анализа текстовой информации при помощи морфологического анализа.

Конечно, можно разработать собственные методы морфологического анализа, или создать свою нейронную сеть, натренированную на анализ (и собственную методику), можно воспользоваться библиотеками, предназначенными для такого обучения (например OpenCorpora), а можно использовать готовые морфологические анализаторы, разрабатываемые под конкретные языки программирования.

Раз уж речь зашла о программировании, впредь и далее все примеры будут действительны только в отношении Python, так как все дальнейшие изыскания проводились на нем, все библиотеки использовались для его третьей версии. Однако в целом мне не хочется акцентировать внимание на конкретном языке программирования, так как аналоги есть и в других средах разработки. Мной же использовался Python, так как также рассматривалась возможность включения результатов морфологического анализа в более сложный проект, также написанный на этом языке.

Для оценки правильности работы анализатора, его парсинг слов и предложения сравнивался с заранее подготовленным для этого эталон.

Были рассмотрены две библиотеки, это NLTK (версии 3.5) и Pymorphy (Версия, работающая под третьим python»ом называется pymorphy[2]). Средняя вероятность успешного разбора тем и иным анализатором показана на Рис. 1. Стоит отметить что ожидаемо результат далек от совершенства, но не так уж и плох.

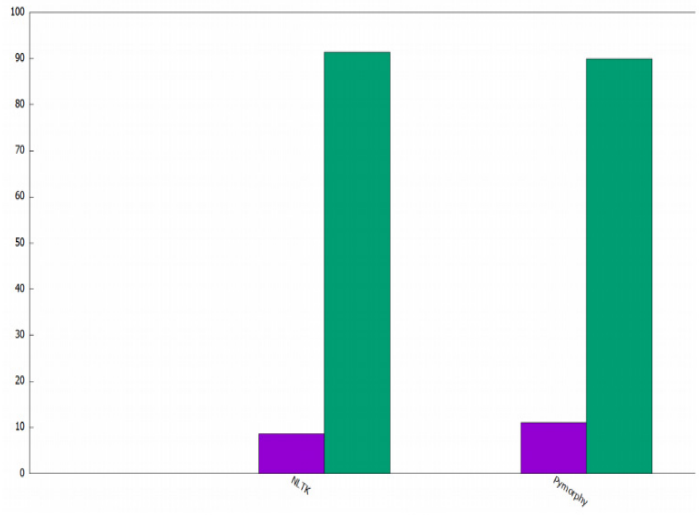


Рис. 1: **Средняя вероятность ошибки при разборе разными средствами**

Также следует отметить зависимости нарастания ошибки разбора при увеличении длины вводимого предложения (Рис. 2), и зависимость средней оценки точности разбора (Рис. 3-4). Подробнее обратим внимание на последнее: сама по себе эта оценка зависит от изучаемого материала и характеризует вероятность данного употребления в тексте на основе библиотечных прецедентов.

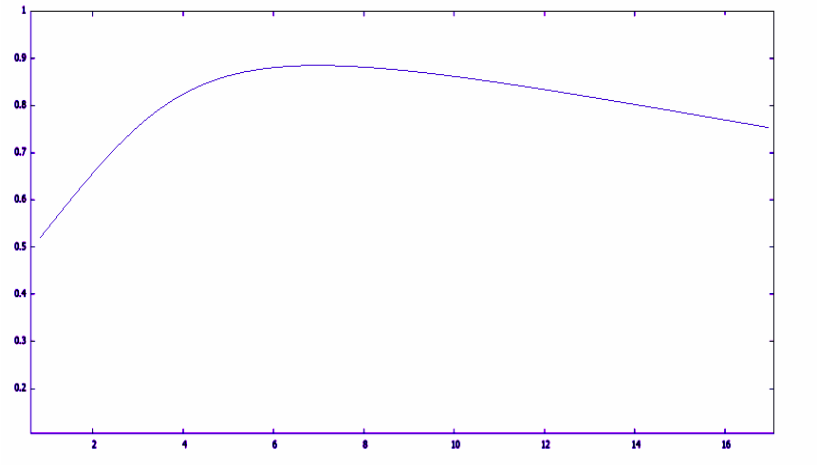


Рис. 2: **Процент выбора верного разбора при различной длине разбираемого материала (1=100%)**

Дело в том, что в речи есть такие слова, как омонимы, которые могут обозначать совершенно разные части речи в совершенно разных формах, при этом имея абсолютно идентичное написание. Оценка же правильности разбора будет зависеть от используемой библиотеки обучения. Это одна из возможных причин иной интерпретации контекста предложения и его частей, коих может быть очень много, ведь даже люди порой не всегда понимают тот смысл который был заложен в слова изначально.

На втором рисунке можно заметить, что для коротких предложений в 6-7 слов достигается наибольшая точность анализа. Т. е. для тех предложений, которые достаточно распространены, чтобы передавать основную мысль простыми конструкциями, исключив неоднозначность, вызванную краткостью, и без осложненности конструкциями, разбор которых будет происходить труднее.

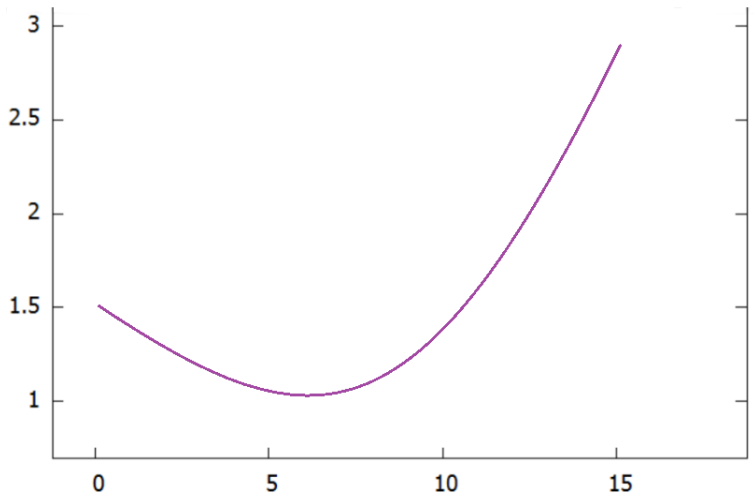


Рис. 3: **Увеличение вероятности неправильного разбора слова в зависимости от длины анализируемой последовательности для модуля Pymorphy**

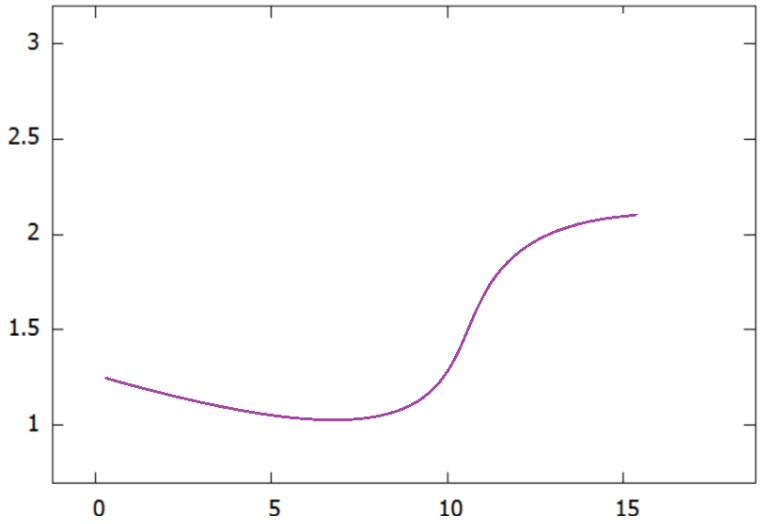


Рис. 4: **Увеличение вероятности неправильного разбора слова в зависимости от длины анализируемой последовательности для модуля NLTK**

Аналогичную картину на Рис. 3 и на Рис. 4 заметно, что Pymorphy куда более чувствителен к длине предложения. И дело тут не только в используемых алгоритмах или общем качестве, NLTK работает на основе английского языка, данные к которому и из которого в случае русского языка нужно переводить (автономно), что в свою очередь не только занимает больше времени, но также и сглаживает возможную неточность, образуя этакий фильтр, поскольку в современных переводчиках используется похожая технология.

Оценить ошибку F процентно можно по следующей формуле:

$$F = \frac{1}{2N} \cdot \frac{\sum_i^K (1 - k_{ci}) \cdot f_i}{\sum_i^K k_{ci}}$$

где f_i — это ошибки при данной длине предложения в каждом из испытаний (при n=2 это f_1 и f_2), k_c — это средние оценки достоверности разбора слов в данном предложении, N — объем выборки, K — количество разбираемых слов.

$$k_{cn} = K^{-1} \int_0^n f = K^{-1} \sum_{i=1}^{n} \frac{f_i \cdot (L_i + L_f)}{2}$$

где n — количество испытаний, f_i _ количество ошибок на каждом из испытаний, L — достоверность разбора.

$$L_i = L^{-1} \sum_{j=1}^{K} L_{ij}$$

$$L_f = \sum_{j=1}^{K} L_{ij} \cdot f_j$$

где f_j — характеристика слова, показывающая ошибочный разбор или нет.

$$k_c = K^{-2} \sum_{i=1}^{n} \frac{f_i \cdot (\sum_{j=1}^{K} L_{ij} + \sum_{j=1}^{K} L_{ij} \cdot f_j)}{2}$$

Для того чтобы увеличить вероятность правильного разбора слова можно выделить несколько локальных решений:

— Разбивать сложные конструкции на более простые.

— Проводить поверхностный анализ частей речи, выделяя те, что получается установить достоверно, и согласно ним косвенно устанавливать наиболее точный разбор возникших неоднозначностей.

— Использовать комбинирование методик анализа текста для разрешения возникающих неопределенностей

Стоит вспомнить о том, как хорошо на данный момент развились онлайн-сервисы перевода, и перспектива использования nltk заиграла новыми красками. Так как нам на самом деле нужен смысл предложения, то некоторую точность придется оставить при переводе, сочтем это допустимым, но только в том случае когда после обратного перевода сохранился смысл. В английском языке несколько иное представление о грамматической основе предложения. В простейшем случае это подлежащее и сказуемое, однако выделяют предикат предложения и полный предикатив, первое и будет содержать самую важную информацию, а его полная вариация содержит уточняющие факторы. Сложные механики перевода по словарям и синонимичным выражениям сделают свое дело.

С целью установить, какое из API предпочтительнее использовать в своих целях, было решено провести небольшое исследование зависимостей разных переводчиков, а точнее установить, как они будут справляться с задачами разного характера:

— насколько точным будет перевод, как дословным, так и передачей общего смысла. Отметим сразу, что была подобрана база из не самых простых предложений, зачастую имелись иносказания, осложнения или не одна грамматическая основа. Это было сделано с той целью, чтобы рассмотреть в самых разных условиях результаты, так как резонно предположить, что на самых простых предложениях проблем не будет никаких.

— зависимость перевода от длины предложения, от количества слов.

— зависимость перевода от осложненности предложения (обороты, перечисления, союзы, вводные слова и т. д.)

— зависимость перевода от того, сложное предложение (несколько грамматических основ) или простое (одна).

А также сравнить взаимосвязь этих факторов.

Таблица 1. **Пример результатов для выявления взаимосвязанностей при переводе через распространенные API**

№	Кол-во слов	Осложненность да/нет (1;0)	Сложное предложение да/нет (1;0)	Точность перевода (-1;0 … 1) Yandex	Google	DeepL
1	3	0	0	1	0.7	0.8
2	11	0	1	1	1	0.7
3	9	1	0	0	1	0.8
4	6	0	0	1	1	1
5	12	0	1	0.5	0	0
…	…	…	…	…	…	…
90	16	1	1	0.6	0.9	0

По результатам были построены несколько графиков для анализа.

Общая зависимость усредненных оценок точности двойного перевода от количества слов в предложении показана на Рис. 5. Можно заметить, что перевод сервисом Google более правильно сохраняет смысл предложения, часто заменяя слова синонимами, пусть и несколько меняющих эмоциональную окраску, а также это позволяет избежать внезапных неверных интерпретаций слов, в отличие от сервиса Yandex.

Наиболее предсказуемым и поддающийся анализу взаимосвязанностей также оказался сервис Google Translate (Рис. 6), в то время как у других сервисов тоже прослеживаются похожие тенденции, но куда слабее. Так можно заметить, что распространенное предложение обрабатывается лучше нераспространенного, наличие нескольких грамматических основ — слабо влияющий фактор, а вот осложненность предложения — напротив, ухудшает результат.

Выводы

В результате рассмотрения вариантов проведения морфологического анализа с целью разбора предложения можно сказать, что такой метод обработки естественной речи человека имеет перспективы для дальнейшего раз-

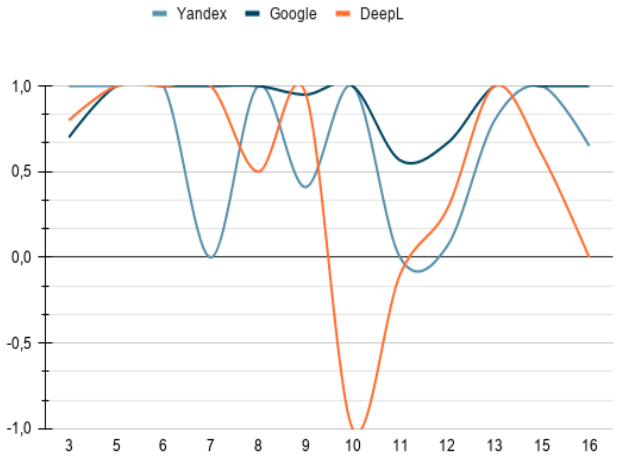


Рис. 5. **Общая зависимость точности двойного перевода от количества слов в предложении через различные API (-1: перевод неверный; 0: сохранен общий смысл, получены заметные искажения или несогласованность второстепенных членов предложения; 1: при переводе сохранен смысл, не нарушена структура предложения или перевод дословно совпал)**

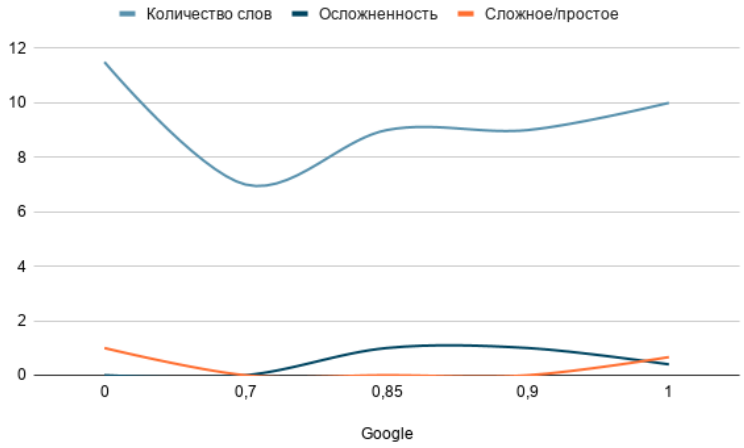


Рис. 6. **Взаимная зависимость характеристик на качество перевода для сервиса от Google**

вития и улучшения и пригоден для выполнения более сложных задач, относящихся к нечеткой логике и анализа текста. Получена приемлемая точность, без учета улучшений и модификаций, дополнительных проверок, и разборе только по одной стратегии вычисления: top-down (около 77,2% по примерным расчетам)

Литература:

1. Steven Bird, Ewan Klein, Edward Loper. Natural Language Processing with Python. — O»Reilly Media, 2009..
2. Perkins, Jacob. Python Text Processing with NLTK 2.0 Cookbook. — Packt Publishing, 2010.
3. Tom Young, Devamanyu Hazarika, Soujanya Poria, Erik Cambria. Recent Trends in Deep Learning Based Natural Language Processing. — 2018-11-24.
4. Shervin Minaee, Nal Kalchbrenner, Erik Cambria, Narjes Nikzad, Meysam Chenaghlu. Deep Learning Based Text Classification: A Comprehensive Review. — 2020-04-05.

БИОЛОГИЯ

Влияние нейропептида бомбезина (Бмб) на условно-рефлекторную деятельность варанов

Амиршоев Файзулло Сафарович, доктор биологических наук, профессор, вице-президент
Академия сельскохозяйственных наук Республики Таджикистан (г. Душанбе, Таджикистан)

Азимова Гулнора Норбобоевна, кандидат биологических наук, доцент
Таджикский государственный медицинский университет имени Абуали ибни Сино (г. Душанбе, Таджикистан)

Influence of neuropeptide bombesin (bmb) on conditional reflective activities of varans

Amirshoev Fajzullo Safarovich, doctor of biological sciences, professor, vice-president
Academy of Agricultural Sciences of the Republic of Tajikistan (Dushanbe, Tajikistan)

Azimova Gulnora Norboboevna, candidate of biological sciences, associate professor
Tajik State Medical University named after Abuali ibni Sino (Dushanbe, Tajikistan)

Актуальность исследование. Нейропептид бомбезин (Бмб) был получен из кожи европейской лягушки Bombino. Затем он был обнаружен в мозге лягушек, что дало основание называть этот пептид нейропептидом [Erspamer, Melchiorri, 1973, 1975; Anastasi-etal., 1975]. Главной характеристикойБмб является его гипотермический эффект. Согласно ряду исследований Бмб участвует в торможении электрической активности мозга, в то же время он вызывает возбуждение нейронов гиппокампа крыс.

Цель исследования. Изучить влияние нейропептида бомбезина (бмб) на условно-рефлекторную деятельность варанов.

Результат исследование. В условиях наших экспериментов было обнаружено, что внутримышечное введение Бмб варанам, находящимся в неврозе, из расчета 150 мкг/кг, приводило к значительным изменениям условно-рефлекторной деятельности. Соответственно, эти изменения были нами условно подразделены на 4 периода. Экспериментальная работа на варанах по изучению роли неопиоидного нейропептида бомбезина (Бмб) осуществлялась в несколько этапов.

На первом этапе вараны приучились к условиям экспериментальной камеры. Спустя 4-5 дней они обучались выходить в рабочий отсек экспериментальной камеры и после получения безусловного раздражителя возвращаться в стартовый отсек.

На втором этапе (6-8 дней) у варанов вырабатывали пищедобывательную реакцию в виде выдергивания зубами кормушки с пищевым подкреплением (кусочки мяса).

На третьем этапе угашали ориентировочную реакцию на посторонние световые стимулы. После угашения ориентировочно-исследовательских реакций приступали к выработке условных пищедобывательных рефлексов на световой стимул.

Было установлено, что у серого варана условные пищедобывательные инструментальные рефлексы на световые условные раздражители происходят медленно. Появившись впервые на 21.21 ± 3.0 сочетания, они упрочивались после 82.5 ± 2.4 сочетаний условного раздражителя с безусловным. Условная реакция считалась выработанной, когда вараны после получения пищевого подкрепления возвращались в стартовый отсек камеры, откуда они начинали пищедобывательную реакцию на условный положительный сигнал.

Изучение особенности угасательного торможения (путем острого угашения — применение до 15 условных раздражителей в один опытный день без подкрепления) показало следующее: образование угасательного торможения у варанов возможно, в среднем оно наступает после 9.2 ± 0.1 и укрепляется после 63.7 ± 2.7 неподкреплений.

К выработке дифференцировочного торможения у варанов мы приступили после упрочения условных

положительных реакций. В экспериментах на трех интактных варанах было обнаружено, что формирование дифференцировочного торможения со зрительного анализатора у всех варанов происходит волнообразно. Оно появляется в среднем после 12.3± 1.3 применений светового стимула без подкрепления и упрочивается после 25.4±0.4 его неподкрепления, достигая 75-80%-го критерия. В условиях наших опытов мы не отмечали 100%-го критерия его выработки. Попытка упрочения дифференцировочного торможения вызывала ослабление положительного условного рефлекса, удлинение латентного периода двигательных реакций до 10 ± 0.7 сек., при норме 4.2 ±. 0.5 сек., появлению парадоксальных отношений. Так, вараны отказывались выходить на положительный условный сигнал, не выходили на дифференцировочный раздражитель. При дальнейшей работе по упрочению дифференцировочного торможения у животных возникали невротические нарушения.

Помимо выработки простых пищедобывательных условных рефлексов, в специальной серии опытов мы вырабатывали запаздывающие условные рефлексы с различным временем оставления от 10 до 30 с. Было установлено, что формирование запаздывающих условных рефлексов у варанов возможно при 10-20 с. отставления условного стимула от безусловного. При указанном интервале времени запаздывающие условные рефлексы появляются на 16.3 ± 1.3 сочетаний условного раздражителя с безусловным и упрочивается после 71.4 ± 4.3 сочетаний. Попытка выработать запаздывающие условные реакции с большим оставлением (25 сек) приводила к срывам высшей нервной деятельности.

В серии специальных опытов у варанов изучалась подвижность основных нервных процессов путем переделки сигнального значения условного раздражителя. Было установлено, что переделка сигнального значения условных раздражителей появляется после 21.4 ± 0.2 сочетаний отрицательного условного раздражителя с безусловным подкреплением. Условная реакция закреплялась после 40.3 ±1.7 сочетаний. Следует отметить, что переделка сигнального значения раздражителей по сравнению с дифференцировочным торможением происходила медленнее и потребовала в два раза большего количества подкреплений.

Для суждения о процессах краткосрочной и долгосрочной памяти у варанов в серии специальных опытов мы изучали ее сохранение после 14-дневных, 3-месячных и 6-месячных перерывов. Обнаружено, что после 14-дневного перерыва восстановление положительных условных реакций до 80-90%-го критерия выполнения происходит уже к концу 3-4-го опытного дня. Трехмесячный перерыв приводит к полному исчезновению условного рефлекса на световой стимул. 6-месячный перерыв в работе приводил также к полному исчезновению ранее выработанных условных реакций на световой раздражитель. Условные реакции после такого перерыва полностью восстанавливались к концу 10-го опытного дня.

Таким образом, изложенные данные свидетельствуют о том, что на уровне рептилий формирование сложных форм положительных условных реакций возможно. Процессы внутреннего торможения еще недостаточно сформированы и при попытке их упрочения возникают нарушения высшей нервной деятельности.

Литература:

1. Белехова, М. Т. Таламо-теленцефальная система рептилий. — Л.: Наука. — 1977. — 215 с.
2. Карамян, А. И. Эволюция конечного мозга позвоночных. — Л.: Наука. — 1976. — 280 с.
3. Нуритдинов, Э. Н. Влияние гиппокампэктомии на условно-рефлекторную деятельность рептилий. — Изв. АН Тадж. ССР. — 1986. — № 4. — с. 127-132.
4. Сафаров, Х. М., Нуритдинов Э. Н. Влияние поэтапной экстирпации различных участков переднего мозга на условно-рефлекторную деятельность ящериц. — Изв. АН Тадж. ССР. — 1981. — № 4. (85) — с. 78-82.
5. Холбегов, М. Ё., Устоев М. Б. «Эколого-физиологические механизмы торпидности в сравнительном ряду позвоночных». Типографии «Эр-граф» Душанбе, 2016.

Строение биологической мембраны

Водопьянова Виктория Александровна, студент
Курский государственный университет

В статье автор описывает особенности структуры и основные функции эритроцитарной мембраны.
Ключевые слова: *клеточная мембрана, липиды, белки, бислой.*

Весомую роль в эритроците делает клеточная (плазматическая) мембрана, которая пропускает газы, ионы и воду.

Толщина всех биомембран оформляет от 5 до 10 нм. В их наличествуют белки, липиды, углеводы, неорганические соли, вода и ряд иных соединений.

В реальное время общепризнанной моделью строения мембран считается жидкостно-мозаичная.

Фосфолипидный бислой считается структурной единицей мембраны. Липидный бислой с обеих сторон покрыт белками. Внешняя и внутренняя стороны мембран в большинстве случаев имеют неодинаковый состав, то есть мембраны асимметричны. Липиды и белки, которые находятся на внешней стороне плазматической мембраны, имеют ковалентно связанные с ними углеводы. Внутриклеточные мембраны и внутренняя мембрана лишены данных углеводов. В согласовании с водянистой мозаичной моделью мембраны сами липиды и кое-какие белки готовы передвигаться в плоскости бислоя.

Липиды считаются более наиболее подвижным компонентом мембраны. Они имеют все шансы достаточно бегло ехать в плоскости липидного слоя (латеральное перемещение), изменяя собственных «соседей» в среднем 106 один в секунду. Латарально передвигаться в плоскости мембраны еще имеют все шансы и молекулы белков. Вполне вероятно еще, собственно, что они вертятся кругом перпендикулярных и параллельных осей плоскости бислоя, что собственно считается необходимым смыслом при функционировании макромолекул и мембран в целом.

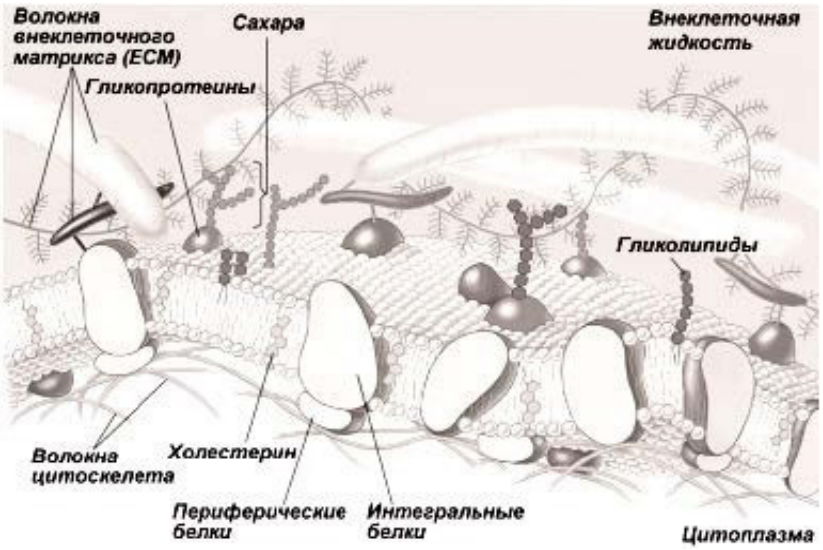


Рис. 1. **Строение жидкой мозаичной мембраны**

Впрочем, движение белковых молекул в плоскости мембраны не безусловно бегло, по причине существования взаимодействия меж отдельными белковыми молекулами и, не считая такого, меж белками мембран и цитоскелетом клеточки. В собственную очередь месторасположение белковых молекул в мембране оказывает воздействие на рассредоточивание и ориентацию липидных молекул в зависимости от сродства определенных конкретных белков и липидов.

Мембрана, как правило, содержит жидкокристаллическое положение (промежуточное меж водянистым и твердым) при подходящих для жизнедеятельности живых организмов температурах. Это положение обосновано до этого всего наличием в мембранах системы липид — белок — вода, формирующей разного на подобии упорядоченные структуры, владеющие в то же время конкретной подвижностью. Это положение мембран оказывает значительное воздействием на их функционирование и разъясняет огромную аффектация к разным наружным моментам.

Жидко-мозаичная модель разъясняет почти все качества биомембран, к примеру, неодинаковое количество молекул белка на единицу площади, асимметрию, вероятность месторасположения белков лишь только на вну-

тренней или же лишь только на внешней плоскости, различную толщину мембраны и иные.

Предоставленная модель открывает понятие о высочайшем электронном сопротивлении мембраны, избирательности проницаемости, изменчивости, а еще латеральной диффузии — движение отдельных липидов и белков в плоскости внешнего монослоя со значимой скоростью.

В перечень ведущих функций плазматической мембраны входят: избирательная проницаемость, межклеточные взаимодействия, эндоцитоз, экзоцитоз.

Липиды (фосфолипиды, сфинголипиды, холестерин) оформляют до 45% массы мембран.

Молекула фосфолипида произведено из полярной (гидрофильной) части (головка) и аполярного (гидрофобного) двойного углеводородного хвоста. В аква-фазе молекулы фосфолипидов механически агрегируют задолженность к хвосту, создавая каркас биомембраны в облике двойного слоя (бислой). Этим образом, в мембране хвосты фосфолипидов ориентированы вовнутрь бислоя, а головки обращены кнаружи.

Сфинголипиды — липиды, которые содержат базу с длинноватой вереницей (сфингозин или же схожую с ним группу).

Холестерин, имеющй очень весомое смысл для клеточки, циркулирует во внутренней среде организма в составе липопротеинов.

Главные фосфолипиды эритроцитарной мембраны — кислые липиды (заряженные отрицательно) сфингомиелин и фосфатидилэтаноламин, и нейтральные липиды (цвиттерионы) фосфатидилхолин и фосфатидилсерин.

Всевозможные классы липидов в мембране находятся не беспорядочно. Есть как трансмембранная асимметрия, например и планарная гетерогенность их рассредоточивания. К примеру, для мембраны эритроцитов человека свойственно надлежащее асимметричное месторасположение фосфолипидов: во наружной половине бислоя размещено 70% фосфатидилхолина и 80% сфингомиелина, во внутренней же половине располагается практически целый фосфатидилсерин и до 70% фосфатидилэтаноламина.

Это говорит о том, собственно, что при физическом смысле pH внутренняя сторона мембраны заряжена негативно.

Белки оформляют больше 50% массы мембран. Основная масса мембранных белков содержит глобулярную структуру.

Интегральные мембранные белки крепко интегрированы в липидный бислой. Их гидрофильные аминокислоты ведут взаимодействие с фосфатными группами фосфолипидов, а гидрофобные — с цепями жирных кислот. Молекула белка, проходящая сквозь всю толщу мембраны и выступающая из нее как на внешней, например и на внутренней плоскости, — трансмембранный белок.

Периферические мембранные белки присутствуют на одной из плоскостей клеточной мембраны (наружной или же внутренней) и нековалентно связаны с интегральными мембранными белками.

Гидрофобный нрав сердцевины бислоя определяет вероятность (или невозможность) конкретного проникания сквозь мембрану всевозможных с физико-химической точки зрения препаратов (в первую очередь, полярных и неполярных).

Неполярные препараты (например, холестерин и его производные) бегло попадают сквозь биомембраны.

Полярные препараты (например, белки и ионы) не имеют все шансы просачиваться сквозь биомембраны.

Пути реализации избирательной проницаемости мембран:

— Инертный автотранспорт характеризуется невысокой спецификой. Молекулы в обоих инструкциях передвигаются по градиенту сосредоточении без расходов энергии.

— Облегченная диффузия. Автотранспорт препаратов исполняется с ролью компонент мембраны (каналы и/или белки-переносчики) по градиенту сосредоточении и без конкретных расходов энергии; показывают специфика к транспортируемым молекулам.

— Деятельный автотранспорт — происходящий при участии АТФаз энергозависимый трансмембранный перенесение ионов напротив химического градиента.

Литература:

1. Учебно-методическое пособие В. А. Лавриненко А. В. Бабина, Новосибирск, 2015.
2. Учебное пособие для проведения практических занятий по курсу «Цитогенетика» Алиева И. Б., Киреев И. И., Курчашова С. Ю., Узбеков Р. Э., МОСКВА — 2010

Особенности экспериментальных неврозов у животных

Нурматов Акпар Абдусатторович, доктор медицинских наук, профессор
Гулистанский медицинский колледж (Узбекистан)

Азимова Гулнора Норбобоевна, кандидат биологических наук, доцент
Таджикский государственный медицинский университет имени Абуали ибни Сино (г. Душанбе, Таджикистан)

В работе установлено, что, несмотря на то, что двигательно-пищевые условные рефлексы у ушастого ежа (Hemiechynus auritus) формируются быстро, функциональные временные связи образуются долго (в течение 2,5 месяца). После усложнения задачи эксперимента у животных появляются невротические состояния возбудительного и тормозного типов, которые состоят из 3-х стадий.

Ключевые слова: *ушастый еж, условные рефлексы, невротические состояния.*

Features of experimental neurosis in animals

Nurmatov Akpar Abdusattorovich, doctor of medical sciences, professor
Gulistan Medical College (Uzbekistan)

Azimova Gulnora Norboboevna, candidate of biological sciences, associate professor
Tajik State Medical University named after Abuali ibni Sino (Dushanbe, Tajikistan)

In experiments with defensive behavior using multiparametrie recording of indices, stadies have been made on the origin and development of pathological disturbances in higher nervous activity on insectivores during presentation of difficult conditioned reflecx problems of extreme stimulation. It was found that elaboration of absolute differentiation retarded conditioned reactions with a delay of 2-5 months in insectivores is a difficult task which results in pathological charges in the higher nervous activity. In hedgehogs, neurotic changes are immediate, all the investigated indices being affected, if has 3 stages.

Keywords*; Eared hedgehog, conditioned reflexes, neurotic states.*

Актуальность работы. В работах [1, 2], выполненных на представителях различных дивергентных линий животных, был обнаружен уникальный феномен легкого возникновения патологических нарушений высшей нервной деятельности (ВНД), получивший известность как феномен «торможения с подкреплением». В других исследованиях [3] на модели пищевого подкрепления у позвоночных при выработке форм внутреннего торможения также имело место нарушение высшей нервной деятельности, в связи с чем было высказано важное положение о том, что невротические нарушения легко возникают у животных, стоящих на низких этапах эволюционного развития.

Особый интерес представляют именно те формы невротических нарушений, которые не сразу обнаруживаются, остаются незамеченными в обычном стереотипе и выявляются лишь в ходе усложнения задач эксперимента (экспериментальные неврозы) и которые нельзя назвать «скрытыми», так как при них постоянно наблюдаются выраженные расстройства процессов высшей нервной деятельности.

Целью настоящей работы явилось изучение особенностей высшей нервной деятельности и ее патологических нарушений у насекомоядных (ежей) в различных функциональных состояниях. С помощью условно-рефлекторной методики и корреляции с поведенческими и вегетативными показателями были обнаружены патологические нарушения высшей нервной деятельности, возникающие у животных при предъявлении им сложных условно-рефлекторных задач.

Было обнаружено, что невротические нарушения у ежей имели место уже в процессе укрепления пищедобывательных условных реакций, после применения более 20 сочетаний условных и безусловных сигналов в течение каждого опытного дня. Однако эти нарушения имели кратковременный характер и быстро купировались после 1-2-дневных перерывов в работе.

Основными этиологическими признаками экспериментального невроза подопытных ежей явились: нерегулярная (атипичная) условно-рефлекторная деятельность, нарушение траекторий движения, нарушения функциональной лабильности мозга, неадекватные ответы на слуховые и зрительные раздражители, нарушение функций сердечно-сосудистой и дыхательной системы, а также ряд трофических расстройств.

Увеличение времени запаздывающего торможения от 25 до 35 секунд вызвало полный отказ ежей участвовать в эксперименте. На условные положительные сигналы реакция животных была неадекватна, систематически падала динамика условных правильных ответов (в %), латентный период реакции увеличивался постепенно, дифференцировка была расторможена полностью.

Сильно изменилась динамика формирования вегетативных и двигательных компонентов условного пищедобывательного рефлекса (рис. 1).

Результаты опытов по выработке запаздывающих условных рефлексов у ежей с большим временем отставления и анализ полученных данных позволили нам выделить три стадии невротических состояний:

1-я стадия заключается в ускорении латентного периода условных реакций. При 25-секундной отсрочке эта реакция сокращается до 8-25 сек. Увеличиваются межсигнальные реакции, чесательные движения, хаотические круговые движения, отказ возвратиться в стартовый отсек.

2-я стадия невротических нарушений характеризовалась, помимо условно-рефлекторных изменений и двигательного беспокойства, значительными вегетативными нарушениями, как-то: непрерывная дефекация, диурез, вокализация, афагия и т. д.

3-я стадия невроза, выявляющаяся преимущественно у ежей со слабым типом высшей нервной деятельности, заключалась в резком падении веса тела, трофических расстройств в виде выпадения игл, облысения, отказа от пищи. Животные в 3-й стадии невроза обычно погибают.

Выводы. Таким образом, можно заключить, что на уровне насекомоядных процессы внутреннего торможения еще слабо выражены. Вследствие этого выработка абсолютной дифференцировки или запаздывающих условных реакций для них является биологически трудной задачей, и животные легко впадают в невротическое состояние. На этом этапе филогенеза невроз развивается «с места», при этом в патологические нарушения высшей нервной деятельности одновременно включаются все изученные функциональные системы — поведенческие, соматические и вегетативные.

Литература:

1. Нуритдинов, Э. Н. Нейропептиды и поведение. — Душанбе: Сино, 2002. — 180 с.
2. Нуритдинов, Э. Н., Рафиев А. Н. Дерморфин и поведение. — Душанбе: Сино, 1994. — 158 с.
3. Холбегов, М. Ё., Устоев М. Б. «Эколого-физиологические механизмы торпидности в сравнительном ряду позвоночных». Типографии «Эр-граф» Душанбе, 2016

МЕДИЦИНА

Кристаллическая дистрофия Bietti — редкое генетическое аутосомно-рецессивное заболевание

Айрапетян Аркадий Арменович, студент;
Карасов Илья Андреевич, студент;
Умаров Акбарджон Хусейнович, студент;
Колесникова Юлия Андреевна, студент
Научный руководитель: Пономаренко Елена Владимировна, кандидат медицинских наук, доцент
Пермский государственный медицинский университет имени академика Е. А. Вагнера

Кристаллическая дистрофия Биетти (КДБ) — редкое аутосомно-наследственное наследственное заболевание, вызываемое мутациями в CYP4V2 гена. Профессор Джан Баттиста Битетти впервые описал это заболевание в 1037 году [1], сообщив о трех пациентах, включая двух братьев, с кристаллическими пятнами сетчатки в заднем полюсе, рассеянными скоплениями пигмента сетчатки, атрофией и поверхностными отложениями в роговице.

КДБ наследуется по аутосомно-рецессивному типу, что означает, что обе копии гена в каждой клетке имеют мутации. Каждый из родителей человека с аутосомно-рецессивным заболеванием — несут по одной копии мутировавшего гена, но обычно не проявляют признаков и симптомов этого состояния. [7] КДБ связана с мутацией гена CYP4V2, этот ген способствует созданию фермента цитохрома P450, эти ферменты участвуют в образовании и распаде различных химических веществ в клетках, фермент CYP4V2 участвует в многоступенчатом процессе, называемом окислением жирных кислот, в котором липиды расщепляться и превращаются в энергию, при мутациях гена CYP4V2 функция фермента нарушается, и это влияет на распад липидов.

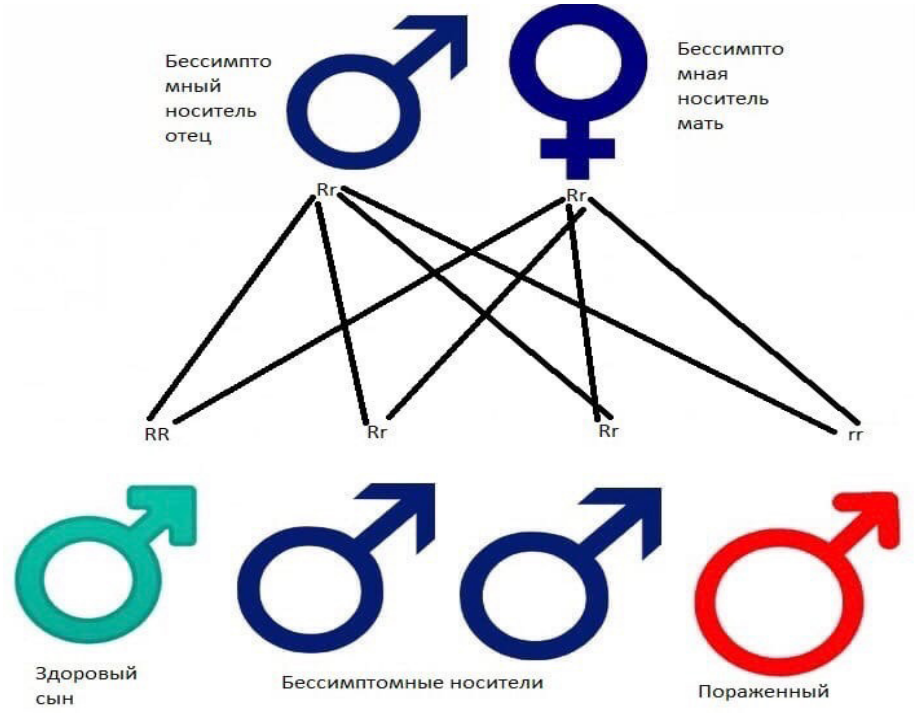


Рис. 1. **Рецессивный образец наследования**

Оценить распространенность КДБ довольно сложно, так методы сбора информации отличаются, в зависимости от страны, авторов и опросов, автор Hu [2], сделал заключение и оценил частоту гена 0,005, изучая первых двоюродных братьев и сестер при обследовании в Китае в 1983 году. Автор Okialda et al [3] оценил распространенность КДБ на 1 человека из 67000 человек, из которых страдают 21000 пациента в Китае и около 5000 в США. Но данное заболевание распространенно по всему миру и является обычным явлением на востоке Азии, являясь более распространенным среди китайского, японского и корейского населения, так же много есть зарегистрированных случаев, диагностированных в Европе, относящиеся к пациентам из Италии, Ливана и Испании, вследствии чего можно сделать вывод, что возможно и средиземноморское распространение болезни [4].

КДБ — это прогрессирующая дистрофия с поражением роговицы, характеризующаяся обильными желтоватыми сверкающими отложениями на сетчатке, потерей хориокапилляров, атрофией и кристаллических отложений в периферической роговице.

Кристаллическую дистрофию Биетти Yuzawa et al [5], разделил на 3 стадии:

1 стадия — атрофия пигментного эпителия сетчатки с кристаллическими отложениями в области макулы;

2 стадия — атрофия пигментного эпителия сетчатки выходит за пределы заднего полюса, происходит атрофия хорикокапилляров на заднем полюсе;

3 стадия — обширная атрофия пигментного эпителия сетчатки и хорикокапилляров, кристаллические отложения по всему глазному дну.

Первые клинические проявления будут проявляться между вторым и третьим десятилетием жизни, но могут развиваться у подростков и у пожилых людей, самые ранние стадии протекают бессимптомно, что усложняет его диагностику. Поэтому при диагностировании заболевания на самых ранних стадиях происходит часто случайным образом, по мере прогрессирования КДБ симптомы будут проявляться медленно и безболезненно, ограничивая периферическое зрение и сужение поля зрения, нарушение цветового зрения, помутнения, фотопсия. На поздних стадиях заболевание обнаруживается уже с серьезными нарушениями зрения. Так же стоит подметить, что заболевание может быть асимметричным в обоих глазах. [6].

Диагностика КДБ основана на офтальмологической оценке многочисленных мелких блестящих желто-белых кристаллических отложений в сетчатке или же без каких-либо кристаллических отложений в роговице, атрофии пигментного эпителия сетчатки и склероза сосудистой оболочки глаз, [8] кристаллы обычно изолированы в субэпителиальной и передней строме периферической роговицы [9]. Диагностические инструменты включают электроретинографию для оценки степени дисфункции палочек и колбочек, тест поля зрения Хамфри для выявления дефицита поля зрения, зеркальная микроскопия [10]. Так же можно прибегнуть к молекулярно-генетическому тестированию для идентификации патологических вариантов CYP4V2, если клинические признаки сомнительны [11].

Литература:

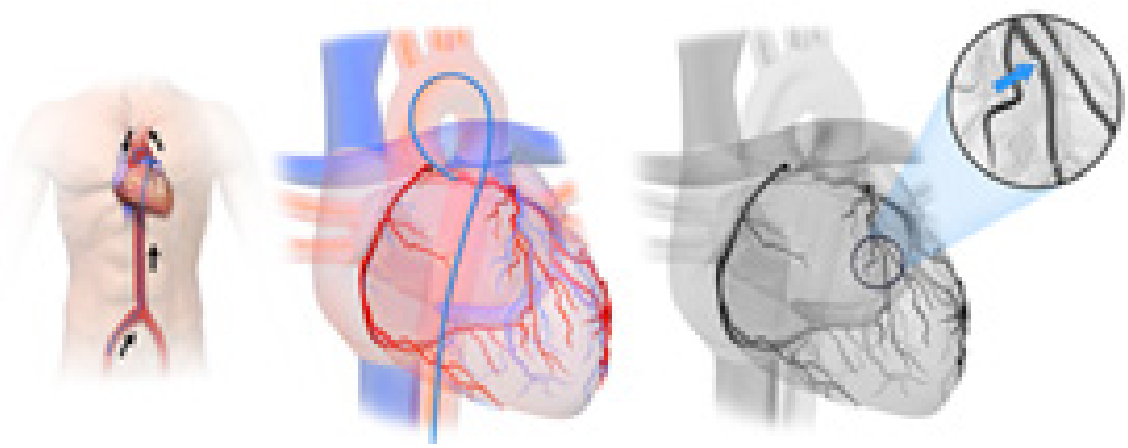
1. Bietti, G. Ueber faxmiliares Vorkommen von «Retinitis punctata albescens» (verbunden mit «маргинальная дистрофия роговицы»), glitzern, des glaskorpers und anderen degenerativen augenveranderungen. Klin Monbl Augenheilkd. 1937; 99: 737-756.
2. Hu DN. Ophthalmic genetics in China. Ophthal Paed Genet. 1983;2:39-45.
3. Okialda KA, Stover NB, Weleber RG et al. Bietti Crystalline Dystrophy. In: Pagon RA, Bird TD, Dolan CR et al. editors. Gene ReviewsTM. Seattle (WA) University of Washington, Seattle: 1993-2014
4. García-García GP, Martínez-Rubio M, Moya-Moya MA, Pérez-Santonja JJ, Escribano J. Identification of novel CYP4V2 genotypes associated with Bietti crystalline dystrophy and atypical anterior segment phenotypes in Spanish patients. Acta Ophthalmol. 2018;96 (7):e865 — e873. doi:10.1111/aos. 13768
5. 5-Yuzawa M, Mae Y, Matsui M. Bietti»s crystalline retinopathy. Ophthalmic Paediatr Genet. 1986;7:9-20. doi:10.3109/13816818609058037
6. Haddad NM, Waked N, Bejjani R, et al. Clinical and molecular findings in three Lebanese families with Bietti crystalline dystrophy: report on a novel mutation. Mol Vis. 2012;18:1182-1188
7. Li, A; Jiao, X; Munier, Fl; Schorderet, Df; Yao, W; Iwata, F; Hayakawa, M; Kanai, A; Shy, Chen, M; Alan, Lewis, R; Heckenlively, J; Weleber, Rg; Traboulsi, Ei; Zhang, Q; Xiao, X; Kaiser-Kupfer, M; Sergeev, Yv; Hejtmancik, Jf. Bietti crystalline corneoretinal dystrophy is caused by mutations in the novel gene CYP4V2 (англ.) // American Journal of Human Genetics (англ.): journal. — 2004. — May (vol. 74, no. 5). — P. 817-826. — doi:10.1086/383228. — PMID 15042513.
8. Furusato E, Cameron JD, Chan CC. Evolution of Cellular Inclusions in Bietti»s Crystalline Dystrophy. Ophthalmol Eye Dis. 2010;2010 (2):9-15.
9. Krachmer J, Mannis M, Holland E: CORNEA, 4th ed. Elsevier Mosby, 2017, 251-264.
10. Vargas M, Mitchell A, Yang P, Weleber R. Bietti Crystalline Dystrophy. GeneReviews. 2012.

11. Xiao X, Mai G, Li S, Guo X, Zhang Q. Identification of CYP4V2 mutation in 21 families and overview of mutation spectrum in Bietti crystalline corneoretinal dystrophy. Biochem Biophys Res Commun. 2011;409 (2):181-6.

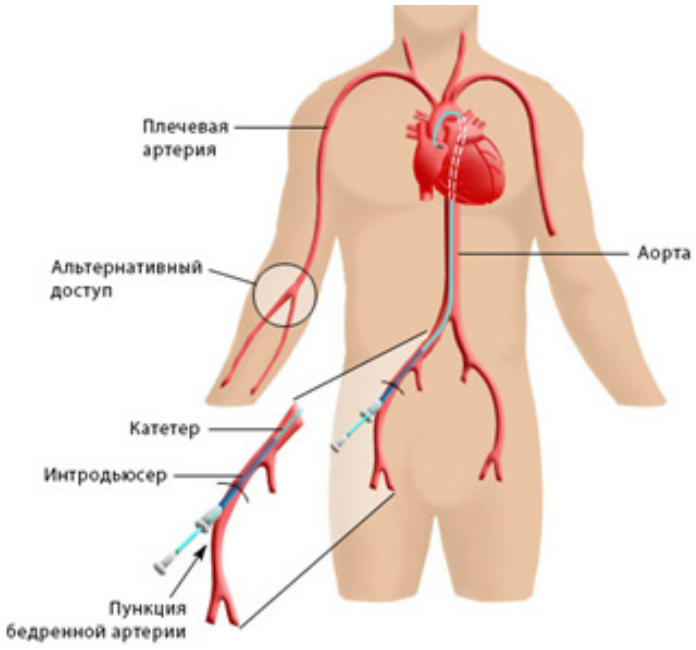
Осложнения после коронароангиографии

Болотова Алтана Эрдэниевна, ординатор
Читинская государственная медицинская академия (г. Чита)

В настоящее время отмечается постоянное увеличение количества и объема различных кардиохирургических вмешательств, расширяются показания к их применению, активно внедряются современные технологии, развиваются новые направления, прогрессирует эндоваскулярная хирургия. Однако такие инвазивные методы приводят к росту сосудистых осложнений, нередко опасных для жизни больного.



Коронароангиография — это инвазивная диагностическая процедура, при которой радиоконтрастное вещество вводится с в коронарные артерии с целью изучения анатомии и возможных нарушений проходимости коронарных сосудов. Используются доступы через общую бедренную артерию (феморальный) или через лучевую артерию (радиальный).



Факторы риска, предрасполагающие к появлению осложнений:

Модифицируемые:

— применение медикаментов (антикоагулянты, дезагреганты)
— артериальный доступ
— метод обеспечения гемостаза

Немодифицируемые:

— пол (женский)
— возраст (старше 70 лет)
— масса тела
— отягощенный аллергологический анамнез
— артериальная гипертензия
— выраженный атеросклероз
— почечная недостаточность
— сахарный диабет и сердечная недостаточность.
—

Осложнения, возникающие на разных этапах коронароангиографии

Этап процедуры	Возможные осложнения
Седация и местная анестезия	Аллергические реакции
Пункция артерии и введение в нее инструментов	Кровотечение из места пункции Ретроперитонеальное кровотечение Гематома Псевдоаневризма Артериовенозная фистула Расслоение бедренной и подвздошной артерии Тромбоэмболическая окклюзия Феморальная нейропатия Вазоспазм Инфекция локальная и (крайне редко) генерализованная
Введение контрастного вещества	Анафилактоидные реакции Токсические эффекты Нефропатия
Введение гепарина	Кровотечение Гепарин-индуцированная тромбоцитопения
Проведение проводников и катетеров к коронарным артериям	Вазовагальные реакции Нарушения ритма и проводимости Холестериновая эмболия Расслоение аорты и коронарных артерий Инфаркт миокарда Рестеноз внутри стента Феномен «no reflow» Церебральный инсульт

Цель работы. Оценить характер и частоту ангиологических осложнений после инвазивных вмешательств в кардиологическом и кардиохирургическом отделениях.

Материалы и методы. Проанализирована деятельность отделений кардиологии и кардиохирургии в Краевой клинической больнице г. Чита за 2017 год. В отделении кардиохирургии было выполнено 2327 операций на сердце и сосудах, из них операции на открытом сердце, в том числе 48 АКШ, 1 ЭКМО; произведено 658 коронарографий, 20 стентирований коронарных артерий, 23-сонных, подключичных, подвздошных, бедренных, подколенных, берцовых артерий. В отделении кардиологии было выполнено 539 ЧТКА со стентированием. Проведен анализ отчетов профильных отделений: историй болезней, протоколов вмешательств, процедур, исследований. Регистрировались такие осложнения, как постпункционные гематомы, тромбозы стентов.

Результаты. Частота сосудистых осложнений в отделении кардиохирургии: 0,6% — 14 постпункционных гематом, в отделении кардиологии: 3,52% — 16 постпункционных гематом, 3 тромбоза стента.

Заключение. Допустимый процент сосудистых осложнений (постпункционная гематома) по мировой статистике составляет 0,43%. Единственным требованием после пункции является строгий постельный режим в течение суток (который нередко пациенты нарушают) и адекватная компрессионная давящая повязка в месте пункции. Большая часть данных осложнений прошла в отделении кардиологии, что связано с приемом больными антикоагулянтов, антиагрегантов в раннем послеоперационном периоде. Для снижения частоты указанных осложнений целесообразно сосредоточение совместных усилий кардиологов, сердечно-сосудистых хирургов, эндоваскулярных интернистов; внедрение современных технологий; обеспечение высокого уровня квалификационной подготовки специалистов.

Влияние загрязнения атмосферного воздуха на здоровье детей дошкольного возраста

Кайпова Динара Бекеновна, резидент;
Мамау Зере Алимбеккызы, резидент
Научный руководитель: Мамбетова Индира Зинабдиновна, кандидат медицинских наук, доцент
Казахский национальный медицинский университет имени С. Д. Асфендиярова (г. Алматы, Казахстан)

В статье авторы изучают влияние солей тяжелых металлов на общую заболеваемость и состояние физического развития детей дошкольного возраста.

Ключевые слова: *соли тяжелых металлов, структура заболеваемости, физическое развитие, дети*

Проблема загрязнения атмосферного воздуха мегаполисов оказывает неблагоприятное влияние на здоровье населения, где наиболее уязвимой группой является детская популяция. *В настоящее время экологические проблемы Алматы являются наиострейшими, источниками загрязнения являются выбросы от автотранспорта и стационарных объектов* [1,2].

Цель исследования: Изучить влияние солей тяжелых металлов на общую заболеваемость и состояние физического развития детей дошкольного возраста.

Материалы и методы исследования: Проводилось обследование и анализ амбулаторных карт (Ф-112у) 250 детей в возрасте от 3 до 6 лет, проживающих в 2-х условных экологических зонах г. Алматы. Для более глубокого анализа детей разделили по возрасту на 2 группы: основную группу (175 детей), проживающих в экологически неблагополучном нижнем районе и группу контроля (75детей), проживающих в относительно чистом горном *микро*районе.

При распределении по возрастным группам установлено, что в основной и в контрольной группах большинство детей были в возрасте 6 лет: 62/35,5% и 21/27,7%. Детей в возрасте 4-5 лет в процентном соотношении было почти одинаковое количество: 42/24,1% и 19/25,4% соответственно. Наименьшее количество детей в основной группе было в возрасте 3-х лет — 31/17,7% по сравнению с контрольной группой — 18/24,1%.

Для сравнительного анализа изучали содержание солей тяжелых металлов в волосах, заболеваемость и антропометрические показатели у детей обеих групп [3].

Статистическая обработка проводилась общепринятыми в вариационной статистике методами. Достоверность различий устанавливалась с помощью критерия Стьюдента-Фишера (t), различия считались статистически достоверными при $p<0,05$ [4].

Результаты и обсуждение. В ходе исследования наблюдается достоверное увеличение концентрации свинца по мере увеличения возраста детей. В возрасте 3-4 лет различался только уровень Zn (0,007±0,002), при отсутствии изменений со стороны других металлов. Тогда как у детей более старшего возраста уровень концентрации свинца у 110/62,3%) и цинка у 100/56,5% выше по сравнению с контрольной группой ($p<0,001$) (Таблица № 1).

Таблица 1. **Частота встречаемости солей тяжелых металлов в исследованных волосах детей дошкольного возраста**

Соли тяжелых металлов	Группы				P
	Основная (n=175)		Контрольная (n=75)		
	n	M±m, %	n	M±m, %	
Zn, %	100	56,5±4,*	2	2,4±1,8	<0,001
Se, %	92	51,9±4,*	2	2,4±1,8	<0,001
Cd, %	32	18,1±3,*	1	1,2±1,2	<0,001
Pb, %	110	62,3±3,*	2	2,4±1,8	<0,001
Ni, %	22	12,4±3,*	1	1,2±1,2	<0,001

Таким образом, концентрация свинца выше у детей из основной группы, чем в контрольной. По результатам наших анализов установлена взаимозависимость концентраций: чем выше содержание свинца, тем ниже оказалась концентрация селена и цинка ($p<0,01$), что входит в понятие дисэлементоз [5].

По результатам использования критериев оценки здоровья нами определены группы здоровья. Наибольший процент детей имели IIB группу здоровья — 75/42,4% ($p<0,001$) и III группу — 42/23,7% ($p>0,05$). В IIA группу здоровья вошли 28/15,8% и 32/18,1% детей в I группу [6].

Изучение амбулаторных карт детей показало, что в основной группе у 118 детей отмечались различные заболевания. Чаще встречались дети с заболеваниями органов дыхания и неблагополучным аллергическим фоном у 17,3% мальчиков и. 15,2% девочек. В структуре заболеваемости у детей дошкольного возраста у мальчиков до-

Таблица 2. **Структура заболеваемости детей 3-6 лет по нозологическим формам в зависимости от пола у детей основной группы**

Нозологические формы	Мальчики, n=52		Девочки, n=66		p
	n	M±m, %	n	M±m, %	
Заболевания дыхательной системы, в т. ч. аллергические	9	17,3±3,4	10	15,2±3,2	>0,05
Заболевания нервной системы	19	36,5±3,5*	18	27,3±3,0	<0,05
Заболевания ЖКТ	5	9,6±2,6	6	9,1±2,6	>0,05
Заболевания ССС	3	5,7±2,1	5	7,6±2,4	>0,05
Анемия ЖД	5	9,6±2,6	9	13,6±3,1	>0,05
Заболевания мочеполовой системы	5	9,6±2,6	7	10,6±2,8	>0,05
Ожирение	2	3,9±1,7	5	7,6±2,4	>0,05
Заболевания кожи	2	3,9±1,7	3	4,5±1,8	>0,05
Другие	2	3,9±1,7	3	4,5±1,8	>0,05
Итого:	52	100%	66	100%	
Примечание — * — достоверное отличие мальчиков от девочек, p<0,05					

стоверно преобладали заболевания нервной системы — 19/36,5% (p<0,05) (Таблица 2).

Мы предполагаем, что относительно высокой уровень болезней нервной системы связан с наличием в атмосферном воздухе высокого уровня. свинца. Как известно, наиболее подверженной его вредному воздействию является нервная система [7].

У детей контрольной группы также выявлена патология органов и систем, но значительно ниже, чем в основной (p<0,05).

В основной и контрольной группах в сравнительном аспекте проведена оценка физического развития детей. Анализ показателя роста продемонстрировал снижение в основной группе детей — у 152/85,9% по сравнению с контрольной группой (p<0,001). В пределах нормы ростовой показатель установлен у 20/12,4%, превышение нормы в 3 случаях/1,7%. Дети контрольной группы только в 3,6% характеризовались превышением ростового показателя (Таблица 3).

Таблица 3. **Средние показатели физического здоровья детей в зависимости от возраста (M±m)**

Возраст детей	Основная, n=175			Контрольная, n=75		
	масса	рост	ОГК, см	масса	рост	ОГК, см
3 года	13,1±0,29**	95,7±1,27**	50,8±0,34**	15,6±0,20	112,4±1,0	54,5±0,32
4 года	15,5±0,30**	102,7±0,66**	52,2±0,24**	17,4±0,23*	115,8±0,39*	56,9±0,25*
5 лет	17,1±0,31**	107,8±1,0**	52,9±0,26**	19,4±0,24*	117,7±0,18*	58,5±0,30*
6 лет	19,6±0,30**	111,8±0,71**	55,2±0,22**	22,5±0,41*	119,7±0,15*	60,3±0,24*
Примечания — 1* — достоверные различия между показателями по возрастам, p<0,001 2** — достоверное отличие от контрольной группы, p<0,001						

Анализируя физическое развитие детей в основной группе по возрастам, можно отметить, что антропометрические данные у детей 3-х лет не имеют выраженного отставания, хотя и находятся на нижней границе нормы. Наиболее заметен дефицит весовых показателей детей дошкольного возраста 4-6 лет. Только у 30 детей/17.1%, (p<0,001) в основной группе масса тела была в пределах нормы, в отличие от контрольной группы 71/94,6%, (p<0,001). Выявлено 9 (5,1%) детей с повышенным весом, что является отклонением от нормы. В дальнейшем эти дети имеют риск развития ожирения, сахарного диабета и заболеваний сердечно-сосудистой системы.

Выводы:

1. В неблагоприятной зоне г. Алматы наибольшую концентрацию накопления в организме имеет свинец, который оказывает наиболее агрессивное действие на здоровье детей. Выявлена взаимозависимость концентрации свинца от концентрации цинка и селена у детей 3-6 лет.

2. Выявлено влияние содержания концентраций тяжелых металлов на высокую заболеваемость детей 3-6 лет.

3. Накопление солей тяжелых металлов оказывает негативное влияние на физическое развитие. Отмечается отставание окружности грудной клетки у детей 5-6 лет. У детей 4 лет отстают все показатели антропометрии; масса 15,5±0,3 (контроль 16,5±0,2) рост 102,7±0,6 (контроль 105,1±0,6) и окружность грудной клетки 52,1±0,2 (контроль 54,6±0,6).

Литература:

1. Салимбаева, Р. А. Журнал «Вестник КазЭУ» (2012). «Экология и устойчивое развитие города Алматы»: http://articlekz. com/article/13892.
2. Информационные бюллетени о состоянии окружающей среды в РК. https://www. kazhydromet. kz/ru/ecology/informacionnye-byulleteni-o-sostoyanii-okruzhayuschey-sredy-respubliki-kazahstan
3. Бондаренко, В. П., Киреева Г. Н. Методы лабораторной диагностики здоровья детей в экологически неблагоприятных районах/Междисциплинарная научно-практическая конференция с международным участием: «Здоровье населения моногородов. — Челябинск, 2014. — с. 13-16
4. Ланг, Т. А. Описание статистики в медицине. Руководство для авторов, редакторов и рецензентов/Т. А. Ланг, М. Сесик. — М.: Практическая медицина. — 2011. — 477 с.
5. Гичев, Ю. П. Загрязнение окружающей среды и здоровье человека/Ю. П. Гичев. — Новосибирск: СО РАМН, 2002. — 230 с.
6. Основы здоровья детей и подростков: руководство для врачей. Часть I. Комплексная оценка здоровья детей и подростков — Екатеринбург: УГМУ, 2017. — 126 с.
7. Кудрин, А. В. Микроэлементы в неврологии/А. В. Кудрин, О. А. Громова. — М.: ГЭОТАРМедиа, 2006. — 304 с.

Болезнь мойя-мойя — редкая причина ишемии головного мозга и интракраниальных кровоизлияний

Карасов Илья Андреевич, студент;
Айрапетян Аркадий Арменович, студент;
Умаров Акбарджон Хусейнович, студент;
Колесникова Юлия Андреевна, студент
Научный руководитель: Пустоханова Людмила Васильевна, кандидат медицинских наук, доцент
Пермский государственный медицинский университет имени академика Е. А. Вагнера

Болезнь мойя-мойя — редкое хроническое прогрессирующее заболевание, которое характеризуется сужением просвета внутренних сонных артерий у основания головного мозга, где происходит последующее деление на средние и передние мозговые артерии. При данной патологии стенки артерий утолщаются, что приводит к стенозу сосудов, и, как следствие, к развитию коллатерального кровообращения. Эти новообразованные сосуды будут иметь на ангиограмме характерный вид «облака» («Мойя-мойя» в переводе с японского означает «клубок дыма»). Опасность коллатеральных сосудов при болезни мойя-мойя заключается в том, что они имеют более хрупкие стенки, нежели нормальные кровеносные сосуды и имеют повышенный риск образований аневризм и разрывов, что может привести к кровоизлиянию [1-3].

По сей день точная этиология болезни мойя-мойя неизвестна, однако недавние генетические исследования идентифицировали RNF213 в области 17q25-ter как важный ген в развитии болезни мойя-мойя среди населения Восточной Азии [3, 4]. При этом в Японии у 10% пациентов с данной патологией имеются родственники, так же страдающие от мойя-мойя [5]. Однако не стоит думать, что данное заболевание распространено только среди лиц азиатского происхождения, но в настоящее время это заболевание наблюдается во всем мире и у людей разных этнических групп.

Что касается возрастных особенностей, то пики заболевания приходятся на два возрастных диапазона: дети в возрасте 5-и лет, взрослые люди в возрасте от 40 до 11 лет [1], однако необходимо отметить, что пациенты женского пола страдают от этого недуга в два раза чаще, нежели пациенты мужского пола [2]. Что касается распространенности в популяции, то по данным масштабного американского обзора 2005 года (Uchino et al.), можно увидеть, что заболеваемость составляет 0,086 случая на 100000 человек, что позволяет отнести данную патологию к орфанным заболеваниям. [3].

Так как основным проявлением заболевания являются изменение кровотока по каротидному бассейну, выделяют две основные группы симптомов — вызванные непосредственно ишемией головного мозга и те симптомы, которые возникают вследствие формирования компенсаторных механизмов, реагирующих на церебральную ишемию.

Ишемические симптомы могут быть как временными (преходящими), так и постоянными. К этой группе можно отнести такие симптомы как гемипарез, дизартрия, афазия и когнитивные нарушения. Как правило, симптомы связаны с нарушением кровотока по внутричерепному отделу сонной артерии, а так же среднемозговым артериям [2]. Помимо ишемии болезнь мойя-мойя провоцирует так же и внутричерепные кровоизлияния, так

как при данной патологии увеличивается хрупкость сосудистой стенки, что таит в себе повышенный риск ее разрыва. Кровоизлияния могут быть как внтрижелудочковые, так и интрапаренхиматозные или субарахноидальные [6, 7]. Ко второй группе симптомов можно отнести головные боли, спровоцированные сосудами мойя-мойя. Вследствие расширения менингеальных и лептоменингеальных коллатеральных сосудов может произойти стимуляция ноцицепторов твердой мозговой оболочки, которые расположены вдоль крупных ветвей внутричерепного отдела сонной артерии. Такая стимуляция неизбежно приводит к головным болям, которые являются наиболее частым симптомом при болезни мойя-мойя [8-10]. Как правило, головная боль похожа на типичный приступ мигрени, не купируется медикаментозной терапией. Особенно значительной эта проблема выглядит и потому, что данный симптом сохраняется более чем у 60% пациентов даже после успешной хирургической реваскуляризации — так как основная причина подобных головных болей не в ишемии головного мозга, а в стимуляции ноцицепторов патологическими сосудами, которые, как правило, сохраняются при хирургическом лечении [4, 6].

Так как жалобы, характерные для рассматриваемой патологии неспецифичны и присутствуют при многих цереброваскулярных заболеваниях, для постановки окончательного диагноза, звучащего как «болезнь мойя-мойя» необходимо выполнение визуализирующих исследований, позволяющих оценить состояние интракраниального сосудистого русла [11-13].

Ранее критерием постановки диагноза было подтвержденное двухстороннее поражение внутренней сонной артерии, но в настоящее время диагноз болезни мойя-мойя правомочен и при наличии у пациента односторонней терминального стеноза или окклюзии внутренней сонной артерии в дистальных отделах. Как правило, для диагностики используют каротидную артериографию, так же возможно применение мультиспиральной компьютерной томографии или магнитно-резонансной томографии с контрастным усилением [12, 13]. Ультразвуковое дуплексное сканирование малоэффективно. На основании стадийного прогрессирования болезни Сузуки и Такау предложили следующие шесть последовательных этапов ангиографической картины при болезни мойя-мойя [12]:

Стадия 1 — сужение внутренних сонных артерий

Стадия 2 — расширенные передние и средние мозговые артерии с сужением бифуркации ВСА с характерными изменениями

Стадия 3 — дальнейшее изменение бифуркации ВСА и сужение передних и средних мозговых артерий (чаше всего диагностируют на этой стадии)

Стадия 4 — минимизация сосудов мойя-мойя и увеличение коллатеральных сосудов

Стадия 5 — сокращение сосудов мойя-мойя и значительное сужение внутренней сонной артерии

Стадия 6 — исчезновение сосудов мойя-мойя, полная закупорка внутренних сонных артерий и коллатеральных сосудов головного мозга. На терминальной стадии кровоснабжение головного мозга осуществляется за счет ветвей наружной сонной артерии.

В настоящее время не разработано специфического консервативного лечения для болезни мойя-мойя. При наличии в анамнезе у пациента с мойя-мойя перенесенного острого нарушения мозгового кровообращения с высоким риском повторного сосудистого события, применяют хирургическую реваскуляризацию [10]. При лечении данной патологии применяют как прямую, так и непрямую реваскуляризацию. Прямая реваскуляризация заключается в наложении сосудистого анастомоза между экстра и интракраниальными сосудами. Как правило, используется ветвь наружной сонной артерии (обычно поверхностная височная артерия)

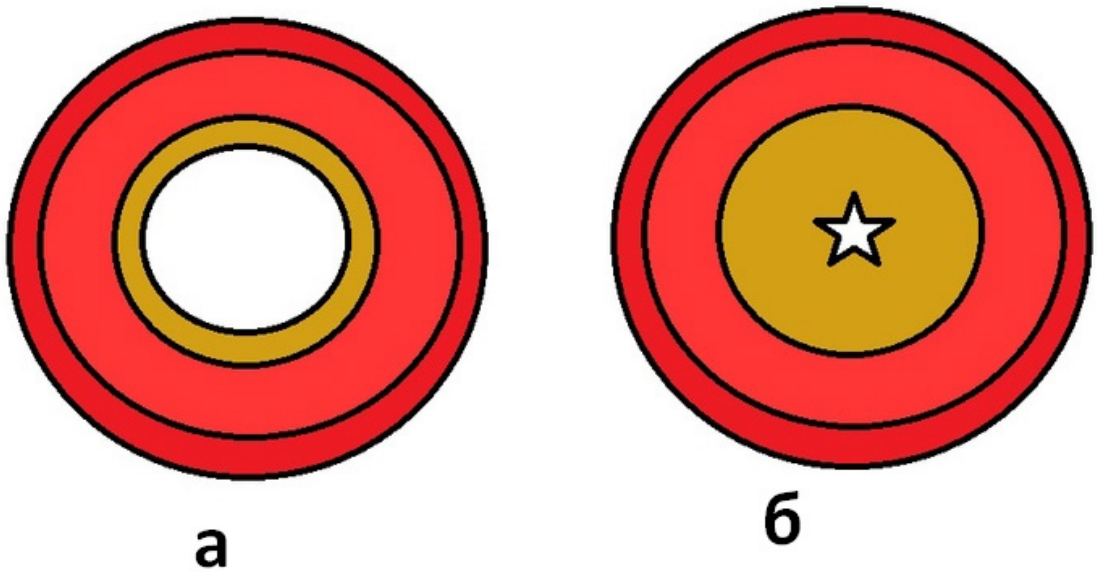


Рис. 1. **Изменение стенок сосудов при болезни мойя-мойя: а — нормальная стенка, б — пораженный сосуд**

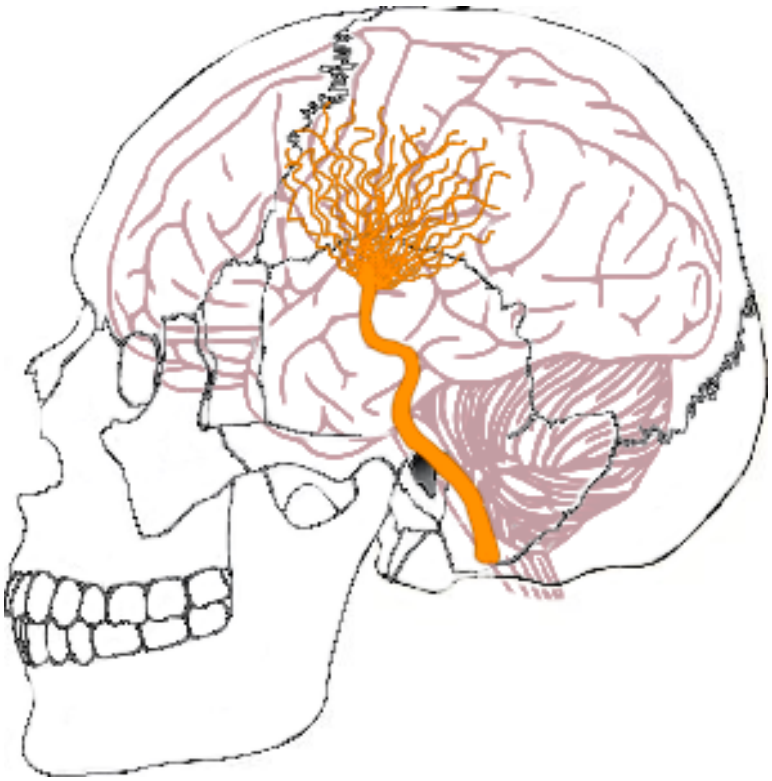


Рис. 2. **Характерный вид при церебральной ангиографии пациента с болезнью мойя-мойя 2-3 стадий болезни**

к внутренней сонной артерии или более дистальной ветви (среднемозговой артерии). Непрямой метод реваскуляризации включает в себя размещение трансплантата на васкуляризированной ножке (такой трансплантат способен к артериогенезу) на поверхности мозга [11].

Подводя итог необходимо отметить, что несмотря на небольшую распространенность в популяции, болезнь мойя-мойя является серьезной проблемой для здравоохранения, так как часто приводит к инвалидизации пациентов и значительному ухудшению качества их жизни. Не забывая принцип «Частое — часто, редкое — редко», специалисты, занимающиеся цереброваскулярными заболеваниями должны иметь настороженность по диагностике болезни мойя-мойя.

Литература:

1. Baba T, Houkin K, Kuroda S. Novel epidemiological features of moyamoya disease. J Neurol Neurosurg Psychiatry 2008; 79:900-4
2. Scott RM, Smith JL, Robertson RL, Madsen JR, Soriano SG, Rockoff MA. Long-term outcome in children with moyamoya syndrome after cranial revascularization by pial synangiosis. J Neurosurg 2004;100: Suppl:142-9
3. Uchino K, Johnston SC, Becker KJ, Tirschwell DL. Moyamoya disease in Washington State and California. Neurology 2005;65:956-8
4. Miki Fujimura, Oh Young Bang, Jong S Kim. Moyamoya Disease. Front Neurol Neurosci. 2016;40:204-220. doi:10.1159/000448314. Epub 2016 Dec 2.
5. Fukui M, Kono S, Sueishi K, Ikezaki K. Moyamoya disease. Neuropathology 2000;20: Suppl: S61-S64.
6. Guzman R, Lee M, Achrol A, et al. Clinical outcome after 450 revascularization procedures for moyamoya disease. J Neurosurg May 22, 2009
7. Irikura K, Miyasaka Y, Kurata A, et al. A source of haemorrhage in adult patients with moyamoya disease: the significance of tributaries from the choroidal artery. Acta Neurochir (Wien) 1996;138:1282 —
8. Seol HJ, Wang KC, Kim SK, Hwang YS, Kim KJ, Cho BK. Headache in pediatric moyamoya disease: review of 204 consecutive cases. J Neurosurg 2005;103: Suppl: 439-42.
9. Shuling Shang, Da Zhou, Jingyuan Ya, Sijie Li, Qi Yang, Yuchuan Ding, Xunming Ji, Ran Meng. Progress in moyamoya disease. Neurosurg Rev. 2020 Apr;43 (2):371-382. doi: 10.1007/s10143–018–0994-5. Epub 2018 Jun 18.
10. J U Choi, D S Kim, E Y Kim, K C Lee. Natural history of moyamoya disease: comparison of activity of daily living in surgery and non surgery groups. Clin Neurol Neurosurg. 1997 Oct;99 Suppl 2: S11–8. doi: 10.1016/s0303–8467 (97) 00033-4

11. Raphael Guzman, Gary K Steinberg. Direct bypass techniques for the treatment of pediatric moyamoya disease. Neurosurg Clin N Am. 2010 Jul;21 (3):565-73. doi: 10.1016/j. nec. 2010.03.013.
12. Suzuki J, Takaku A: Cerebrovascular «moyamoya» disease. Disease showing abnormal net-like vessels in base of brain. Arch Neurol 1969;20:288-299
13. Yamada I, Suzuki S, Matsushima Y: Moyamoya disease: Comparison of assessment with mr angiography and mr imaging versus conventional angiography. Radiology 1995;196:211-218.

Распространенность зубочелюстных аномалий и деформаций у детей и подростков в Российской Федерации

Михайлова Ангелина Сергеевна, студент;
Юдинцев Максим Александрович, студент
Чувашский государственный университет имени И. Н. Ульянова (г. Чебоксары)

Проведен обзор литературных источников, посвященных проблеме распространенности зубочелюстных аномалий и деформаций среди детей разного возраста в различных регионах Российской Федерации.

Ключевые слова: *распространенность, зубочелюстные аномалии и деформации, дети.*

Актуальность.

Зубочелюстные аномалии и деформации (ЗЧАД) являются одной из наиболее важных проблем современной стоматологии и характеризуются высокой распространенностью среди населения.

Зубочелюстные аномалии имеют полифакторное происхождение и характеризуются вариабельностью патогенетических механизмов их формирования и развития. При этом существуют основные эндогенные и экзогенные факторы риска. Следует отметить, что значительная часть этиологических факторов возникновения зубочелюстных аномалий являются управляемыми и при своевременном устранении и ослаблении их влияния предупреждают формирование нарушений зубочелюстных и скелетных структур. К данной группе этиологических факторов относятся: раннее искусственное вскармливание, постоянное использование сосок-пустышек, нарушения функции дыхания, глотания, жевания и речи. Также в эту группу можно отнести вредные привычки, такие как сосание пальцев, языка, губ, ротовое дыхание и сосание предметов. При этом неуправляемые факторы риска связаны с наследственно-обусловленными патологиями, состоянием здоровья матери и ребенка в период беременности, токсикозом беременных, патологическими состояниями беременных, обусловленными угрозой прерывания беременности, анемией, тяжелыми родами (преждевременные и переношенные роды). Кроме того, влияют такие факторы как родовые травмы, патологические состояния новорожденных, обусловленные асфиксией и гемолитической болезнью, болезни раннего детского возраста, а также инфекционные, аллергические и общесоматические заболевания детей [25].

При этом ЗЧАД приводят к нарушению функций жевания и речи, а также являются значимым фактором риска развития кариеса; заболеваний пародонта и слизистой оболочки полости рта, болезней височно-нижнечелюстного сустава; ЛОР-органов; органов пищеварительной системы [11, 17, 23, 24]. Описано отрицательное влияние ЗЧАД на развитие костно-мышечной системы у детей [25]. Безусловно, своевременное выявление и рациональная коррекция ЗЧАД у детей способно внести существенный вклад в сохранение и укрепление их здоровья, а также являются приоритетной задачей детской стоматологии.

В достижении этой задачи существенную роль играет грамотная организация диагностического и лечебного процесса в лечебно-профилактических учреждениях различного уровня. При этом изучение распространенности ЗЧАД среди детей различного возраста помогает разрешить следующие организационные вопросы: выявление потребности и расчёт необходимого числа врачей-ортодонтов, организация сети ортодонтических отделений и кабинетов, планирование лечебно-профилактических мероприятий.

Цель исследования — изучить распространенность зубочелюстных аномалий и деформаций среди детей различных возрастных групп на территории Российской Федерации.

Материалы и методы. Проведен анализ 26 литературных источников, посвященных проблеме распространенности зубочелюстных аномалий и деформаций среди детей разного возраста в различных регионах Российской Федерации.

Результаты исследования и их обсуждение. По данным различных исследователей распространенность зубочелюстных аномалий среди детей в возрасте от 3 до 18 лет варьируется в пределах от 37,27±5,21% до 89±1,3%. При этом некоторые авторы считают, что частота ЗЧАД выше у до-

школьников, хотя большинство отмечают их увеличение с возрастом.

С. Н. Лебедев при изучении распространенности ЗЧАД среди детей коренного населения Ханты-Мансийского автономного округа — Югры, обследовав 251 учащегося в возрасте 12 лет и 227 учащихся в возрасте 15 лет установил, что распространенность ЗЧАД среди детей 12 лет составляет 32,06%, а в возрасте 15 лет — 42,84% [1].

По данным А. М. Атоевой, полученным после обследования 2248 детей Карачаево-Черкесской Республики в возрасте от 6 до 14 лет: 520 детей, проживающих в Черкесске (252 мальчика и 268 девочек) и 530 детей из г. Врасновосточный (263 мальчика и 267 девочек) распространенность ЗЧАД составила 48,46% среди лиц мужского пола и 51,54% среди лиц женского пола [5].

В Волгоградской области, по данным Я. П. Боловина распространенность ЗЧАД среди детей от 3 до 6 лет составляет 64,86%, а в возрасте от 6 до 14 лет распространенность данной патологии составила 44,4-50,5% [6].

Изучив распространенность ЗЧАД в Белгородской области В. С. Мельник указывает на то, что среди детей в возрасте от 8 до 15 лет распространенность ЗЧАД составляет 77,19±3,24% и характеризуется возрастной уровень вариабельностью. Самый низкий уровень частоты ЗЧАД характерен для периода сменного прикуса [7].

Распространенность ЗЧАД в Троицком и Новомосковском АО г. Москвы, по данным А. Г. Арзуманяна, составляет 76,5%. При этом было исследовано 502 ребенка в трех возрастных периодах: 187 детей в возрасте 6-9 лет, 207 детей в возрасте 10-13 лет и 108 детей возрастной категории 14-16 лет. В первой возрастной группе распространенность ЗЧАД составила 81,3%; во второй группе — 45,9%: в третьей группе — 24,1% [8].

И. С. Мохамад и В. М. Водолацкий проведя клиническое обследование 718 учеников средних школ г. Ставрополя выявили, что 61,55% из них имели ЗЧАД различной степени выраженности [9].

В г. Симферополь, по данным Колесник К. А. и Каблова О. В., изучившим состояние ЗЧС 3112 детей в возрасте от 8 до 15 лет, ЗЧАД выявили в 63,05% случаях [10].

В результате проведенного А. В. Лосевым исследования детей и подростков Республики Алтай в возрасте 5-17 лет было выявлено, что распространенность зубочелюстных аномалий различна в изучаемых группах и составила: северные европеоиды — 64,3±3,0%; северные алтайцы — 69,8±2,7%; метисы — 86,1±2,2% [11].

Проведенный Фирсовой И. В. с соавт. анализ встречаемости различных видов зубочелюстных аномалий среди детей от 3 до 18 лет в Саратовской области выявил, что доля лиц с зубочелюстными аномалиями среди обследованных достигает 44,5% [12].

При проведении ситуационного анализа в городах Тюменской области — региона с нефтехимической промышленностью — Матвеевым Р. С. с соавт. был изучен стоматологический статус 5743 детей (2945 мальчиков и 2798 девочек) в возрасте от 6 до 16 лет. Распространенность ЗЧАД у детей (6-16 лет), проживающих на изучаемой территории, оказалась наиболее высокой в Тюмени — 89±1,3% [13].

При обследовании детей 3-6 лет г. Воронеж выявлена высокая распространенность зубочелюстных аномалий и деформаций — 81,88%, в 30,1% случаев обследованные дошкольники нуждались в протезировании [14].

В Республике Татарстан, по данным А. Н. Галлиулина, проводившего исследование среди 1562 воспитанников дошкольных учреждений г. Казани, распространенность зубочелюстных аномалий и деформаций среди детей в возрасте от 8 месяцев до 3 лет составляет 71±1,4% [24].

Сопоставив современные данные о распространенности ЗЧАД с данными эпидемиологического исследования, проведенного в 80-90-х годах прошлого столетия [3, 21, 22], можно сделать вывод о сохранении высокого уровня распространенности на протяжении нескольких десятилетий, а в некоторых регионах и неуклонный рост этого показателя.

Вместе с тем сопоставимость показателей распространенности зубочелюстных аномалий может быть достигнуто при строгом соблюдении принципов возрастной группировки обследуемых контингентов, одинаковом методическом подходе к оценке состояния зубов, зубных рядов и прикуса на основе единой классификации, с учетом этнических особенностей строения лица и отдельных его частей.

Выводы и практические рекомендации. Обобщив множество исследований, можно сделать вывод о высокой распространенности ЗЧАД на территории Российской Федерации. При этом анализ литературы свидетельствует об отсутствии снижения распространенности ЗЧАД в последние десятилетия.

Таким образом, проведение эпидемиологических исследований с целью выявления распространенности ЗЧАД у детей в различных регионах России имеет большое значение для планирования и разработки комплексных программ профилактики зубочелюстных аномалий с учетом регионального компонента и требует унификации методов возрастной группировки и диагностики на основе единой классификации.

Литература:

1. Лебедев Сергей Николаевич, Галимуллина Валерия Радиславовна, Нагаева Марина Олеговна, Тимофеева Юлия Егоровна Распространенность и структура зубочелюстных аномалий у подростков коренного малочисленного населения Ханты-Мансийского автономного округа — Югры // Проблемы стоматологии. 2019. № 1.
2. Суслова, О. В., Желизняк Н. А., Стеценко Д. В., Кордонец Е. Л., Анисимов М. В. Аномалии зубных рядов в структуре зубочелюстных аномалий у детей 7-18 лет // Вестник стоматологии. 2019. № 1 (106).

3. Олесов Егор Евгеньевич, Каганова Олеся Сергеевна, Фазылова Татьяна Александровна, Миргазизов Марсель Закеевич, Ильин Александр Александрович, Шугайлов Игорь Александрович Динамика структуры и тяжести зубочелюстных аномалий на фоне раннего ортодонтического лечения в период сменного прикуса // Клиническая практика. 2019. № 3.
4. Ганжа Ирина Ремовна, Постников М. А., Модина Т. Н. Планирование лечения и профилактики слизисто-десневых осложнений на этапах ортодонтической реабилитации // ТМЖ. 2020. № 2 (80).
5. Атоева Максад Амоновна, Собиров Шухрат Солижонович Взаимообусловленность частоты зубочелюстных аномалий у детей, проживающих в различных экологических условиях и оказания им профилактической помощи // Биология и интегративная медицина. 2020.
6. Боловина, Я. П., Вологина М. В., Фиталь Э. А., Боловина А. Д. Проблема комплаентности ортодонтических пациентов в Волгоградской области // Вестник ВолГМУ. 2019. № 2 (70).
7. Мельник, В. С., Горзов Л. Ф. Распространенность и структура зубочелюстных аномалий у детей и подростков районных центров Закарпатья // Вестник стоматологии. 2019. № 3 (108).
8. Арзуманян, А. Г., Фомина А. В. Анализ распространенности и структуры зубочелюстных аномалий среди детей школьного возраста // ВНМТ. 2019. № 3.
9. И. С. Мохамад, В. М. Водолацкий Распространенность зубочелюстных аномалий и деформаций у детей и подростков // Вестник новых медицинских технологий. Электронное издание. 2020.
10. Колесник, К. А., Каблова О. В. Частота и характеристика сверхкомплектных зубов у пациентов стоматологических клиник г. Симферополя (ретроспективный анализ) // Вятский медицинский вестник. 2021. № 1 (69).
11. Лосев, А. В. Изучение влияния изменения генетического состава популяции на распространенность зубочелюстных аномалий [Текст]/А. В. Лосев // Материалы XXI и XXII Всероссийских научно-практических конференций. — М., 2009. — с. 52-53.
12. Фирсова, И. В. Показатели стоматологического здоровья у детей и подростков Саратова и Саратовской области/И. В. Фирсова, Д. Е. Суетенков, А. В. Егорова, Т. Е. Магомедов, Т. П. Харитонова, Н. В. Давыдова, С. И. Лебедева, Э. А. Бахметьева, Е. А. Гриценко // Саратовский научно-медицинский журнал. — Vol. 9. — Issue 3. — 2013. — с. 484-486
13. Матвеев, Р. С. Алгоритм пренатальной профилактики зубочелюстных аномалий у детей, проживающих в регионе с неблагоприятными экологическими факторами/Р. С. Матвеев, Ю. Н. Белоусов, Ж. К. Есингалеева, А. В. Глотова //Здравоохранение Чувашии. — 2015. — № 2. — с. 37-40
14. Ипполитов, Ю. А. Оценка эпидемиологической картины зубочелюстных аномалий и деформаций у детей дошкольного возраста с ранней потерей временных зубов/Ю. А. Ипполитов, М. М. Татринцев, М. Э. Коваленко, Е. Ю. Золотарева, Н. А. Анисимова, М. В. Леонов // Вестник новых медицинских технологий. — 2013. — № 1. — с. 80-83.
15. Суслова, О. В., Желизняк Н. А., Стеценко Д. В., Кордонец Е. Л., Анисимов М. В. Аномалии зубных рядов в структуре зубочелюстных аномалий у детей 7-18 лет // Вестник стоматологии. 2019. № 1 (106).
16. Олесов Егор Евгеньевич, Каганова Олеся Сергеевна, Фазылова Татьяна Александровна, Миргазизов Марсель Закеевич, Ильин Александр Александрович, Шугайлов Игорь Александрович Динамика структуры и тяжести зубочелюстных аномалий на фоне раннего ортодонтического лечения в период сменного прикуса // Клиническая практика. 2019. № 3.
17. Ганжа Ирина Ремовна, Постников М. А., Модина Т. Н. Планирование лечения и профилактики слизисто-десневых осложнений на этапах ортодонтической реабилитации // ТМЖ. 2020. № 2 (80).
18. Ефимова Евгения Юрьевна, Краюшкин А. И., Ефимов Ю. В. Взаимосвязи показателей ширины зубных дуг верхней челюсти с некоторыми линейными параметрами лицевого отдела черепа при мезокранном типе его строения // ТМЖ. 2019. № 1 (75).
19. Зубарева Анна Владимировна, Гараева Карина Линаровна, Исаева Адель Ильгизовна Распространенность зубочелюстных аномалий у детей и подростков (обзор литературы) // European research. 2015. № 10 (11).
20. Козлов, Д. С. Изучение распространенности зубочелюстных аномалий и деформаций среди детей школьного возраста. Мониторинг проведенного ортодонтического лечения и анализ его эффективности: автореф. дис…. канд. мед. наук. — Воронеж, 2009. — 24 с.
21. Лавриков, В. Г. Распространенность зубочелюстных деформаций и дефектов зубных рядов у детей г. Белгорода и Белгородской области/В. Г. Лавриков, В. В. Беляев, Т. М. Бакерникова, О. Л. Саламатина // Технологии XXI века в стоматологии и челюстно-лицевой хирургии: материалы науч.-практич. конф. стоматологов и челюстно-лицевых хирургов ЦФО РФ с международным участием. — Тверь, 2008. — с. 215216.
22. Осетрова, Т. С. Обоснование мер по совершенствованию ортодонтической помощи детям на региональном уровне: автореф. дис…. канд. мед. наук. — Хабаровск, 2009-24 с.

23. Ешиев Данияр Абдыракманович Классификатор зубочелюстно-лицевых аномалий // Наука, образование и культура. 2019. № 10 (44).
24. Галиуллин, А. Н., Хадыева М. Н., Хусаинова Г. А. Распространенность зубочелюстных аномалий у детей дошкольного возраста в крупном мегаполисе // Современные проблемы науки и образования. — 2018. — № 6.
25. Попова Елена Святославовна, Кухаренко Юлия Викторовна, Смоляков Сергей Николаевич Изменение гемодинамики в патогенезе заболеваний пародонта у детей с зубочелюстными аномалиями в условиях Забайкалья // Российский стоматологический журнал. 2013. № 2.
26. Ушницкий, И. Д., Алексеева Т. В., Пинелис И. С., Юркевич А. В., Михальченко Д. В., Давыдов И. Е. Этиологические факторы и патогенетические механизмы формирования и развития деформаций зубочелюстной системы // Дальневосточный медицинский журнал. 2019. № 2.

Ведущие факторы риска развития инсульта

Расулова Дилбар Камалиддиновна, кандидат медицинских наук, доцент;
Рахматуллаева Гульнора Кутбиддиновна, кандидат медицинских наук, доцент;
Рустамова Мафтуна Абдуманнап кизи, студент магистратуры
Ташкентская медицинская академия (Узбекистан)

В статье дан анализ результатов научных исследований по вопросам ведущих факторов риска, способствующих развитию инсульта.

Ключевые слова: *инсульт, факторы риска, заболеваемость, инвалидизация, смертность, артериальная гипертензия.*

В последние годы отмечается рост заболеваемости инсультом, особенно среди лиц молодого возраста. Цереброваскулярные заболевания занимают второе место в структуре смертности и первое место в структуре первичной инвалидизации. При этом доля ишемических инсультов в популяции составляет 80%, из них 11-15% случаев случаются у лиц молодого возраста. В связи с увеличением и омоложением инсульта, он приобретает особое медицинское, социальное и экономическое значение [1,2,7,8,10,12]. В Узбекистане число больных с инсультом также имеет тенденцию к увеличению — ежегодно регистрируется порядка 40-45 тысяч случаев мозгового инсульта [,,,,,]. В большинстве случаев (80%) пациенты, перенесшие инсульт, стойко утрачивают трудоспособность и лишь 10,2% выживших больных возвращаются к трудовой деятельности. Во всем мире к 2030 г. прогнозируется рост смертности от инсульта до 7,8 млн. человек в год, в случае если не будет предпринято активных глобальных мер по борьбе с этой патологией. При этом примерно у 1/3 пациентов не представляется возможным установить причину развития инсульта и ведущие факторы риска [3,4,5,6,8,10,11].

Цель исследования: на основе анализа проведенных исследований определить наиболее значимые факторы риска, способствующие развитию цереброваскулярной и кардиоваскулярной патологии.

Материал и методы исследования: Материалом исследования были монографии, диссертации, журнальные статьи и тезисы, опубликованные в материалах научно-практических конференций. Были использованы исторический, аналитический и выкопировочный методы.

Результаты исследования: Проведенные в течение последних десятилетий многочисленные исследования позволили идентифицировать и обосновать роль различных факторов риска в развитии цереброваскулярной и кардиоваскулярной патологии. Сегодня не вызывает сомнения значимость таких базисных факторов, как артериальная гипертензия, атеросклероз пре- и интрацеребральных сосудов, дислипидемия, сахарный диабет [10,11,12,18,20].

По данным различных исследований, лишь менее десятой части пациентов, перенесших инсульт, могут вернуться к прежней работе, почти треть — нуждаются в посторонней помощи в повседневной жизни. Увеличение процента выживших с тяжелыми неврологическими нарушениями определяет необходимость активного совершенствования процесса и улучшения результата медико-социальной реабилитации больных в восстановительный период заболевания [9,13,16,17].

В течение последних лет в мировой неврологической практике сформировалась тенденция к индивидуализации подходов к коррекции факторов риска. На сегодняшний день разработаны ряд программ и протоколов по коррекции базисных факторов риска, включающие рекомендации по модификации образа жизни и применению лекарственных средств. Все это позволило добиться определенного снижения случаев цереброваскулярной патологии. Тем не менее до 25% случаев инсульта связано с воздействием новых факторов риска, особенно у лиц молодого возраста.

Все более актуальной становится проблема сосудистых заболеваний в молодом возрасте, когда действие базисных факторов менее значимо. Обнаруженные новые

факторы риска в сочетании с базисными факторами дают основание клиницисту (неврологу, терапевту, семейному врачу) выявить у пациента индивидуальные факторы риска и разработать эффективную программу как первичной, так и вторичной профилактики цереброваскулярной патологии [4,6,8,14,17].

По данным ряда исследований в настоящее время отмечается рост заболеваемости инсультом у лиц молодого возраста. При этом примерно у 1/3 пациентов не представляется возможным установить причину развития инсульта и ведущие факторы риска. Исследование под эгидой ВОЗ MONICA показало, что действием лишь общеизвестных, базисных факторов риска невозможно полностью объяснить развитие цереброваскулярной патологии [7,11,13,18,19,20].

Другой актуальной проблемой является возрастающая роль немых инфарктов мозга, которые являются предиктором последующих нарушений мозгового кровообращения с формированием стойкого неврологического дефицита. В последнее время появилась и другая проблема в неврологии — возрастающая роль ятрогенных инсультов как следствие назначения терапии при не до конца верифицированных факторах риска. К настоящему времени выявлено более 50 новых потенциальных факторов риска развития инсульта. При этом можно выделить ряд факторов, обладающих наибольшим потенциалом и доказательной базой. К таким факторам относится генетическая предрасположенность, т. е. наличие семейных случаев острых нарушений мозгового кровообращения (ОНМК). Сегодня уже не вызывает сомнения влияние на риск развития инсульта таких факторов, как фибрилляция предсердий, патология клапанов, ишемическая болезнь сердца (ИБС). Вместе с тем полученные в последнее время данные свидетельствуют о возрастающей роли новых кардиогенных факторов риска, особенно у лиц молодого возраста. К таким факторам относят аномалии развития (открытое овальное окно — ООО, аневризма межпредсердной перегородки, сеть Киари в правом предсердии, евстахиев клапан в правом предсердии, дисплазия правого желудочка), кардиомиопатии, нарушения ритма сердца (WPW-синдром, синдром слабости синусового узла) и др. Анализ данных литературы показывает, что ишемические нарушения мозгового кровообращения обусловлены парадоксальной кардиальной эмболией, сопряжены с риском повторных эмболий. наиболее частой причиной развития внутримозговых кровоизлияний являются артериовенозные мальформации [3,4,5,6,8,14,16,17,20].

Многочисленные клинические исследования показали, что прием пероральных контрацептивов, особенно в сочетании с курением, является существенным фактором риска развития инсульта у женщин молодого возраста, что связано с повышением свертываемости крови в результате действия эстрогенов на синтез факторов свертывания. У определенной категории женщин фактором риска инсульта может быть и беременность. Доказано, что при беременности увеличивается нагрузка на правые отделы сердца, а также возрастает риск тромбоза вен нижних конечностей и таза. Независимыми факторами риска инсульта являются преэклампсия и гестационная гипергликемия.

Многие пациенты имеют сопутствующие заболевания, которые увеличивают риск повторного инсульта и снижают возможность больного участвовать в активной реабилитации. Исследования частоты сопутствующих заболеваний у больных, перенесших инсульт, показали, что у больных с инсультом значительно чаще встречаются артериальная гипертония, коронарная патология, ожирение, сахарный диабет, артриты, гипертрофия левого желудочка и сердечная недостаточность [8,9,11,12].

Таким образом, проведенный далеко не полный анализ литературных источников позволил сделать вывод, что изучение факторов риска развития инсульта даст возможность проводить глобальную, а также персонифицированную профилактику данных заболеваний и повысить её эффективность.

Литература:

1. Боголепова, О. Н. Современные подходы к диагностике и лечению сосудистой деменции/О. Н. Боголепова// Эффективная фармакотерапия. — 2013. — № 2. — С 12-17.
2. Бойцов, С. А. Смертность и факторы риска развития неинфекционных заболеваний в России: особенности, динамика, прогноз/С. А. Бойцов, А. Д. Деев, С. А. Шальнова// Терапевтический архив. — 2017. — N 1. — с. 5-13.
3. Бочеев, А. П. Факторы риска и ранние проявления заболеваний нервной системы на современном этапе (обзор литературы)/А. П. Бочеев, Е. С. Кипарисова// Клиническая неврология. — 2015. — N 2. — с. 36-39.
4. Захарова, Е. М. Современные представления о цереброваскулярных заболеваниях/Е. М. Захарова // Медицинский альманах. — 2010. — № 2. — с. 42-47.
5. Кулеш, С. Д. Пятилетняя выживаемость после мозгового инсульта/С. Д. Кулеш, С. А. Лихачев, Н. А. Филина // Анналы клинической и экспериментальной неврологии. — 2012. — Т. 6 — № 1. — с. 14-19.
6. Петрухин, И. С. Контроль поведенческих факторов риска — основа профилактики сердечно-сосудистых и других неинфекционных заболеваний/И. С. Петрухин, И. А. Эльгардт, Е. А. Низова. — Тверь: Тверской печатный двор, 2010. — 180 с.
7. Прилепская, О. А., Дубровина О. А. Инсульт у лиц молодого возраста: Все ли мы знаем? // Университетская медицина Урала. — 2016. — Т. 2. — №. 1. — с. 75-79.

8. Профилактика и факторы риска ОНМК (обзор литературы)/Е. Н. Карпова [и др.]// Клиническая неврология. — 2015. — N 2. — с. 31-35.
9. Реабилитация больных, перенесших инсульт/В. А. Епифанов, А. В. Епифанов, О. С. Левин. — 4-е изд. — М.: МЕДпресс-информ, 2014. — 248 с.
10. Фазлиахметова, А. Г. Эпидемиология и факторы риска ишемического инсульта у молодых// А. Г. Фазлиахметова, Э. И. Богданов//Неврологический вестник. — 2016. — N 3. — с. 77-81.
11. Факторы риска цереброваскулярных заболеваний в нейрогериатрии/Л. В. Новикова [и др.] // Фарматека. — 2017. — N 9 — с. 61-64
12. Хайдаров, Н. К. Организационные аспекты совершенствования медицинской реабилитации больных с острыми нарушениями мозгового кровообращения. //дис. … докт. мед. наук. — М., 2019. — 312 с.
13. Чемакин, Н. Ю. Этиологические аспекты инсульта в молодом возрасте с разбором клинического случая/Н. Ю. Чемакин // Университетская медицина Урала. — 2019. — № 2. — с. 43-44.
14. European Stroke Organisation (ESO) guidelines for the management of spontaneous intracerebral hemorrhage/T. Steiner [et al.] // Int J Stroke — 2014. — Vol. 9 — № 7 — P. 840–855c
15. Guidelines for the Management of Aneurysmal Subarachnoid Hemorrhage: A Guideline for Healthcare Professionals From the American Heart Association/American Stroke Association/E. S. Connolly [et al.] // Stroke — 2012. — Vol. 43 — № 6-1711–1737c.
16. Micieli, G. Guideline compliance improves stroke outcome: a preliminary study in 4 districts in the Italian region of Lombardia/G. Micieli, A. Cavallini, S. Quaglini // Stroke — 2002. — Vol. 33 — № 5 — P. 1341–1347c.
17. Pan, An. Depression and risk of stroke morbidity and mortality. A meta-analysis and systematic review/An. Pan [et al.] // JAMA. — 2011. — Vol. 306 (11). — P. 1241-1249.
18. Pre-existing hypertension and the impact of stroke on cognitive function/J. S. Elkins [et al.] // Ann Neurol. — 2005. — Vol. 58. — P. 68-74. Primary prevention of ischemic stroke: A statement for healthcare professionals from the Stroke Council of the American Heart Association/L. B. Goldstein [et al.] // Stroke. — 2001. — Vol. 32. — P. 280-299
19. Quality of ischemic stroke care in emerging countries: the Argentinian National Stroke Registry (ReNACer)/L. A. Sposato [et al.] // Stroke — 2008. — Vol. 39 — № 11 — P. 3036–3041c
20. Risk factors for ischaemic and intracerebral haemorrhagic stroke in 22 countries (the INTERSTROKE study): a case-control study./M. J. O»Donnell [et al.] // Lancet — 2010. — T. 376 — № 9735 — P. 112-123.

Молодой ученый

Международный научный журнал

№ 21 (363) / 2021

Выпускающий редактор Г. А. Кайнова

Ответственные редакторы Е. И. Осянина, О. А. Шульга, З. А. Огурцова

Художник Е. А. Шишков

Подготовка оригинал-макета П. Я. Бурьянов, М. В. Голубцов, О. В. Майер

Журнал размещается и индексируется на портале eLIBRARY.RU, на момент выхода номера в свет журнал не входит в РИНЦ.

Свидетельство о регистрации СМИ ПИ №ФС77-38059 от 11 ноября 2009 г. выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)

ISSN-L 2072-0297

ISSN 2077-8295 (Online)

Учредитель и издатель: ООО «Издательство Молодой ученый»

Номер подписан в печать 02.06.2021. Дата выхода в свет: 09.06.2021.

Формат 60×90/8. Тираж 500 экз. Цена свободная.

Почтовый адрес редакции: 420126, г. Казань, ул. Амирхана, 10а, а/я 231.

Фактический адрес редакции: 420029, г. Казань, ул. Академика Кирпичникова, д. 25.

E-mail: info@moluch.ru; https://moluch.ru/

Отпечатано в типографии издательства «Молодой ученый», г. Казань, ул. Академика Кирпичникова, д. 25.