АКТУАЛЬНЫЕ ИССЛЕДОВАНИЯ

МЕЖДУНАРОДНЫЙ НАУЧНЫЙ ЖУРНАЛ

ISSN 2713-1513

#51 (286), 2025

ЧАСТЬ I

Актуальные исследования

Международный научный журнал
2025 • № 51 (286)
Часть I

Издается с ноября 2019 года Выходит еженедельно

ISSN 2713-1513

РЕДАКЦИОННАЯ КОЛЛЕГИЯ

Кузнецов Игорь Анатольевич, кандидат медицинских наук, доцент, академик международной академии фундаментального образования (МАФО), доктор медицинских наук РАГПН, профессор, почетный доктор наук РАЕ, член-корр. Российской академии медико-технических наук (РАМТН) (Астраханский государственный технический университет)

Литвинова Жанна Борисовна, кандидат педагогических наук (Кубанский государственный университет)

Мамедова Наталья Александровна, кандидат экономических наук, доцент (Российский экономический университет им. Г.В. Плеханова)

Мукий Юлия Викторовна, кандидат биологических наук, доцент (Санкт-Петербургская академия ветеринарной медицины)

Никова Марина Александровна, кандидат социологических наук, доцент (Московский государственный областной университет (МГОУ))

Насакаева Бакыт Ермекбайкызы, кандидат экономических наук, доцент, член экспертного Совета МОН РК (Карагандинский государственный технический университет)

Олешкевич Кирилл Игоревич, кандидат педагогических наук, доцент (Московский государственный институт культуры)

Попов Дмитрий Владимирович, доктор филологических наук (DSc), доцент (Андижанский государственный институт иностранных языков)

Пятаева Ольга Алексеевна, кандидат экономических наук, доцент (Российская государственная академия интеллектуальной собственности)

Редкоус Владимир Михайлович, доктор юридических наук, профессор (Институт государства и права РАН)

Самович Александр Леонидович, доктор исторических наук, доцент (ОО «Белорусское общество архивистов»)

Сидикова Тахира Далиевна, PhD, доцент (Ташкентский государственный транспортный университет)

Таджибоев Шарифджон Гайбуллоевич, кандидат филологических наук, доцент (Худжандский государственный университет им. академика Бободжона Гафурова)

Тихомирова Евгения Ивановна, доктор педагогических наук, профессор, Почётный работник ВПО РФ, академик МААН, академик РАЕ (Самарский государственный социально-педагогический университет)

Хаитова Олмахон Саидовна, кандидат исторических наук, доцент, Почетный академик Академии наук «Турон» (Навоийский государственный горный институт)

Цуриков Александр Николаевич, кандидат технических наук, доцент (Ростовский государственный университет путей сообщения (РГУПС)

Чернышев Виктор Петрович, кандидат педагогических наук, профессор, Заслуженный тренер РФ (Тихоокеанский государственный университет)

Шаповал Жанна Александровна, кандидат социологических наук, доцент (Белгородский государственный национальный исследовательский университет)

Шошин Сергей Владимирович, кандидат юридических наук, доцент (Саратовский национальный исследовательский государственный университет имени Н.Г. Чернышевского)

Эшонкулова Нуржахон Абдужабборовна, PhD по философским наукам, доцент (Навоийский государственный горный институт)

Яхшиева Зухра Зиятовна, доктор химических наук, доцент (Джиззакский государственный педагогический институт)

СОДЕРЖАНИЕ

ФИЗИКА

НЕФТЯНАЯ ПРОМЫШЛЕННОСТЬ

ТЕХНИЧЕСКИЕ НАУКИ

ВОЕННОЕ ДЕЛО

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

АРХИТЕКТУРА, СТРОИТЕЛЬСТВО

ФИЗИКА

РЯЗАНОВ Николай Данилович
директор, ООО «Импульсные комплексные технологии»,
Россия, г. Томск

РЕАЛЬНАЯ ГИПОТЕЗА ЗАРОЖДЕНИЯ И РАЗВИТИЯ ГРОЗОВОЙ МОЛНИИ

Аннотация. *В статье на основании последних научных достижений в области изучения возникновения и развития грозовой молнии представлена наиболее реальная картина зарождения и развития грозовой молнии.*

Ключевые слова: *напряжённость электрического поля, рентгеновское и гамма-излучения, радиоизлучение, стример, лидер, молния, «поджигающий» разряд.*

На данный момент изучению формирования и развития молнии посвящено огромное количество работ, в которых рассмотрены процессы начиная от зарождения электрических зарядов в облаках кончая формированием грозового разряда – молнии. Процесс зарождения молнии остаётся одной из наиболее важных, нерешенных задач физики атмосферного электричества.

Для объяснения процесса возникновения молниевого разряда в разное время было предложено несколько концепций. Одной из первых гипотез образования молний является теория, разработанная учёными под руководством Александра Гуревича, в которой молнии рождаются под влиянием высокоэнергетических частиц космического излучения 10^{16}ev [1, с. 1177-1199; 2, с. 452-456]. Однако теория возникновения молний, связанная с космическим излучением сверхвысоких энергий не нашла поддержки в научном сообществе из-за её несостоятельности.

В 1991 году Норвежские учёные открыли «тёмную молнию» [3, с. 8]. Авторы работы утверждают, что гамма-лучи возникают в результате взаимодействия молекул воздуха с электронами, которые двигаются со скоростью, близкую к скорости света. В результате их столкновения с молекулами воздуха возникает гамма-излучение, которое вызывает мощный радиоимпульс. Далее в грозовом облаке возникает электрический разряд – молния. Практическое подтверждение существования «тёмных молний» было опубликовано в работе [4, с. 47-49], в которой экспериментально был доказан механизм образования «тёмной молнии».

Наиболее признанной на сегодняшний день моделью возникновения гамма-вспышек в грозовых облаках является «Релятивистская модель разряда с обратной связью» американского ученого Джозефа Дуайера, выдвинутая им в 2003 году [5]. В грозовом электрическом поле есть электроны, летящие со скоростью света. Сталкиваясь с атомами воздуха, они выбивают новые электроны, и таким образом их количество увеличивается. Один электрон рождает тысячи, получается лавина. Согласно модели, предложенной американским ученым, взаимодействуя с молекулами воздуха, электроны порождают тормозное гамма-излучение, которое позволяет высвободиться позитронам. Они положительно заряжены и движутся в обратную сторону относительно лавины электронов. Позитроны, в свою очередь, также сталкиваются с молекулами воздуха и также выбивают из них электроны, порождая новые лавины. Таким образом реализуется позитронная обратная связь.

В работе [6] в результате многочисленных измерений установлено, что «радиоизлучение каждой молнии начинается с очень короткого биполярного импульса с длительностью первого пика порядка 100 ns. Перед ним в течение, по крайней мере, 500 ms не регистрируется радиоизлучения, отличного от фонового. Форма,

ширина и амплитуда начального импульса согласуются со значениями, предсказываемыми теорией совместного действия пробоя на убегающих электронах и широкого атмосферного ливня (ШАЛ), инициированного первичной частицей с энергией порядка 10^{16} eV. С помощью фоторегистратора с временной развёрткой было детально изучено развитие разряда молнии от облака до земли. Разряд развивается лавинообразно, сначала в виде ионизованного канала, получившего название лидера молнии, который ступенчато продвигается от облака к земле. Скорость ступенчатого движения лидера к земле равна приблизительно $45 \cdot 10^6$ м/с, при чем интервал между ступенями составляет около 100 мкс. Длина каждой ступени лидера – около 45 м, так что полное время движения до земли может достигать 0,02 с. Затем по этому ионизованному каналу от земли к облаку движется основной разряд со скоростью от $2 \cdot 10^7$ м/с до $15 \cdot 10^7$ м/с. Был обнаружен мощный поток γ-излучения в период ≈ 100 μs перед возвратными ударами молний. Наблюдаемое излучение занимает обширную пространственную область».

Лю и Дуайер [7] предположили, что инициация молнии может начаться с множества мелкомасштабных разрядов, случайным образом возникающих между противоположно заряженными гидрометеорами в локализованной области грозового облака.

Юдин и соавторы [8] показали, как практически непроводящее грозовое облако засеивается областями повышенной ионной проводимости, пространственной протяжённостью 0,1–1 м и временем жизни 1–10 с. В работе показано, что электрическое поле на поверхности областей повышенной ионной проводимости в как минимум в 3 раза выше, чем у окружающей среды. Для максимального окружающего электрического поля 100 кВ/м, обычно измеряемого в грозовых облаках, такого усиления поля достаточно для инициации положительных стримеров и их распространения на расстояния порядка дециметров, и это будет происходить естественным образом, без каких-либо внешних агентов (например, сверхэнергетических частиц космических лучей). При условии, что каждая область повышенной ионной проводимости сгенерирует хотя бы один стример в течение своего жизненного цикла, стримеры сформируют 3D-сеть, некоторые части которой будут содержать сегменты горячих каналов, созданные за счёт кумулятивного нагрева и/или термоионизационной нестабильности. Эти же исследователи [9] впервые предложили теоретическую схему, поэтапно объясняющую процесс зарождения молний. Согласно ей, «мелкие кристаллы льда и капли воды в грозовых облаках – так называемые гидрометеоры – сталкиваясь, создают «всплески» электрического поля, которые генерируют большое количество разноимённо заряженных частиц – ионов. Если таких центров образования ионов в облаке много, и они возникают близко друг к другу, их общий электрический заряд постепенно накапливается и создаёт сильное электрическое поле, превышающее порог пробоя воздуха. Локальное усиление поля на дециметровых масштабах без каких-либо других внешних воздействий приводит к формированию стримеров – холодных слабопроводящих плазменных каналов. В дальнейшем разрозненные стримеры сливаются в более жизнеспособную трехмерную сеть, внутри которой в местах сосредоточения наибольших токов формируется «зародыш» молнии. Удлиняясь вдоль направления электрического поля, он превращается в полноценный молниевый канал».

В работе [10, с. 867-894] для объяснения процесса возникновения молниевого разряда учёные разработали численную модель, объясняющую механизм формирования молнии в грозовых облаках, в которой за счёт слияния множественных стримерных каналов в единую сеть возникает «зародыш» молнии даже при сравнительно слабых внутриоблачных электрических полях. Даже при слабом электрическом поле в облаке они могут формировать протяжённые проводящие кластеры. Когда длина такого кластера достигает критической величины – нескольких десятков метров – он становится зародышем молнии и способен развиваться дальше благодаря высокой поляризации. Для образования такой структуры необходимы два условия. Во-первых, стримеры должны появляться достаточно близко и почти одновременно, так как их существование ограничено долями миллисекунды. Во-вторых, рост каналов возможен только при достаточной напряжённости поля, которая возникает локально вследствие предыдущей разрядной активности.

При исследовании импульсного электрического разряда амплитудой до 6 МВ генерируемого генератором Маркса [11] был зафиксирован сверхширокополосный электромагнитный импульс, который возникал примерно за 1 мкс до того, как напряжение на высоковольтном электроде достигнет своего максимального значения, и может рассматриваться как новое физическое явление.

Анализируя все предложенные теории, используя новейшие достижения и расчёты ведущих учёных в области изучения молниевого разряда, то теорию его развития можно описать следующим образом. Грозовое облако представляет собой локализованную область с резко выраженной конвективной и электрической активностью [12]. Оно может состоять из одной или нескольких ячеек. Напряжённость электрического поля в таких облаках может достигать нескольких тысяч вольт на метр. Исследования показали, что на фоне относительно малых объёмных зарядов в облаке случайным образом располагаются отрицательные и положительные объёмные заряды высокой плотности. В среднем зоны экстремальных нагрузок имеют размеры от десяти до ста метров. Однако в грозовом облаке, особенно в стадии его развития, существуют сильные турбулентные потоки, которые создают существование хаотически расположенных по облаку зарядов, способные формировать значительные электрические поля, характерные для активных зон грозовых облаков. По мере развития облаков зоны неоднородностей становятся существенно больше, возрастая с 50–100 м до 200–400 м в стадии зрелости [13, с. 3-8]. Ракетные зондирования грозовых облаков [14; 15, с. 359-370] позволили уточнить раннее полученные результаты, значения величин напряжённости электрического поля, характерные для активной зоны грозовых облаков, и они оказались равными (100–200) кВ/м и более.

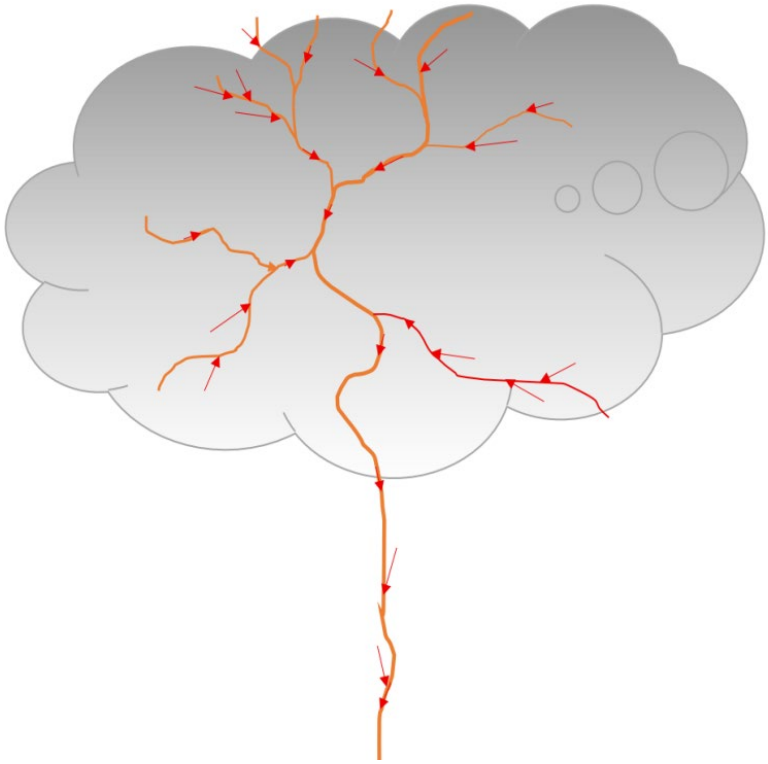

Рис. 1. Схема образования и развития грозовой молнии

Исследователи Д. И. Юдин и др. [16] впервые предложили теоретическую схему, поэтапно объясняющую процесс зарождения молний. «Согласно ей, мелкие кристаллы льда и капли воды в грозовых облаках – так называемые гидрометеоры – сталкиваясь, создают «всплески» электрического поля, которые генерируют большое количество разноименно заряженных частиц – ионов. Если таких центров образования ионов в облаке много, и они возникают близко друг к другу, их общий электрический заряд постепенно накапливается и создает сильное электрическое поле, превышающее порог пробоя воздуха. Возникает первичный

электрический разряд. Согласно открытию, опубликованным в работе [17, с. 46-51], при резком уменьшении радиуса электрода (в данном случае уменьшении площади заряженной области облака) происходит скачок напряжённости электрического поля:

$$\frac{dE}{dr} = k_1 \frac{U}{r_2^2} = \frac{10^2}{(1^{-5})^2} k_1 \approx 10^{12} \text{ В/м}, \quad (1)$$

При условии, что напряжение составляет 100 В, а радиус зарождения разряда 1 мкм, то возникающая при этом напряжённость достигает 10^{12} В/м. Под действием такой напряжённости происходит ионизация областей вокруг первичного разряда с последующим образованием стримера. Каждый образовавшийся стример порождает как минимум один, а то и больше новых стримеров. Объединяясь в замкнутую цепь, они создают все условия для образования лидера, при этом выполняются все моменты отражённые в работе [10, с. 867-894], а именно - стримеры появляются достаточно близко и почти одновременно, а рост каналов обеспечен достаточной напряжённостью поля, которая возникает локально вследствие предыдущей разрядной активности. Образовавшийся лидер (лидеры) ступенчато продвигается (продвигаются) от облака к земле, образуя ветвистую структуру разряда. Каждая ступень лидера излучает радиоимпульс, а при достижении определённой энергии разряда и достижения напряженности электрического поля более 10^{16} В/м, каждая последующая ступень порождает гамма-излучение. Впервые всплески рентгеновского излучения с энергиями в десятки мегаэлектронвольт были обнаружены в 1994 году обсерваторией Комптона, при изучении грозовой активности в атмосфере Земли [18, с. 1313-1316]. Эти излучения подтверждаются результатами работы [6], в которой экспериментально установлено, что грозовые облака изучают «сотни или тысячи» коротких мощных радиоимпульсов непосредственно перед ударом молнии.

Рис. 2. Схема образования и развития грозовой молнии из облака на землю (на снимке)

Их форма, как отмечают исследователи, соответствует модели убегающих электронов. Такая напряжённость электрического поля (более 10^{16} В/м) порождает все условия для образования сильно разветвлённого «проводящего дерева». Авторами работы [19] установлено, что «внутриоблачные разряды почти всегда возникают либо сами по себе, либо в начале вспышки молнии, это убедительно свидетельствует о том, что они являются инициирующими формированиями для образования грозовых электрических разрядов». В результате моделирования развития внутриоблачных молний [20, с. 50-71] получена гипотеза, что импульс тока внутриоблачной молнии протекает как чисто стримерный пробой (гигантская лавина стримеров), развивающийся без формирования лидерного канала.

Рис. 3. Схема образования и развития грозовой молнии от земли к облаку (на снимке)

Каждый лидер при образовании новой ступени своего развития образует импульс высокой напряжённости 10^{16} В/м, преимущественно распространяющийся в направлении электрического поля грозового облака, так и во всех остальных направлениях. В результате происходит ионизация окружающего пространства, образование новой ступени развития лидера и разрастание «ветвей проводящего дерева». Ранее в работе [21, с. 9-15] было показано, что каждая часть молнии является поджигающим разрядом для формирования следующей «черной молнии» при чем, чем мощнее поджигающий разряд, тем мощнее «темная молния», тем ниже пробивные градиенты для развития длинной молнии. В образовавшийся основной канал молнии происходит вливание боковых каналов молнии, которые и образуют видимую древовидную структуру образовавшейся молнии. Наиболее мощные «темные молнии» создают более мощные гамма и рентгеновское излучения, основная мощность которых направлена вдоль молнии.

В результате работы [22, с. 6-9] была предложена гипотеза развития молнии, которая в свете дополнения достижениями новых научных исследований получила практически полную концепцию образования и развития грозового разряда – молнии, изложенную в данной работе. В подтверждение данной модели доказывают результаты работы [23, с. 8165-8171] в которой исследователи наблюдали так называемые необычные плазменные образования в искусственных облаках отрицательно заряженных капель воды. Эти образования появились в виде сетей стримеров дециметрового масштаба со встроенными сегментами горячих каналов, сложным образом взаимодействующими друг с другом.

Таким образом, образовавшаяся молния между облаком и землёй похожа на «дерево» (рис. 1–3) с тем лишь отличием, что все внутриоблачные заряды стекаются по ветвям к стволу «дерева» (основному каналу разряда молнии), увеличивая его (её) диаметр и мощность разряда.

Литература

1. Гуревич А.В., Зыбин К.П. Пробой на убегающих электронах и электрические разряды во время грозы // УФН, 171, 2001 г, С. 1177-1199.
2. Бабич Л.П., Бочков Е.И., Куцык И.М. Механизм генерации убегающих электронов лидером молнии. Письма в ЖЭТФ, том 99, вып. 7, 2014 г, С. 452-456.
3. Журнал Discovery № 6 (54) июнь 2013. С. 8.
4. Рязанов Н.Д. Научное подтверждение существования «темных молний». Электронный научный журнал «Austria-science», 1 часть, № 20/2018, С. 47-49.
5. Джозеф Р. Дуайер. Релятивистская модель разряда с обратной связью земных гамма-вспышек 2012/2 Журнал геофизических исследований: Космическая физика Т. 117. № А2.

6. Антонова В.П., Вильданова Л.И., Гуревич А.В., Зыбин К.П., Караштин А.Н., Крюков С.В., Рябов В.А., Птицын М.О., Чубенко А.П., Шлюгаев Ю.В., Щепетов А.Л. Изучение взаимосвязи процессов в грозовой атмосфере с высокоэнергичными космическими лучами на Тянь-Шаньском экспериментальном комплексе «Гроза» Журнал технической физики, 2007, Т. 77, вып. 11.

7. Лю Н.Й., Дуайер Д.Р. Высокочастотные радиовсплески Tunderstorm со слабым низкочастотным излучением. Геофиз. Res. Lett. 47, e2020GL090325.
https://doi.org/10.1029/2020GL090325 (2020).

8. Юдин Д.И., Раков В.А., Сысоев А.А., Булатов А.А., Хаякава М. Формирование дециметровых долгоживущих областей повышенной ионной проводимости в грозовых облаках. NPJ Clim. Atmos. Sci. 2, 46. https://doi.org/10.1038/s41612-019-0102-8 (2019).

9. Юдин Д.И., Раков В.А., Сысоев А.А., Булатов А.А., Хаякава М. От областей повышенной ионной проводимости в облаках размером в дециметр до возникновения молний. Scientific Reports Т. 11, номер статьи: 18016 (2021).

10. Иудин Д.И., Сысоев А.А., Раков В.А. Проблемы инициации и развития молнии // Изв. вузов. Радиофизика. 2021. Т. 64, № 11. С. 867-894.

11. Гущин М.Е., Зудин И.Ю., Вершинин И.М., Микрюков П.А., Сыссоев В.С., Сухаревский Д.И., Орлов А.И., Наумова М.Ю., Кузнецов Ю.А., Швец Н.Н., Мареев Е.А. Субнаносекундный электромагнитный импульс, генерируемый длинным искровым разрядом: влияние молнии Т. 51, 11.

12. Ермаков В.И., Стожков Ю.И. Физика грозовых облаков, Москва, 2004.

13. Имянитов И.М. О зонах неоднородностей в грозовых облаках / И.М. Имянитов, Т.В. Лободин // Труды ГГО. – 1964. – Вып. 157. – С. 3-8.

14. Имянитов И.М. Электричество облаков / И.М. Имянитов, Е.В. Чубарина, Я.М. Шварц. – Ленинград: Гидрометеоиздат, 1971. – 93 с.

15. Evans W.A. Differential mill for measuring electric fields and conductivities in thunderclouds / W.A. Evans, R.L. Peek // Pure Appl. Geophys. – 1970. – Vol. 80. – № 3. – P. 359-370.

16. Юдин Д.И., Раков В.А., Сысоев А.А., Булатов А.А., Хаякава М. От областей повышенной ионной проводимости в облаках размером в дециметр до возникновения молний. Scientific Reports Т. 11, номер статьи: 18016 (2021).

17. Рязанов Н.Д. Явление снижения электрической прочности диэлектриков // Электронный научный журнал «Исследования технических наук». – 2014. – Выпуск 3(13) Июль-Сентябрь. С. 46-51.

18. Fishman G.J., Bhat P.N., Mallozzi R., Horack J.M., Koshut T., Kouveliotou C., et al. (1994). Discovery of intense gamma-ray flashes of atmospheric origin. Science, № 264 (5163), P. 1313-1316. https://doi.org/10.1126/science.264.5163.1313)

19. Тиллес Д.Н., Лю Н., Стэнли М.А., Кребил П.Р., Рисон У., Сток М.Г., Дуайер Д.Р., Браун Р., Уилсон Д. Быстрый отрицательный пробой в грозу Nature Communications. Т. 10, Номер статьи: 1648 (2019).

20. Сысоев А.А., Иудин Д.И., Раков В.А. и др. Численное моделирование сильноточных атмосферных разрядов с учетом термодинамики плазменных каналов. Ч. 1. Описание модели // Глобальная энергия. 2023. Т. 29, № 4. С. 50-71. DOI: https://doi.org/10.18721/ JEST.29403

21. Рязанов Н.Д. Особенности развития грозовой молнии. Norwegian Journal of development of the International Science No 121/2023. С. 9-15.

22. Рязанов Н.Д. Решена загадка развития грозовой молнии. Norwegian Journal of development of the International Science No 49/2020. С. 6-9.

23. Костинский А.Ю. и др. Наблюдение нового класса электрических разрядов в искусственных облаках заряженных капель воды и его значение для инициирования молнии в грозовых облаках. Геофиз. Res. Lett. 42, С. 8165-8171. 20 https://doi.org/10.1002/2015GL0656 (2015).

RYAZANOV Nikolay Danilovich
Director, Pulse Complex Technologies LLC, Russia, Tomsk

THE REAL HYPOTHESIS OF THE ORIGIN AND DEVELOPMENT OF THUNDER LIGHTNING

Abstract. *Based on the latest scientific achievements in the field of studying the origin and development of thunder lightning, the article presents the most realistic picture of the origin and development of thunder lightning.*

Keywords: *electric field strength, X-ray and gamma radiation, radio radiation, streamer, leader, lightning, "igniting" discharge.*

НЕФТЯНАЯ ПРОМЫШЛЕННОСТЬ

ВАСИЛЕВСКАЯ Светлана Петровна
кандидат технических наук, доцент,
Оренбургский государственный университет, Россия, г. Оренбург

ИОВА Виктория Игоревна
магистрантка, Оренбургский государственный университет, Россия, г. Оренбург

КОРРОЗИЯ РЕЗЕРВУАРОВ ДЛЯ ХРАНЕНИЯ НЕФТИ

Аннотация. *Резервуары являются основным видом сооружения, для хранения нефти и нефтепродуктов. С увеличением срока эксплуатации резервуаров возрастает скорость коррозионных повреждений. На интенсивность и характер влияют различные отложения из продуктов коррозии, тяжелых компонентов нефти и солей. Исследования показывают, что 70% аварий на нефтехранилищах происходят из-за коррозионных повреждений. Таким образом, проблема резервуаров для хранения нефти приобретает особую актуальность.*

Ключевые слова: *коррозия, резервуары, нефть, нефтепродукты, коррозионные процессы.*

Последствия коррозии не только уменьшают срок службы оборудования, но и представляют собой непосредственную опасность. Ослабление структуры металла коррозией может привести к разрушению стенок резервуара, даже не превышая эксплуатационной нагрузки. В поврежденном оборудовании может быть ослаблена прочность конструкций: проржавевшие опоры могут рухнуть, а верхняя часть резервуара может стать неспособной выдержать вес.

Для эффективной защиты от коррозии необходимо понимать, что коррозионные процессы по-разному влияют на отдельные участки резервуара. Коррозионные процессы отдельных участков резервуара описаны в таблице (табл. 1) [1, с. 12].

Таблица 1

Коррозионные процессы отдельных участков резервуара

Зона резервуара	Типы коррозии	Факторы, ускоряющие коррозию
Стенки (подземная часть)	Электрохимическая	Нарушение барьерной изоляции, воздействие почвенных электролитов
Стенки (паровое пространство, крыша)	Атмосферная	Влага, токсичные пары, конденсация летучих кислот
Днище (внутренняя сторона)	Питтинговая коррозия	Наличие агрессивной среды, соли, высокая температура
Днище (наружная сторона)	Электрохимическая, микробиологическая	Высокая влажность грунта, неоднородность почвы

На коррозионные процессы в резервуарах влияют химические, физические и биологические факторы.

Внешняя коррозия, разрушает днище и подземные части стенок, носит преимущественно электрохимический характер из-за влажного грунта, выступающего в роли электролита. Разность потенциалов, вызванная неоднородностью почвы или наличием блуждающих токов, приводит к образованию активных гальванических пар и ускоренному разрушению металла [2, с. 101].

Внутренняя коррозия резервуаров для нефти и нефтепродуктов в основном зависит от многоуровневой среды. Наибольший риск представляет подтоварная вода,

скапливающаяся на дне. Содержание агрессивных компонентов в водной среде таких как, растворенный кислород, хлориды, сероводород и углекислый газ, снижают pH и ускоряют коррозию.

Коррозия в паровом пространстве, включая крышу и верхний пояс стенок, обусловлена конденсацией влаги, в которой растворяются летучие кислые компоненты, приводя к образованию агрессивных кислот и локальному разрушению [3, с. 5].

Критической зоной является днище резервуара, которое подвержено двойному риску: внутренней коррозии подтоварной водой и внешней почвенной коррозии.

Резервуары без противокоррозионной защиты обладают коротким сроком эксплуатации. Методы защиты от коррозии резервуаров описаны в таблице (табл. 2) [4, с. 4].

Таблица 2

Методы защиты от коррозии

Метод защиты	Принцип действия	Область применения
Катодная защита	Приложение внешнего тока: резервуар – катод, вспомогательные аноды в грунте отдают ток, подавляя растворение металлов	Подземные и грунт контактирующие резервуары
Анодная защита	Поддержание металла под слабым анодным потенциалом, на котором он пассивируется прочной оксидной пленкой	Химические резервуары из нержавеющей стали
Металлическое покрытие	Нанесение на сталь слоя более активного металла, который изолирует поверхность и играет роль анодного протектора при повреждении	Наружные поверхности резервуаров, опорные конструкции, внутренние части оборудования
Лакокрасочное покрытие	Барьерный изолирующий слой на поверхности металла, предотвращающий контакт с электролитом	Внутренние стены, днище и наружная поверхность всех резервуаров
Протекторная защита	Присоединение жертвенного металла (Mg, Zn, Al), который корродирует вместо стали, делая ее катодом	Днища резервуаров с подтоварной водой, автономная защита без электроэнергии

Коррозия резервуаров – многофакторный процесс, требующий комплексного подхода. Сочетание современных методов защиты, регулярного мониторинга и соблюдения нормативов позволяет:

- увеличить срок службы резервуаров до 30–40 лет;
- снизить риск аварий на 80–90%;
- сократить затраты на ремонт и ликвидацию последствий утечек [5, с. 5].

Коррозия резервуаров для хранения нефти и нефтепродуктов представляет собой серьезную опасность для окружающей среды. Применение современных технологий, регулярные проверки и правильный выбор материалов могут существенно продлить срок службы резервуаров, предотвратив утечки и аварии.

Литература

1. Николаева М.В., Атласов Р.А. Особенности коррозии резервуаров // Нефтегазовое дело. – 2018. – С. 12.

2. Коваленко М.Н. Исследование и обоснование применения эффективных методов борьбы с корпоративным разрушением резервуаров товарной нефти: дис. техн. наук: 21.04.01. – Томск, 2017. – 101 с.

3. Исанбердина Л.Р. Коррозионные повреждения стальных резервуаров для хранения нефти и нефтепродуктов // Технология техносферной безопасности. – 2016. – С. 5.

4. Гужва В.Е. Коррозия внутренней части резервуаров для хранения нефти / В.Е. Гужва. – Текст: непосредственный // Молодой ученый. – 2019. – № 41 (279). – С. 4-8.

5. Маскаева А.Ф. Предотвращение распространения коррозии нефтяных резервуаров как мера повышения надёжности их эксплуатации // Вестник магистратуры. – 2022. – С. 5.

VASILEVSKAYA Svetlana Petrovna
Candidate of Technical Sciences, Associate Professor,
Orenburg State University, Russia, Orenburg

IOVA Victoria Igorevna
Graduate Student, Orenburg State University, Russia, Orenburg

CORROSION OF OIL STORAGE TANKS

Abstract. *Reservoirs are the main type of structure for storing oil and petroleum products. As the service life of the tanks increases, the rate of corrosion damage increases. The intensity and character are influenced by various deposits from corrosion products, heavy components of oil and salts. Studies show that 70% of accidents at oil storage facilities occur due to corrosion damage. Thus, the problem of oil storage tanks is becoming particularly relevant.*

Keywords: *corrosion, reservoirs, oil, petroleum products, corrosion processes.*

ТЕХНИЧЕСКИЕ НАУКИ

БАРАНОВ Тихон Дмитриевич
ученик, МБОУ «Коляновская СШ», Россия, г. Иваново

ПЛАЗМЕННО-ФОТОННЫЙ КИНЕТИЧЕСКИЙ ЭЛЕКТРОГЕНЕРАТОР (ПФКЭТ): КОНЦЕПЦИЯ И ПРЕИМУЩЕСТВА

Аннотация. *Работа посвящена исследованию принципиально нового способа генерации электроэнергии посредством объединения процессов плазмообразования, фотоэлектричества и кинетической энергии. Рассматривается концепция плазменно-фотонного кинетического электрогенератора (ПФКЭТ), отличающегося существенным повышением эффективности и уменьшением размеров по сравнению с ныне используемыми устройствами. Изучение теоретических основ концепции обещает значительные улучшения в сфере производства энергии и защиту окружающей среды.*

Ключевые слова: *альтернативная энергетика, плазма, фотоэлектроника, кинетическая энергия, ПФКЭТ, экология, экономика.*

Введение

Современные системы энергообеспечения сталкиваются с растущими проблемами истощения ископаемых ресурсов и негативного влияния на природу. Переход к возобновляемым источникам становится необходимым условием устойчивого развития цивилизации. Одной из многообещающих областей являются технологии плазмы и фотоэлектрики, позволяющие производить электроэнергию экологически чистыми способами. Однако традиционные методы ограничиваются низкой эффективностью и высокими материальными затратами.

Для преодоления указанных трудностей было предложено объединить три фундаментальные составляющие: образование плазмы, фотоэлектрику и кинетическую энергию. Полученное устройство получило название «Плазменно-фотонный кинетический электрогенератор» (ПФКЭТ). Данный аппарат способен существенно увеличить выработку энергии при снижении общих расходов и минимизации вреда экологии.

Принцип работы устройства

Основу конструкции ПФКЭТа составляют три ключевые компоненты:

- Плазменная камера. Газ внутри камеры подвергается воздействию мощного разряда, образуя плазму, богатую свободными электронами и фотонами.
- Фотоэлектрические элементы. Располагаясь вблизи плазменной камеры, собирают и преобразуют фотоны в электричество, повышая общую эффективность устройства.
- Кинетический механизм. Роторные лопасти в камере испытывают давление потока горячей плазмы, создавая механическое вращательное движение, которое далее превращается в электрическую энергию.

Описание

Шаг 1

Проведите осевую линию по центру – это ось плазменного шнура.

Разделите цилиндр на зоны сверху вниз (примерные пропорции):

- Верхняя крышка: 5% высоты.
- Зона ввода газа: 10%.
- Центральная камера плазмы: 40%.
- Роторный узел: 20%.
- Система охлаждения + нижнее основание: 25%.

Шаг 2. Верхняя крышка

Наверху цилиндра – плоская герметичная плита с уплотнением.

На плите три патрубка с клапанами (нарисуйте как короткие вертикальные трубки):

- входной (подача азота) – слева;
- выходной (сброс газа) – справа;
- аварийный предохранительный – по центру.

Мелкие кружки-датчики вокруг клапанов (давление, состав газа).

Шаг 3. Зона ввода газа

Под крышкой – конический или цилиндрический канал-распределитель (сужается вниз).

Внутри канала – две-три сетчатые диафрагмы (горизонтальные круги с мелкими отверстиями).

Шаг 4. Центральная камера плазмы

Электроды: два вертикальных стержня, выступающих изнутри стенок навстречу друг другу (не соприкасаются).

Катушка Тесла: наружная спираль из 5–8 витков вокруг цилиндра (в зоне плазмы).

Плазменный шнур: светящийся столб по оси (заштрихуйте ярко-голубым или фиолетовым).

Мембраны-волноводы: 2-3 горизонтальных кольца с резонансными отверстиями (нарисуйте как тонкие круги с 6–12 радиальными прорезями).

Шаг 5. Фотооптическая система

Внутреннее покрытие: тонкая зеркальная линия вдоль всей камеры (серый с блёстками).

Фотоэлементы: 6–10 прямоугольников снаружи цилиндра, равномерно по высоте (закрасьте тёмно-синим или чёрным).

Токособирающее кольцо: горизонтальный круг снаружи, к которому подведены провода от фотоэлементов.

Шаг 6. Роторный узел

Роторное кольцо: толстый горизонтальный круг в нижней половине камеры плазмы.

Лопатки (8–12 шт.):

- нарисуйте как узкие треугольники или трапеции, прикреплённые к кольцу;
- угол наклона к радиусу: 30–45° (острые края смотрят «по ходу» потока плазмы);
- профиль: заострённая передняя кромка, плавно сужающаяся задняя.

Вал ротора: вертикальная линия через центр, проходящая сквозь нижнее основание.

Подшипники: два маленьких круга по бокам вала у нижней границы роторного узла (закрасьте серым).

Шаг 7. Система охлаждения

Каналы для теплоносителя: две концентрические линии вдоль всей высоты (между внутренней и внешней стенками цилиндра); заштрихуйте синим.

Патрубки: два коротких горизонтальных отвода внизу слева и справа (вход/выход теплоносителя).

Насос и теплообменник: снаружи, рядом с патрубками (нарисуйте как прямоугольники со стрелками).

Шаг 8. Нижнее основание

Опорные лапы: три-четыре треугольных «ножки» под цилиндром.

Выходной вал: продолжение центрального вала внизу, выходит через герметичный сальник (круг с уплотнением).

Кабельные вводы: 2-3 маленьких патрубка сбоку для проводов.

Шаг 9. Электронная система управления

Блок управления: прямоугольник сбоку вверху (закрасьте зелёным или серым).

Дисплей: маленький экран на блоке (прямоугольник с цифрами).

Интерфейсы: несколько кружков и разъёмов на панели блока.

Шаг 10. Вспомогательные компоненты

Баки с азотом: два-три вертикальных цилиндра слева/справа от основного корпуса (подпишите «N_2»).

Аккумуляторные модули: прямоугольные блоки под основным цилиндром (подпишите «Акк.»).

Модули управления нагрузкой: маленькие коробки рядом с аккумуляторами (подпишите «УН»).

Цветовые обозначения (для наглядности):

- Плазма: ярко-голубой или фиолетовый (штриховка).
- Лопатки: серый/металлический.
- Охлаждение: синий (каналы и патрубки).
- Электроника: зелёный (блок управления), чёрный (фотоэлементы).
- Газ: светло-серый (в баках и каналах).
- Металл корпуса: тёмно-серый с контуром.

Итог

У вас должен получиться вертикальный разрез цилиндра с:

- верхней крышкой и клапанами;
- зоной ввода газа с диффузорами;
- центральной камерой с электродами, плазмой и катушкой;
- ротором с наклонными лопатками;
- системой охлаждения в стенках;
- нижним основанием с валом и опорами;
- внешними блоками управления, баками и аккумуляторами.

Интеграция всех трех процессов гарантирует эффективное использование всей

доступной энергии, снижая количество потерь и увеличивая выход полезного продукта.

Преимущества и перспективы

Основные достоинства разработанной концепции включают:

- Экономичность: низкие затраты на единицу выработанной энергии.
- Экологичность: отсутствие вредных выбросов и минимальное загрязнение атмосферы.
- Компактность: малые габариты упрощают транспортировку и монтаж оборудования.
- Автономность: независимость от центральных сетей, позволяющая использовать устройство в удаленных и труднодоступных регионах.
- Область применения ПФКЭТа широка: от бытового сектора до промышленного уровня. Небольшие размеры и мобильность позволяют применять систему в качестве основного или резервного источника питания для любых объектов инфраструктуры.

Заключение

Представленная концепция плазменно-фотонного кинетического электрогенератора показывает огромный потенциал для совершенствования методов генерации электроэнергии. Объединение процессов плазмообразования, фотоэлектричества и кинетики открывает путь к созданию эффективных устройств, обеспечивающих доступность чистого и дешевого электричества. Дальнейшие научные эксперименты и практические испытания подтвердят жизнеспособность и надежность предложенной схемы, выводя мировую энергетику на качественно новый уровень.

Литература

1. Алферов Ж.И. Проблемы и перспективы полупроводниковой электроники. // Физтеховский вестник. – 2010. – № 1.
2. Николаев Г.А. Физика плазмы и управляемый термоядерный синтез. Учебное пособие. – Москва: Физматлит, 2012.
3. Широков Ю.М. Механизмы преобразования энергии в молекулярно-массивных средах. // Известия вузов. Серия «Физиоматематические науки». – 2015. – № 3.

BARANOV Tikhon Dmitrievich
Student, MBOU Kolyanovskaya Secondary School, Russia, Ivanovo

PLASMA PHOTON KINETIC ELECTRIC GENERATOR (PFCAT): CONCEPT AND ADVANTAGES

Abstract. *The work is devoted to the study of a fundamentally new method of generating electrical energy by combining the processes of plasma formation, photoelectricity and kinetic energy. The concept of a plasma-photonic kinetic electric generator (PFCAT) is considered, which is characterized by a significant increase in efficiency and a reduction in size compared to currently used devices. Studying the theoretical foundations of the concept promises significant improvements in energy production and environmental protection.*

Keywords: *alternative energy, plasma, photovoltaics, kinetic energy, PFCAT, ecology, economics.*

ГРЕБНЕВ Сергей Андреевич
студент, Уральский государственный университет путей сообщения, Россия, г. Екатеринбург

МАЙЕР Роберт Дмитриевич
студент, Уральский государственный университет путей сообщения, Россия, г. Екатеринбург

Научный руководитель – старший преподаватель Уральского государственного университета путей сообщения Чебаков Сергей Алексеевич

ГАРМОНИКИ ТОКА В СИЛОВЫХ ЦЕПЯХ ЭЛЕКТРОВОЗА ВЛ-10 И ИХ ВЛИЯНИЕ НА РАБОТУ ОБОРУДОВАНИЯ

Аннотация. *Статья посвящена комплексному исследованию актуальной проблемы генерации высших гармоник тока в силовых цепях современного тягового электроподвижного состава ВЛ 10. Актуальность работы обусловлена повсеместным переходом от традиционных коллекторных машин к высокоэффективным, но нелинейным тяговым приводам на основе мощных полупроводниковых преобразователей. Основное внимание уделено детальному анализу ключевых источников гармонических искажений, которыми являются силовые полупроводниковые преобразователи (выпрямители и инверторы), лежащие в основе импульсного регулирования тягового электропривода. Рассматривается физический механизм их возникновения, связанный с нелинейным, импульсным характером потребления тока от контактной сети, что приводит к формированию несинусоидальной формы тока, богатой высшими гармониками со специфичным спектральным составом. Наряду с выявлением причин, в работе всесторонне исследуется негативное влияние гармонических искажений на стабильность и надежность работы критически важного бортового оборудования электровоза, подчеркивая значимость проблемы для эксплуатационной безопасности и долговечности подвижного состава.*

Ключевые слова: *гармоники тока, электровоз ВЛ-10, тяговый привод, несинусоидальные токи, высшие гармоники, коэффициент искажения, полупроводниковый преобразователь, влияние на оборудование.*

Электрическая энергия для электровозов является ключевым ресурсом, обладающим уникальными свойствами. Её качество напрямую влияет на надёжность тяги и работу всех бортовых систем. Понятие качества электроэнергии (КЭ) на электровозе отличается от качества электроэнергии других приемников. Каждый электроприёмник электровоза – от тяговых двигателей до систем управления – предназначен для работы при строго определённых параметрах (напряжении, частоте, токе), поэтому для стабильной работы подвижного состава должно быть обеспечено требуемое КЭ.

Возросшие требования железнодорожного транспорта к эффективности и точности управления привели к широкому внедрению силовых полупроводниковых приборов. Современные активно используют тиристорные преобразователи, устройства плавного пуска и статические преобразователи. Однако эти же технологии, вытеснив устаревшие решения, изменили картину формы тока и напряжения в контактной сети. Твердотельные элементы, такие как полупроводниковые приборы, значительно изменили схемотехнику, но при этом возникла проблема с генерацией токовых гармоник. Это ухудшает качество электроэнергии и может вызывать помехи.

Гармоники – это синусоидальные волны, суммирующиеся с фундаментальной (основной) частотой 50 Гц (то есть первая гармоника – 50 Гц, пятая гармоника – 250 Гц). Любая комплексная синусоида может быть представлена как сумма определенного количества гармоник, как четных, так и нечетных, с различными амплитудами. Любая несинусоидальная кривая может быть разложена в сумму ряда Фурье, на различные гармоники.

$$i(t) = I_0 + \sum_{k=0}^{n} I_{km} \sin(k\omega + \varphi_k) \quad (1)$$

Где I_0 – постоянная составляющая; $I_{km}\sin(k\omega + \varphi_k)$ – гармоники или гармонические составляющие k-го порядка с амплитудой I_{km} и начальной фазой φ_k; n – номер последней из учитываемых высших гармоник [1].

Анализ спектрального состава гармонических искажений является ключевым методом исследования помех в силовых цепях электровозов. Его основная задача заключается в идентификации частотных составляющих, присутствующих в сигнале, помимо основной частоты, а также в определении их амплитуд и фаз. Это позволяет выявить гармоники, которые могут оказывать опасное или мешающее влияние на смежные системы, в частности, на устройства сигнализации, централизации и блокировки и автоматическую локомотивную сигнализацию.

Теоретической основой для такого анализа служит преобразование Фурье, которое базируется на принципе разложения сложного сигнала в бесконечный, но счетный ряд синусоидальных и косинусоидальных составляющих. Для практических расчетов, особенно при работе с цифровыми сигналами, используется дискретное преобразование Фурье, а его высокоэффективный алгоритм – быстрое преобразование Фурье. Эти методы позволяют перейти от временного представления сигнала к частотному, то есть получить его спектр.

Методика анализа предполагает несколько последовательных этапов. Первоначально производится запись аналогового сигнала, пропорционального току, протекающему в силовой цепи или в рельсах. Далее этот сигнал оцифровывается с определенной частотой дискретизации. Полученный цифровой массив данных подвергается спектральному анализу с помощью быстрого преобразования Фурье. Результатом этого анализа является набор гармонических составляющих, для каждой из которых известна частота, амплитуда и фаза. Эти данные архивируются и могут быть представлены в виде графиков спектра, что обеспечивает наглядность при идентификации проблемных гармоник [2, с. 33-38].

Гармонические искажения тока в тяговой сети возникают вследствие работы полупроводниковых преобразователей в приводах электровоза ВЛ10, в частности входных 4Q-преобразователей. Эти устройства, обеспечивая высокую мощность, генерируют в сети высшие гармоники тока и напряжения, что вызывает дополнительные потери, снижение коэффициента мощности и потенциально влияет на работу другого оборудования.

Спектральный состав гармоник напрямую зависит от алгоритма управления силовыми ключами (IGBT-транзисторов) преобразователей. Исследования [1, 3] показывают, что ключевыми в спектре тока являются 3-я, 5-я, 7-я гармоники. Однако при использовании многочисленных параллельно работающих преобразователей с фазовым сдвигом тактирующих сигналов управления формируется широкий массив нечетных гармоник. Их центр тяжести смещается в область высокой частоты, равной $f_н = 2 \cdot К_т \cdot N \cdot f_с$, где $К_т$ – кратность частоты тактирования, N – число преобразователей, $f_с$ – частота сети.

Уровень искажений количественно оценивается коэффициентом нелинейных искажений (THD). Анализ [1] показал, что для снижения THD входного тока критически важно применение много канальных систем управления с фазовым сдвигом. Например, при шести параллельных преобразователях (N=6) и кратности частоты ($К_т$ =6) коэффициент THD тока составляет всего 0.0039, что свидетельствует о практически синусоидальной форме тока. В то же время THD напряжения сети остается на более высоком уровне (~0.0306), так как на него сильнее влияют импедансы питающей сети.

Таким образом, гармоники тока в силовых цепях электровоза ВЛ 10 существенно влияют на энергетические показатели оборудования. Для минимизации этого влияния необходима оптимизация алгоритмов управления преобразователями, в частности, использование фазового сдвига тактирующих сигналов и выбор оптимальной кратности частоты коммутации, что позволяет снизить уровень гармоник и повысить общую эффективность работы электровоза [3].

Данные гармонические составляющие не выполняют полезной работы, но вызывают существенные дополнительные потери в активных сопротивлениях обмоток ключевого оборудования. В первую очередь это касается тягового трансформатора, сглаживающих реакторов и обмоток самих тяговых электродвигателей. Эти потери выделяются в виде избыточного тепла, что приводит к повышению рабочей температуры критически важных узлов.

Постоянный перегрев ускоряет процесс старения изоляции, снижает механическую прочность материалов и приводит к сокращению расчетного срока службы агрегатов, повышает вероятность внезапных отказов и увеличивает эксплуатационные расходы на техническое обслуживание и ремонт. Кроме того, сами потери снижают общий коэффициент полезного действия силовой установки электровоза.

Электровоз ВЛ 10 оснащен сложной сетью низковольтных цепей управления, защиты, диагностики и автоматического регулирования. Работа этой аппаратуры рассчитана на питание и измерение параметров синусоидального или выпрямленного тока с минимальным уровнем искажений. Наличие в силовой сети высокочастотных гармонических искажений формы кривых тока и напряжения создает серьезные помехи. Через цепи связи и электромагнитное поле эти помехи могут проникать в чувствительные электронные и релейные схемы. Это способно вызывать ложные срабатывания или отказы защитных реле, приводить к искажению данных, получаемых с измерительных трансформаторов тока и напряжения, и, как результат, формировать некорректные показания на пульте машиниста. Наиболее опасно нарушение работы систем автоматического регулирования (например, регулирования возбуждения или плавности пуска), что напрямую сказывается на устойчивости тягового режима и безопасности ведения поезда. Таким образом, гармоники дестабилизируют работу всего комплекса бортовой автоматики.

Процесс импульсного преобразования энергии в выпрямителях и, что особенно характерно для более современных систем управления, использование импульсных регуляторов в цепях тяговых двигателей приводят к возникновению не только дискретных гармоник, но и широкополосного спектра электромагнитных излучений. Эти высокочастотные помехи излучаются контактной сетью, токоприемником и силовыми кабелями локомотива. Они могут создавать значительные помехи в работе систем радиосвязи (поездной, станционной), а также вносить искажения в работу других бортовых электронных устройств. Таким образом, гармонические и импульсные искажения тока усложняют обеспечение электромагнитной совместимости (ЭМС) железнодорожного подвижного состава с окружающей инфраструктурой и средствами связи [4].

Литература

1. Кобелев А.В., Зыбин А.А. Современные проблемы высших гармоник в городских системах электроснабжения / А.В. Кобелев, А.А. Зыбин // Вестник Тамбовского государственного технического университета URL: https://cyberleninka.ru/article/n/sovremennye-problemy-vysshih-garmonik-v-gorodskih-sistemah-elektrosnabzheniya?ysclid=mih1mcht6855948521 5.

2. Сердюк Т.Н. Исследование влияния гармоник тягового тока электровоза на работу рельсовых цепей // Электромагнитная совместимость и безопасность на железнодорожном транспорте. – Днепропетровск: ДНУРТ, 2011. – № 2. – С. 33-38.

3. Назирхонов Т.М., Якушев А.Я., Викулов И. П. Анализ спектрального состава входного тока и напряжения 4q-s преобразователя электровоза переменного тока серии «o'Z-ELR» с использованием компьютерной имитационной модели // Бюллетень результатов научных исследований / 2020.

4. Баранов В.А. Импульсные регуляторы в цепях тяговых двигателей при последовательно-независимом возбуждении.

GREBNEV Sergey Andreevich
Student, Ural State University of Railway Transport, Russia, Yekaterinburg

MAYER Robert Dmitrievich
Student, Ural State University of Railway Transport, Russia, Yekaterinburg

Scientific Advisor – Senior Lecturer at the Ural State University of Railway Transport
Chebakov Sergey Alekseevich

HARMONICS OF CURRENT IN THE POWER CIRCUITS OF THE VL-10 ELECTRIC LOCOMOTIVE AND THEIR EFFECT ON THE OPERATION OF EQUIPMENT

Abstract. *The article is devoted to a comprehensive study of the actual problem of generating high current harmonics in power circuits of modern traction electric rolling stock overhead line 10. The urgency of the work is due to the widespread transition from traditional collector machines to highly efficient, but nonlinear traction drives based on powerful semiconductor converters. The main attention is paid to a detailed analysis of the key sources of harmonic distortion, which are power semiconductor converters (rectifiers and inverters) underlying the pulse control of a traction electric drive. The physical mechanism of their occurrence is considered, related to the nonlinear, pulsed nature of current consumption from the contact network, which leads to the formation of a non-sinusoidal current shape rich in higher harmonics with a specific spectral composition. Along with identifying the causes, the work comprehensively explores the negative impact of harmonic distortion on the stability and reliability of the critically important on-board equipment of an electric locomotive, emphasizing the importance of the problem for operational safety and durability of rolling stock.*

Keywords*: current harmonics, VL-10 electric locomotive, traction drive, non-sinusoidal currents, higher harmonics, distortion factor, semiconductor converter, influence on equipment.*

ЖИРОВА Светлана Анатольевна
инженер-технолог, АО НПП Рубин, Россия, г. Пенза

ТИХОНОВ Евгений Сергеевич
инженер-технолог, АО НПП Рубин, Россия, г. Пенза

СОВЕРШЕНСТВОВАНИЕ ТЕХНОЛОГИИ ИЗГОТОВЛЕНИЯ ДЕТАЛЕЙ СЛОЖНОЙ КОНФИГУРАЦИИ С ПРИМЕНЕНИЕМ ВЫСОКОТОЧНОГО ЧПУ-ОБОРУДОВАНИЯ

Аннотация. *В статье рассмотрены подходы к совершенствованию изготовления деталей сложной конфигурации на высокоточном ЧПУ-оборудовании на основе управляемых и проверяемых параметров точности. Показано, что обеспечение требуемой геометрии и качества поверхности целесообразно подтверждать стандартизованными методами: оценкой позиционирования по ГОСТ ISO 230-2-2016, контурных отклонений по ГОСТ ISO 230-4-2015 и режущей точности по ГОСТ ISO 10791-7-2016. Обоснована значимость корректного пересчёта координат в пятиосевой обработке и применения RTCP, а также использования кинематической симуляции и внутристаночных измерений для повышения воспроизводимости. Сделан вывод о необходимости комплексного подхода, объединяющего диагностику по стандартам, корректную CAM/ЧПУ-подготовку и метрологическое сопровождение процесса.*

Ключевые слова: *высокоточная обработка, ЧПУ, пятиосевая обработка, детали сложной конфигурации, контурная точность, позиционирование осей, интерполяция, кинематическая симуляция, внутристаночные измерения, метрологическое обеспечение.*

Актуальность исследования

Обусловлена ростом доли изделий со сложной пространственной геометрией (тонкостенные элементы, внутренние каналы, криволинейные поверхности), востребованных в авиакосмической технике, энергетике, приборостроении и медико-технической сфере. Для таких деталей характерны повышенные требования к точности, стабильности формы и качеству поверхностного слоя, а традиционные многоустановочные схемы обработки нередко приводят к накоплению погрешностей базирования, увеличению длительности производства и росту брака.

Высокоточное ЧПУ-оборудование, включая многоосевые обрабатывающие центры, позволяет сократить число установов, повысить повторяемость и обеспечить комплексную обработку. Однако для полного использования этих преимуществ требуется совершенствование технологического процесса: оптимизация траекторий и управляющих программ, обоснованный выбор инструмента и режимов резания, а также учёт вибраций, тепловых деформаций, кинематических погрешностей станка и особенностей закрепления заготовки. Поэтому разработка решений, повышающих точность, устойчивость и производительность ЧПУ-обработки деталей сложной конфигурации, представляет собой актуальную научно-техническую задачу с высокой практической значимостью.

Цель исследования

Цель данного исследования – обосновать и систематизировать технологические решения по совершенствованию изготовления деталей сложной конфигурации на высокоточном ЧПУ-оборудовании на основе применения стандартов оценки точности и методов повышения воспроизводимости процесса, включая корректный пересчёт координат в пятиосевой обработке, кинематическую симуляцию и внутристаночный контроль.

Материалы и методы исследования

Использованы положения и требования нормативных документов, регламентирующих оценку точности металлорежущих станков и обрабатывающих центров.

Применены методы аналитического обзора и систематизации технологических факторов точности при многоосевой обработке: анализ источников погрешностей, сопоставление диагностических процедур и их технологической интерпретации, а также структурирование

практических мер обеспечения повторяемости.

Результаты исследования

В технологической практике «высокоточное изготовление» деталей сложной конфигурации на ЧПУ корректно описывать через управляемые и проверяемые параметры станка и процесса. Именно поэтому в качестве основы обычно используют действующие национальные стандарты, гармонизированные с ISO: они фиксируют, что считать точностью, как её измерять и как отделять ошибки позиционирования от ошибок контурного движения. Так, ГОСТ ISO 230-2-2016 задаёт порядок испытаний для определения точности и повторяемости позиционирования управляемых осей при раздельном измерении каждой оси, что важно для понимания «скелета» геометрической точности станка до начала тонкой настройки технологии [3].

Однако при изготовлении сложных криволинейных поверхностей и сопряжений решающим часто становится не только то, насколько точно ось «встаёт» в заданную координату, а то, насколько точно система ЧПУ ведёт контур при одновременном движении нескольких осей. Для этого применяется ГОСТ ISO 230-4-2015, который описывает круговые испытания (в том числе через показатели двунаправленного кругового отклонения и радиальных отклонений), позволяя выявлять проблемы настройки сервоприводов, согласованности осей и интерполяции. В производственной логике это важно тем, что контурные ошибки напрямую проявляются на поверхности как «волнистость», локальные отклонения профиля и уводы геометрии в переходах траектории [4].

Далее, чтобы подтвердить не «абстрактную точность станка», а способность получать требуемую геометрию в резании, используются условия испытаний обрабатывающих центров. ГОСТ ISO 10791-7-2016 устанавливает подход к оценке точности обработки испытательных образцов, то есть переводит разговор в плоскость фактического результата: что получается на детали при заданной постановке, а не только что показывает измерительный прибор в холостых перемещениях. В контексте совершенствования технологии это позволяет сравнивать базовую и улучшенную версии процесса по воспроизводимой методике, а не по единичным «удачным» замерам [2].

Отдельный ключевой блок для деталей сложной конфигурации – корректная работа с поворотными осями и пересчётом координат. На пятиосевых станках траектория, рассчитанная CAM-системой, должна быть правильно преобразована постпроцессором и стойкой ЧПУ в движения конкретной кинематической схемы станка. На практике подчёркивается значение функции RTCP (контроль положения центра инструмента/кончика инструмента): стойка пересчитывает запрограммированные координаты в реальные положения узлов так, чтобы рабочая точка инструмента сохраняла заданное положение относительно детали при изменении ориентации поворотных осей. Это снижает зависимость управляющей программы от компоновки станка и уменьшает риск систематических ошибок при переориентациях, при условии корректной настройки геометрии инструмента и трансформаций [1].

При совершенствовании технологии важно также учитывать, что «точность» на сложных поверхностях зависит от сочетания стратегии траекторий и динамики движения осей. На высоких подачах и при частых изменениях ориентации инструмента возрастают требования к плавности траектории и согласованности осей: резкие повороты могут приводить к локальным отклонениям контура. Поэтому в российских обзорах и практических материалах по пятиосевой обработке обычно акцентируют обязательность кинематической симуляции, проверки переходов и исключения коллизий не только инструмента, но и узлов станка при переориентациях, поскольку именно там часто возникают технологические риски для сложных деталей.

Наконец, устойчивость результата в серии обеспечивается метрологическим сопровождением прямо на станке. В российской практике широко применяется внутристаночное измерение заготовки и баз с помощью щупов: это позволяет уточнять нулевую точку, контролировать установочные смещения и вводить коррекции без снятия детали и без накопления ошибок от повторного базирования. Такой подход особенно важен для деталей сложной формы, где часть элементов «завязана» на взаимное расположение поверхностей и осей, а переустановка резко увеличивает риск ухода геометрии.

Выводы

Таким образом, повышение точности и устойчивости изготовления деталей сложной конфигурации на высокоточном ЧПУ-оборудовании достигается при комплексном

применении стандартизованной диагностики и технологических мер управления процессом. Оценка позиционирования по ГОСТ ISO 230-2-2016, контроль контурных отклонений по ГОСТ ISO 230-4-2015 и подтверждение режущей точности по ГОСТ ISO 10791-7-2016 обеспечивают воспроизводимую основу для сравнения и улучшения технологии. Для пятиосевой обработки критично корректное преобразование траекторий и использование RTCP, а для серийной стабильности – кинематическая симуляция, предотвращение коллизий и внутристаночные измерения с введением коррекций. В совокупности указанные решения позволяют переводить требования к точности из декларативных в измеряемые и управляемые параметры технологического процесса.

Литература

1. RTCP ЧПУ. Пятиосевая трансформация [Электронный ресурс]. – Режим доступа: https://modmash.ru/fms3000/rtcp/.

2. ГОСТ ISO 10791-7-2016. Обрабатывающие центры. Методы испытаний. Часть 7. Проверка точности обработки испытательных образцов. – Введ. 2017-07-01. – М.: Стандартинформ, 2016.

3. ГОСТ ISO 230-2-2016. Станки металлорежущие. Методы испытаний. Часть 2. Определение точности и повторяемости позиционирования управляемых осей. – Введ. 2017-03-01. – М.: Стандартинформ, 2016.

4. ГОСТ ISO 230-4-2015. Станки металлорежущие. Методы испытаний. Часть 4. Проверка точности круговой интерполяции. – Введ. 2016-07-01. – М.: Стандартинформ, 2015.

ZHIROVA Svetlana Anatolyevna
Process Engineer, JSC NPP Rubin, Russia, Penza

TIKHONOV Evgeny Sergeevich
Process Engineer, JSC NPP Rubin, Russia, Penza

IMPROVEMENT OF MANUFACTURING TECHNOLOGY FOR PARTS OF COMPLEX CONFIGURATION USING HIGH-PRECISION CNC EQUIPMENT

Abstract. *The article discusses approaches to improving the manufacture of parts of complex configuration on high-precision CNC equipment based on controlled and verifiable accuracy parameters. It is shown that it is advisable to confirm the required geometry and surface quality using standardized methods: assessment of positioning according to GOST ISO 230-2-2016, contour deviations according to GOST ISO 230-4-2015 and cutting accuracy according to GOST ISO 10791-7-2016. The importance of correct coordinate recalculation in five-axis processing and the use of RTCP, as well as the use of kinematic simulation and in-cell measurements to increase productivity is proved. The conclusion is made about the need for an integrated approach combining diagnostics according to standards, correct CAM/CNC training and metrological support of the process.*

Keywords: *high-precision machining, CNC, five-axis machining, parts of complex configuration, contour accuracy, axis positioning, interpolation, kinematic simulation, in-cell measurements, metrological support.*

РАШОЯН Ирина Игоревна
кандидат технических наук, доцент,
Тольяттинский государственный университет, Россия, г. Тольятти

ОХРАНА ТРУДА, ПРОИЗВОДСТВЕННАЯ, ЭКОЛОГИЧЕСКАЯ И ПОЖАРНАЯ БЕЗОПАСНОСТЬ КАК ПОДСИСТЕМЫ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Аннотация. *В статье показана актуальность создания в организациях систем управления комплексной безопасностью (СУКБ) на основе подсистем пожарной и экологической безопасности, охраны труда и производственной (промышленной) безопасности. Показано перспективное направление создания и совершенствования СУКБ на основе формирования интегрированной системы менеджмента (ИСМ), внедрения сквозной методология оценки и управления рисками, на формировании корпоративной культуры безопасности.*

Ключевые слова: *комплексная система управления, охрана туда, экологическая безопасность, производственная безопасность, пожарная безопасность.*

В современном российском обществе любые организации, предприятия функционируют в условиях воздействия множества взаимосвязанных техносферных рисков. Такие составляющие техносферной безопасности как пожарная и экологическая безопасность, охрана труда и производственная (промышленная) безопасность в структурах управления большинства организаций традиционно рассматриваются как изолированные друг от друга направления. Однако усиление регуляторного давления органов надзора и контроля, рост социальной ответственности бизнеса, увеличение стоимости человеческого капитала и комплексный характер возникающих аварий, инцидентов и ЧС диктуют необходимость интеграции этих элементов в единую систему управления. Такой подход позволяет оптимизировать управленческие и финансовые ресурсы, устранить противоречия в системах управления организаций и добиться синергетического эффекта в обеспечении безопасности людей, антропогенных объектов и окружающей среды. Таким образом, целью настоящей статьи является анализ методики построения системы управления комплексной безопасностью (СУКБ) организаций на основе подсистем охраны труда, производственной, экологической и пожарной безопасностью.

Существующие методы управления отдельными компонентами систем безопасности

Современные исследования предлагают как различные методы управления для каждого направления СУКБ, так и показывают их общие составляющие менеджмента.

Традиционные методы управления пожарной и промышленной безопасностью ранее были основаны на строгом выполнении нормативных требований. Однако для уникальных и сложных объектов эти методы часто являются нереализуемыми. В настоящее время законодательство РФ обеспечило переход в этих областях для организаций к риск-ориентированному управлению [1, с. 98-116; 2, с. 177-179]. В обобщенном виде этот подход реализуется через этапы:

1. Количественная оценка пожарных рисков, рисков аварий и ЧС с использованием программного моделирования их развития и процесса эвакуации людей.
2. Ранжирование объектов и их производственных процессов по уровню потенциальной опасности и категории риска.
3. Дифференциация профилактических мер и частоты контрольных (надзорных) мероприятий в зависимости от категории риска этих объектов.

Риск-ориентированный подход позволяет целесообразно распределять финансовые и материальные ресурсы организаций, обеспечивая их концентрацию на наиболее опасных участках и процессах, а также позволяет обосновывать отклонения от нормативных требований при условии применения современных

технических решений для обеспечения пожарной и промышленной безопасности. С другой стороны, охрана труда характеризуется переходом систем управления от реагирования на уже случившиеся инциденты, аварии и несчастные случаи к их предупреждению и формированию поведенческой культуры безопасности персонала. Современные методы охраны труда уходят от методов пассивного устранения последствий несчастных случаев к методам их активного прогнозирования и профилактики [3, с. 1488-1491; 4, с. 105-109; 5, с. 601-622]. При этом наиболее важным здесь является:

1. Внедрение процедур оценки профессиональных рисков, аналогичных процедурам оценки пожарных рисков и рисков аварий и ЧС. Это можно отнести к наиболее важной составляющей единой методологической базы для интеграции всех подсистем безопасности организаций в СУКБ.

2. Развитие поведенческой культуры безопасности на производстве через методы наблюдений, обратной связи и прямого вовлечения персонала.

3. Использование цифровых платформ для регистрации опасных инцидентов, проведения инструктажей и контроля состояния оборудования.

Если говорить о методах управления экологической безопасностью, то экологический менеджмент в настоящее время не ограничивается простым соблюдением нормативов. Ряд научных работ [5, с. 601-622; 6; 7, с. 11-18] описывает преимущества и широкое применение таких методов управления как:

1. Внедрение системы экологического менеджмента (СЭМ) по стандарту ISO 14001, построенной на цикле PDCA (Plan-Do-Check-Act);

2. Оценка экологических аспектов и рисков на всех стадиях жизненного цикла продукции или услуги;

3. Внедрение принципов рециклинга и оптимизации использования ресурсов, направленных на минимизацию образования отходов и максимальное использование вторичного сырья. При этом данный метод напрямую связан с системой управления охраной труда за счет снижения воздействий вредных веществ на персонал и с системой пожарной безопасности за счет управления отходами, способными к самовозгоранию.

Предлагаемые методы интеграции систем безопасности в единую систему управления комплексной безопасностью (СУКБ)

Ключевая решение при этом состоит в том, что перспективным направлением интеграции является не параллельное существование различных систем управления безопасностью, а их глубокая взаимная интеграция. При этом стоит рассмотреть различные подходы к реализации такого решения:

1. Интеграция на основе единой системы менеджмента. Наиболее концептуально проработанным методом является создание Интегрированной системы менеджмента (ИСМ), объединяющей требования стандартов ISO 45001, ISO 14001, ISO 9001 и национальных нормативных правовых документах. Данный метод может базироваться на следующих принципах:

- унификации процессов, который предусматривает для СУКБ единые циклы планирования, внедрения, мониторинга и улучшений (PDCA).
- синхронизации политик и целей организации, что может быть реализовано через формулирование единой Политики СУКБ, устанавливающей общие обязательства в области охраны труда, производственной (промышленной), пожарной и экологической безопасности.
- консолидации внутренней документации путем создания общих инструкций, регламентов или процедур (например, процедура управления инцидентами),
- организации комплексного аудита безопасности, что снижает нагрузку на отдельные подразделения организаций.

2. Комплексный риск-ориентированный подход. Как следует из проведенного выше анализа, ключевым интегрирующим методологическим инструментом здесь является система управления рисками. Основу для это может составить единый реестр рисков для каждой конкретной организации, где каждый опасный фактор оценивается с точки зрения последствий для жизни и здоровья персонала, для окружающей среды, а также с точки зрения возникновения материального ущерба и сохранения непрерывности деятельности. Это позволит ранжировать риски по комплексному приоритету и разрабатывать единые планы мероприятий СУКБ, направленные одновременно на снижение нескольких видов рисков.

Например, модернизация системы вентиляции снижает риск воздействия на персонал химических факторов (охрана труда), риск превышения ПДК вредных веществ в выбросах (экологическая безопасность) и вероятность взрыва пылевоздушной смеси (пожарная и промышленная безопасность). Этот принцип предполагает не просто соблюдение нормативных предписаний, а активное выявление, анализ и контроль рисков, специфичных для каждой конкретной организации.

3. Формирование культуры безопасности. Эффективная культура безопасности должна быть основана на ответственности и регулярном обучении руководителей и персонала, на своевременном анализе причин и последствий ошибок. При этом существующие формальные процедуры охраны труда, производственной (промышленной), пожарной и экологической безопасности при обучении, мотивации и коммуникации персонала становятся едиными процессами, не разделенными по ведомственному признаку.

Заключение

Анализ современных научных публикаций демонстрирует общее направление развития методов управления комплексной безопасностью организаций, которое основано на формировании интегрированной системы менеджмента (ИСМ), на сквозной методологии оценки и управления рисками, на формирование корпоративной культуры безопасности.

Реализация этих методов требует пересмотра организационной структуры, инвестиций в квалификацию персонала и модернизацию технологий, но ведет в перспективе к качественно новому уровню безопасности и эффективности деятельности организации. Разработка и проектирование СУКБ при этом обеспечивает социальную ответственность, непрерывность бизнеса и долгосрочную конкурентоспособность.

Литература

1. Ершов А.В., Коробко В.Б. О проблеме перехода государственного управления в техносфере на новую риск-ориентированную модель на примере обеспечения пожарной безопасности. // Пожаровзрывобезопасность. 2021. Т. 30. № 2. С. 98-116.

2. Шевелева И.С., Юсупджанов В.И. Внедрение риск-ориентированного подхода в области промышленной безопасности // Неделя науки СПБПУ: материалы научной конференции с международным участием. Ч. 3. Санкт-Петербургский политехнический университет Петра Великого. 2020. С. 177-179.

3. Сулейменова Р.Д., Сергеева А.Д. Цифровизация управления профессиональными рисками на производстве в России // Актуальные вопросы обеспечения комплексной безопасности: Материалы национальной НПК с международным участием, посвященной 35-летию МЧС России и 95-летию Оренбургского ГАУ. Оренбург, 2025. С. 1488-1491.

4. Сидельникова О.П., Власов К.Е. Специальная оценка труда и оценка профессионального риска в системе охраны труда // Вестник Луганского государственного педагогического университета. Серия 5. Гуманитарные науки. Технические науки. 2021. № 3 (68). С. 105-109.

5. Лыскова И.Е. Методологические основы управления результативностью культуры производственной безопасности промышленных предприятий // Экономическая безопасность. 2022. Т. 5. № 2. С. 601-622.

6. Гаврилова Н.С. Изучение особенностей интеграции системы охраны труда и системы экологического менеджмента на примере ООО «Газпром добыча Уренгой» // Электронный научно-методический журнал Омского ГАУ. 2016. № 3. 6 с.

7. Блинова А.Л. Рекомендации по разработке интегрированной системы менеджмента на основе системы менеджмента качества и системы экологического менеджмента // Перспективы развития пищевой промышленности и общественного питания: техника, технологии и управление качеством: материалы Национальной НТК. Федеральное агентство по рыболовству; Дальневосточный государственный технический рыбохозяйственный университет. Владивосток, 2023. С. 11-18.

RASHOYAN Irina Igorevna
Candidate of Technical Sciences, Associate Professor,
Tolyatti State University, Russia, Tolyatti

OCCUPATIONAL SAFETY, INDUSTRIAL, ENVIRONMENTAL AND FIRE SAFETY AS SUBSYSTEMS OF THE ORGANIZATION'S INTEGRATED SAFETY

Abstract. *The article shows the relevance of creating integrated security management systems in organizations (ISMS). The subsystems of fire and environmental safety, labor protection and industrial safety are the basis of the ISMS. A promising direction for the creation and improvement of the ISMS is shown. It is recommended to use the formation of an integrated management system (IMS) and corporate security culture, the introduction of an end-to-end methodology for risk assessment and management.*

Keywords: *integrated management system, occupational safety, industrial safety, environmental safety, fire safety.*

ВОЕННОЕ ДЕЛО

МЕКАМБАЕВ Бауыржан Абдумаминович
старший преподаватель, Институт сухопутных войск,
Университет военной безопасности и обороны Республики Узбекистан,
Республика Узбекистан, г. Чирчик

О СОВРЕМЕННОМ ЗНАЧЕНИИ ЦИФРОВИЗАЦИИ ВОЕННОГО ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Аннотация. *В статье описаны современные тенденции цифровизации военного образования, потенциал цифровых платформ и систем моделирования в подготовке офицерских кадров. Рассмотрены назначения, структура и функциональные возможности интегрированной цифровой платформы Synthetic Training Environment, реализуемой в вооружённых силах США. Особое внимание уделено значению STE для повышения эффективности подготовки командного состава, формирования профессиональных компетенций и развития адаптивных методов обучения в условиях современных военных и технологических вызовов.*

Ключевые слова: *цифровизация, военное образование, подготовка офицеров, моделирование и симуляция, интеграция, цифровая система, платформа, виртуальная реальность, эффективность.*

В условиях бурного развития информационно-коммуникационных технологий современная система военного образования переживает качественную трансформацию. Цифровизация учебного процесса становится неотъемлемым условием подготовки офицеров нового поколения, способных эффективно действовать в условиях динамичной, технологически насыщенной среды. Использование цифровых технологий – систем моделирования и симуляции, платформ искусственного интеллекта и виртуальной реальности – позволяет не только совершенствовать процесс обучения, но и формировать у курсантов стратегическое мышление, навыки анализа и принятия решений в сложных условиях обстановки.

Особое значение цифровые технологии приобретают в процессе интеграции образовательных программ с системами боевой подготовки и последующего анализа полученных результатов. Это обеспечивает единое информационное пространство, где теория и практика интегрируются посредством средств моделирования и симуляции, виртуальных тренажёров, цифровых полигонов и интеллектуальных обучающих систем. В результате создаются условия для непрерывного профессионального роста, индивидуализации обучения и повышения эффективности подготовки будущих офицеров, соответствующих требованиям современной армии.

Президентом Республики Узбекистан Ш. М. Мирзиёевым отмечено, что «в целях устойчивого развития мы должны глубоко освоить цифровые знания и информационные технологии, что даст нам возможность идти по самому короткому пути к достижению всестороннего прогресса. В современном мире цифровые технологии играют решающую роль во всех сферах» [1]. Кроме того, в 90 цели приложения 1 «Стратегия развития Нового Узбекистана на 2022–2026 годы» Указа Президентом Республики Узбекистан № УП-60 от 20 января 2022 года «О стратегии развития Нового Узбекистана на 2022–2026 годы» определено «Создание единой автоматизированной системы управления Вооруженных Сил, дальнейшее совершенствование цифровизации», «Создание единой информационно-коммуникационной системы и обеспечение информационной безопасности в Вооруженных Силах» [2].

Актуальность данной статьи состоит в рассмотрении возможностей цифровых платформ

и систем моделирования, обзоре предназначения, возможностей и состава интегрированной платформы цифровой системы обучения Synthetic Training Environment, реализуемой в вооруженных силах США.

В армиях развитых стран активно применяются цифровые, виртуальные и симуляционные учебные среды для подготовки офицерского состава. В вооруженных силах США в целях повышения уровня подготовленности офицерского состава активно применяются симуляторы для командно-штабной подготовки, виртуальные тренажёры, что позволяет отрабатывать вопросы выработки и принятия решений, без выхода в полевые условия [3]. В данное время в США реализуется проект Synthetic Training Environment (STE) – комплексная цифровая учебная среда, в состав которой включены непосредственные, виртуальные и конструктивные тренировки [4], а на базе полигона Yano Range (штат Кентукки) создаётся цифровой дозорный диапазон (Digital Air-Ground Integration Range, DAGIR): компьютеризированный тренировочный полигон с наземными и воздушными компонентами [5]. Развитию цифрового обучения – средств моделирования и симуляции боевых действий, виртуальной подготовки – также придаётся большое внимание в армиях России, Германии, Франции, Индии, Китая, Австралии, Бразилии и других стран.

Современное развитие цифровых технологий оказывает существенное влияние на систему военного образования, открывая новые возможности для повышения эффективности подготовки будущих офицеров. Интеграция цифровых средств обучения, симуляторов и виртуальных тренажёров позволяет формировать у курсантов не только теоретические знания, но и практические навыки управления войсками, принятия решений в условиях быстроменяющейся обстановки и работы с современными средствами автоматизации управления.

Использование цифровых платформ и систем моделирования способствует созданию интерактивной образовательной среды, где каждый обучающийся может работать в индивидуальном темпе и получать мгновенную обратную связь. Такие технологии позволяют воссоздавать реальные боевые и тактические сценарии без риска для личного состава и техники, что делает процесс подготовки более безопасным, гибким и экономичным.

Внедрение цифровых инструментов также усиливает аналитическую и исследовательскую составляющую военного образования. Офицеры нового поколения осваивают методы обработки данных, искусственный интеллект и технологии анализа больших массивов информации, что становится важнейшей компетенцией для управления войсками в условиях современной войны и гибридных угроз.

Рассматривая частно проект Synthetic Training Environment (STE), важно отметить, что он направлен на создание единой цифровой системы обучения, объединяющей реальные, виртуальные и конструктивные тренировки. Его цель – полностью заменить разрозненные симуляционные системы (OneSAF, JCATS, VBS3 и др.) на интегрированную платформу нового поколения. С 2021 года Synthetic Training Environmentвнедряется поэтапно на военных базах – Fort Benning, Fort Campbell, Fort Hood, а полный ввод в эксплуатацию ожидается к 2027 году.

Основной идеей проекта является обеспечение «единого цифрового поля боя», где офицеры и военнослужащие будут тренироваться в условиях, максимально приближенных к реальным боевым сценариям (рис. 1). Платформа объединяет тренировки на реальных полигонах с датчиками и цифровыми метками, обучение в VR/AR-средах (танки, БТР, вертолёты, штабные операции), а также командно-штабные учения, моделируемые ИИ и симуляторами.

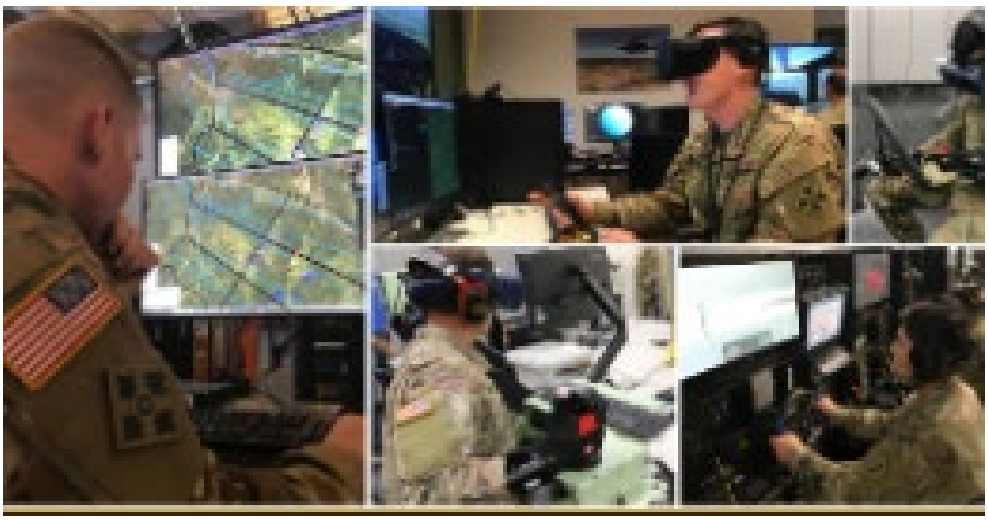

Рис. 1. Подготовка военнослужащих на базе платформы Synthetic Training Environment

Ключевыми компонентами интегрированной платформы цифровой системы обучения являются:

- One World Terrain (OWT) – создание трёхмерной карты Земли на основе спутниковых и дрон-данных, чтобы моделировать любой район мира;
- TrainingSimulation Software (TSS) – ядро, объединяющее все типы тренировок;
- Training Management Tool (TMT) – инструмент для планирования и анализа обучения, даёт инструкторам возможность контролировать сценарии и отслеживать прогресс обучаемых;
- Cloud-based STE Architecture – облачная архитектура, позволяющая подключать военные базы и учебные центры по всему миру.

Заслуживающими внимания качествами данной интегрированной платформы цифровой системы обучения, кроме использования для обучения принятию решений в реальном времени с применением искусственного интеллекта и аналитики, экономии ресурсов, является возможность моделирования сложные операции офицерами штабов на любом уровне – от индивидуальной подготовки (подготовки экипажей) (рис. 2) до межвидовых командных тренировок.

Рис. 2. Индивидуальная подготовка военнослужащего и экипажа

Цифровой полигон проекта Synthetic Training Environment состоит из нескольких типов учебных модулей, которые связаны в единую сеть. Каждая модуль отвечает за отдельный уровень подготовки – от индивидуальной до штабной. В нижеследующей таблице показаны назначение основных модулей.

Таблица

Основные учебные модули проекта Synthetic Training Environment

Название учебного модуля и уровень подготовки	Краткое описание и назначение	Выполняемые задачи
Training and Simulation Center (TSC)	Центральный командно-учебный центр на базе крупных военных гарнизонов (например, Fort Benning, Fort Hood). Здесь размещаются серверы, аналитика, инструкторы и управление всеми локальными тренингами.	
Soldier Virtual Trainer (SVT) *Индивидуальный*	Индивидуальные VR-станции, где военнослужащие и курсанты отрабатывают навыки стрельбы, ориентации, взаимодействия в отделении. Оснащены шлемами VR, системами обратной связи и датчиками оружия.	Тактические навыки, огневая и инженерная подготовка
Squad Immersive Virtual Trainer (SIVT) *Индивидуальный*	Цифровая капсула/комната для обучения отделения или взвода в полном виртуальном окружении – бой в городе, патруль, зачистка зданий и т. п.	
Synthetic Collective Trainer (SCT) *Малые подразделения*	Средний уровень – взаимодействие рот, батальонов, штабов. Используется для тренировки офицеров среднего звена (командиров рот, штабных офицеров). Поддерживает связь с реальными полигонами (Live).	Взаимодействие взвода/роты, командование, связь
Live Training Environment (LTE) *Малые подразделения*	Цифровое оснащение реальных полигонов. Военнослужащие с датчиками на экипировке, оружии и технике; все данные передаются в систему STE для анализа действий.	
Integrated Training Facility (ITF) *Штабной/стратегический*	Объединённый комплекс, где проходят учения с комбинированием Live-, Virtual- и Constructive-элементов. Например, часть подразделений действует на реальном полигоне, а другая – в цифровом пространстве.	Планирование операций, анализ решений, межвидовое взаимодействие
Mission Command Training Center (MCTC) *Штабной/стратегический*	Учебная точка для офицеров и штабов. Используется для командно-штабных игр, анализа решений, моделирования операций на уровне бригады или дивизии.	
Home Station Training Node (HSTN)	Мобильный или стационарный модуль на базе воинской части, позволяющий проводить занятия без выезда в главный центр. Подключён к облаку STE.	

Все модули объединены через облачную сеть STE Cloud и Common Synthetic Environment (CSE), где каждый участник (курсант, офицер, штаб) работает в едином цифровом пространстве, где данные синхронизируются в реальном времени, а результаты обучения (видео, телеметрия, карта действий) автоматически передаются в Training Management Tool (TMT) для анализа.

Исходя из вышеуказанного, можно сделать вывод, что современные цифровые полигоны становятся ключевым элементом подготовки курсантов и офицеров, обеспечивая переход от традиционных методов обучения к интегрированным, моделируемым и интерактивным формам военной подготовки. Использование симуляционных технологий, виртуальной и дополненной реальности позволяет воспроизводить сложные боевые сценарии в безопасной и контролируемой среде, где обучающиеся могут совершенствовать тактическое мышление, навыки управления подразделениями и принятие решений в условиях неопределённости.

Внедрение цифровых полигонов в образовательный процесс способствует повышению эффективности боевой и штабной подготовки,

сокращает материальные затраты и временные ресурсы, а также обеспечивает непрерывную адаптацию учебных программ к реалиям современных конфликтов. Таким образом, цифровые полигоны выступают важным инструментом формирования профессиональных компетенций будущих офицеров, способных действовать в условиях информационно-сетевых войн и высокотехнологичной боевой среды.

Литература

1. Подготовка кадров в эпоху цифровизации: современные стандарты и новые решения. Газета Правда востока № 98 (29868) от 18 мая 2022 года.

2. Указ Президента Республики Узбекистан № УП-60 от 20 января 2022 года «О стратегии развития Нового Узбекистана на 2022–2026 годы». Режим доступа: https://lex.uz/ru/docs/5841077. Дата обращения – 09.11.2025 г.

3. Training Solutions For Land Forces. Режим доступа: https://www.cae.com/media/documents/Defence_Security/Training_Solutions_For_Land_Forces.pdf. Дата обращения – 09.11.2025 г.

4. Военное моделирование и виртуальное обучение – глобальный стратегический бизнес-отчёт. Режим доступа: https://www.researchandmarkets.com/reports/6110292/military-simulation-virtual-training-global. Дата обращения – 09.11.2025 г.

5. Simulation and Training – Recent World News. Режим доступа: https://www.raes-fsg.org.uk/directdocs/2019-09-20World_Sim_News.pdf. Дата обращения – 09.11.2025 г.

MEKAMBAYEV Bauyrzhan Abdumaminovich
Senior Lecturer, Institute of Land Forces,
University of Military Security and Defense of the Republic of Uzbekistan,
Republic of Uzbekistan, Chirchik

ON THE MODERN SIGNIFICANCE OF DIGITALIZATION OF THE MILITARY EDUCATIONAL PROCESS

Abstract. *The article describes current trends in the digitalization of military education, the potential of digital platforms and modeling systems in officer training. The purpose, structure and functionality of the integrated Synthetic Training Environment digital platform implemented in the US armed Forces are considered. Special attention is paid to the importance of STE for improving the effectiveness of command staff training, the formation of professional competencies and the development of adaptive teaching methods in the context of modern military and technological challenges.*

Keywords: *digitalization, military education, officer training, modeling and simulation, integration, digital system, platform, virtual reality, efficiency.*

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Majd S. Ahmed
Department of Computer Science, College of Science, Mustansiriyah University, Iraq, Baghdad

EXPLORING THE IMPACT OF INTERNET OF THINGS ON MODERN SOCIETY

Abstract. *We are living proof of the hyper connected society's expansion. In the foreseeable future, this new cyber era will continue to benefit from the Internet of Things. Communication paradigms have changed from being device-centric to people knowledge-focused. In the future, real, virtual, and knowledge domains can converge thanks to the availability of real-time information about the physical world made possible by machine-to-machine solutions and the Internet of Things. The next generation of Internet protocols is characterized by this connectedness. With the help of a technology like the Internet of Things, which alters how. Individuals, systems, and gadgets interact, it will be feasible to offer solutions for the advancement of various domains that have been waiting for it. When we speak of "things," we mean actual physical objects that exist in our environment. These things are capable of performing functions and interacting with both their surroundings and one another. They can therefore make choices much more complex than just choosing to live. We are not, however, talking about more layers. Before the Internet of Things (IoT), for example, efforts such as the integration of mobile phones into reliable surroundings were made possible. By introducing cyber-physical systems, the Internet of Things allows real things to adapt to changes in their surroundings and exhibit a variety of behaviors.*

Keywords: *Internet of things 'IOT', attacks and threads, experiments.*

1. Introduction

Internet of Things technologies show tremendous promise in enhancing quality of life for many. Significant innovations and advances are helping to propel the development of novel IoT systems. Cheap and readily available hardware components are crucial to ensuring continuous adoption of these exciting networks.

Creating operating systems that support both existing and emerging IoT devices while aligning with current communication standards and best practices will help guide future progress. However, enabling interoperability between diverse operating systems in a way that accommodates heterogeneous deployment scenarios is critical for widespread adoption [1].

IoT infrastructures must intelligently adapt to changing network conditions to achieve their full potential. In this survey, we explore the landscape of existing IoT operating systems and evolving hardware options. We also consider promising directions for ongoing research. Several peer-reviewed studies on IoT operating system management are discussed in relation to opportunities, barriers, and potential remedies. Network capabilities, deployment flexibility, and support for diverse IoT applications are some of the key factors to be addressed. Finally, our conclusions and recommendations aim to inform continued advancement of versatile, scalable, and user-friendly IoT platforms. The internet of things is at the center of the technological transformation. Combining unified technology is challenging. The 5th era of smart Internet of Things, operating systems, communication via the air, liaison from device to device, modern cellular networks, and Internet of Things resources are examples of current "millimeter wave" innovations. The next generation of the Internet of Things is made possible by research. The affordability and progress of Internet of Things technology have led to a rise in long-range connectivity and device accessibility [1].

2. Operational mechanisms and features

Establishing links with other devices to enable information exchange is the aim of Internet of Things devices. Developers may design and deploy the Internet of Things by joining networks of sensors thanks to IOT platforms. Taking seriously the raised areas and materials involved in contrasting the different Internet of Things communication protocols, such as Message Queue Telemetry Transport. Many research studies were conducted

to support Internet of Things applications using various protocols [2].

Data from sensor readings acquired without the usage of Internet of Things platforms was analyzed for four distinct protocols. Finding the amount and contributing causes to latency was the main goal of the investigation. Researchers employed several of these platforms for specialized implementations, relying on the 'Message Queue Telemetry Transport' protocol and pre-built hardware kits.

The researchers did not use Internet of Things operating systems in their past medical and healthcare solutions. Portable processors with a non-current operating system provide a broad platform [2].

The present Internet of Things is strongly interconnected with current cyber and physical systems. Recent IOT systems could be described as a broadly networked network with nodes that can be controlled and linked remotely. Our focus will be on current IoT advancements and security challenges. Providing security in modern times. The Internet of Things has additional challenges compared to traditional systems due to existing limitations.

Our goal is to showcase the security properties, limitations, and risks associated with contemporary Internet of Things technology, as well as security solutions tailored to these critical safety concerns. While there has been research on privacy and protection in IoT systems, The figure 1 shows Internet of things, there has been no comprehensive discussion of security recently [3].

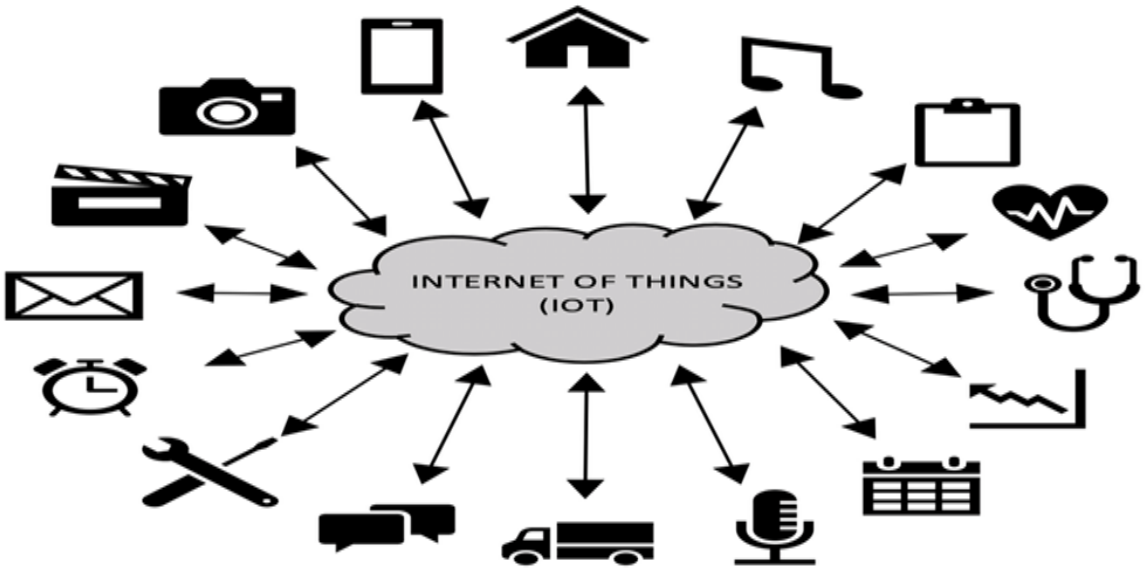

Fig. 1. The figure shows Internet of things

3. Safety requirements and resource limitations

Recent IOTs devices, such as sensors, controllers, and self-driving vehicles, have limited resources and need power tasks accomplished in milliseconds. These devices also require time-based qualities, which are represented by deadlines. The system's value determines the worth of the outcomes produced by missing a specific deadline. If the value decreases rapidly, the system is called hard, such as nuclear power plants or antilock braking systems; if it declines gradually, it is considered soft, such as streaming multimedia or automated glass wipers.

Properties of the majority of recent Internet of Things nodes

The growing popularity of the Internet of Things (IoT) necessitates the use of power efficient nodes capable of connecting to real-world devices. While some devices may communicate wirelessly without requiring electricity, IoT nodes embedded in physical objects require a protocol that is particularly designed to overcome their intrinsic restrictions. These nodes must meet a number of special requirements, including low-power design, cost efficiency, and restricted memory capacity. As a result, low-power, low-cost IoT nodes running over a wide communication range are relatively prevalent [4].

4. Telecommunications traffic is merged

Classic current time systems often consist of numerous nodes operating independently, with limited communication and capabilities. The Internet of Things connects cyber and physical nodes through industrial communication networks, which typically interact via the internet. Current applications need triggering events based on specific information. A reliable communication

connection with required service quality, quantity, and data processing requirements is crucial for allowing these applications [5].

The Internet of Things now includes traffic with varied levels of timeliness, availability, and capacity, making it more versatile. Priority traffic for secure and precise system operation, including sensors for closed-circuit control and real-time control orders in avionics, automobiles, and home security. Moderate priority traffic, such as airliners navigation systems, power substation system monitoring, electric vehicle-charging station communication messages, heating, water sprayers in stations, air conditioning, lighting devices, food cooking machines, etc., is essential for proper system operation but has some delays, tolerances, drops, etc. [6]. Traffic that does not rely on network towers for wireless connection is considered low priority in the system. Examples of such traffic include engineering activity power substations, multimedia content transmission in airplanes, and alerts exchanged between smart equipment within home premises. These towers provide mobile communication and data transfer across wide geographic areas, allowing them to efficiently address the various demands of different businesses and sectors. In reality, these network towers play an essential role in maintaining uninterrupted communication, which is critical for the unrestricted and flawless operation of many sectors [7].

5. Modern Techniques

The idea of combining newer and current data sets may not seem unique. In 2004, the term 'edge computing' was coined to describe a system that sends program instructions and associated information to the network's edge for increased efficiency and performance. In 2009, the notion of virtualizing computer resources in the Wi-Fi subsystem was introduced. The interest in moving computing resources to the network's edge emerged following the advent of 'fog computing' for the Internet of Things. Academics have used many terms to describe 'fog computing', including 'edge computing'.

This word, 'edge computing', was invented by the designer of cloudlets, who considered the usage of virtual computers. Cloudlets were originally created to act as a replacement for remote mobile apps that were previously hosted on faraway clouds. The major reason for the development of cloudlets was to allow apps to offload computationally heavy activities to local virtual machines on the same Wi-Fi network. Recent research and investigations have shown that fog computing is an essential component of the larger domain of 'edge computing'. Fog computing refers to the use of the cloud to complete network gateways, with cloudlets being an appropriate option when nearby server devices are available. Other publications cover 'Edge Computing of Multiple Accesses', a standard created by the European Institute of Standards and Telecommunications. This standard outlines how telecommunications carriers deliver virtualization-based computing services to customers using a programming application interface. Commercial equipment already incorporates the Internet of Things, edge computing, and fog computing. The current partnership between "Open Fog" and the European Institute of Standards of Telecommunications, however, disproves the notion that "edge computing of multiple accesses" is just another term for "fog." The 'Edge Computing of Different Obtains' strategy can help accelerate the introduction of 'fog computing'. Many studies refer to 'edge computing of multiple accesses' as a synonym for 'fog computing'. The European Institute of Standards of Telecommunications introduced 'Edge Computing of Multiple Accesses' as a telecommunications standard. It specifies the interface of programming applications for telecom companies to provide virtualized computing services to their clients based on expansion [8], Internet of Things A to Z: Technologies and Applications. John Wiley & Sons, United States, 113-124). Previously, 'fog' was also called mist computing'. Recent articles classify mist as a subcategory of fog. Mist emphasized the necessity to expand computer capabilities to the Internet of Things 'extreme edge'. Positioning devices can minimize communication latency between Internet of Things devices to milliseconds [9].

Essentially, the goal of 'mist computing' is to provide Internet of Things objects with the ability to identify themselves in terms of self-organization, self-management, and various self-means. As a consequence, Internet of Things devices will be able to operate continuously even if their internet connection is intermittent. Generally speaking, "mist" devices may sound similar to stationary or mobile web services, where application services are embedded into various low-resource devices, including sensors, actuators, and cell phones. However, 'mist' is concerned with self- recognition and condition awareness, enabling the remote distribution of dynamic software code to diverse devices based on state and environment changes. Similar to 'fog', it provides a foundation for flexible reconfiguration and program deployment [9].

Understanding that the 'fog' requires support from all of the connected technologies of 'edge computing' indicates that no one is capable of installing and regulating 'fog' without integrating the technologies of 'edge computing'.

6. Security assaults and risks for the recent Internet of Things

Recent Internet of Things systems face a range of threats, depending on the adversary's goals and technology. In a system constructed using a vendor model, one of the contributing vendors may be malignant. That possible untrustworthy vendor may incorporate a number of malicious functions into the system's responsibilities.

Furthermore, even if the contributing vendors are not malevolent, improper coding approaches may cause difficulties. In a networked system, the opponent may target the communication interfaces. Because most of these technologies lacked authentication, communication channels were easily fabricated and intercepted.

The methods of attacks on recent time strategy are classified depending on the control over computer processes and the functional purpose of the attack. Only one way to get control of a target system is to inject a malicious virus or malware or to utilize lawful code for nefarious objectives. Furthermore, because nodes in the modern Internet of Things can communicate across untrusted channels such as the internet, the system is vulnerable to network attacks [10].

Aside from the repeated tests of forcefully crashing the system, as part of the assaults on the subset channels, the adversary may surreptitiously connect to the system and get sensitive data. Attacks against subset channels rely on determining system characteristics such as memory use patterns, task scheduling, power consumption, and so on. That information might be used later by the attackers to launch new attacks. We will highlight the most prevalent attacks on modern IoT systems:

An integrity violation occurs when malicious code is introduced. A competent adversary is capable of gaining a position in the system.

For example, an adversary may introduce a malicious job that respects the system's recent promises in order to avoid discovery and harm one or more current recent works. The attacker may utilize that task to control sensors and alter the system's behavior in an undesirable way [10]. The loss of integrity via code injection attacks comprises transferring portions of instruction to a device, which are saved in memory by the receiving application. The attacker then manipulates unknown channels, such as subset channels, to make the victim more vulnerable in order to extract sensitive information from them. Because recent time tasks are executed by nodes in the Recent Time Internet of Things (RT IoT), these attacks are particularly effective against these systems due to their predictable behavior. The hackers get access to temperature, memory, power consumption, and time management likes and dislikes, which allows them to collect crucial information. The Internet of Things (IoT) is a valuable communication channel, but it also raises privacy and security concerns. Interference, falsification, and disruption of control and information flows are examples of communication threats.

Protecting against these risks is tough since it is difficult to distinguish between illegal and lawful communication traffic without sacrificing service quality [11].

Cryptographic protection measures are frequently employed to tackle communication risks; however, this might raise the engineering technology of wireless communication and necessitate scheduling changes. Cryptography procedures are extremely costly and constrained, particularly for stationary devices in the IoT.

Therefore, tackling these risks is critical for the security and privacy of IoT systems. Cryptography may not be the best solution for many Internets of Things (IoT) applications owing to resource constraints and severe timing constraints. A method for incorporating security features without changing existing jobs is offered. Nodes in IoT networks are vulnerable to service denial attacks, in which attackers manipulate recent tasks and deplete system resources. Distributed service denial attacks include a large number of rogue nodes targeting devices at the same time, especially when substantial activities are scheduled. This can compromise system integrity and privacy, especially when crucial processes are scheduled to start. Implementing security measures without disrupting existing functions is crucial for IoT devices. The current processes for defending general information technology or permanent systems do not account for the timeliness, resource restrictions, and safety of the Internet of Things. These procedures require considerable revisions to be adaptive. Our recent efforts may be unified to protect against service denial attacks.

To be effective, attackers must conduct investigations and plan their attacks. We will explain this as follows:

7. Strategies to defend against assaults on the modern Internet of Things

These approaches are often classified into two main categories:

1. Solutions that require specific hardware support to provide security.

2. Software-level solutions that require no adjustments.

The first step is to defend yourself with hardware.

The 'Simplex' construction allows for protection without compromising system safety. The term "simplex" refers to a popular current time structure. When a sophisticated controller with excellent performance is not available or isn't working correctly, a simple safety controller is used in its place [12].

The 'Simplex' approach attempts to guarantee that a system is safe even when it is controlled by a sophisticated controller.

Using a 'Simplex' structure for protection involves monitoring attributes including time, memory access, system call traces, and abnormalities. of an unreliable entity that is tasked with more complex tasks and vulnerable to less secure media, including networks, input and output channels, the internet, etc. Furthermore, although architectural modifications can enhance the security posture of Internet of Things nodes, they might not be appropriate for systems that employ connection-oriented transport components [12].

We will discuss several recently proposed approaches to enhance Internet of Things security without requiring hardware support:

To combat subset channel attacks, attackers can use timed attacks to estimate memory allocation behavior. Recent systems lack separation of distributed resources among diverse tasks, causing this issue [13]. The Internet of Things is based on a connection-focused transport service.

When the system transitions between jobs, there is some overlap. Understanding the constraints of safeguarding between jobs is crucial for preventing assaults on specific channels. Integrating security, the Internet of Things is being promoted through techniques that limit the number of jobs scheduled, implementing high-priority scheduling tools. The scheduler clears the distributed cache when switching from a project with high protection, which demands greater privacy, to a process with low protection, which is unprotected and largely harmed [13].

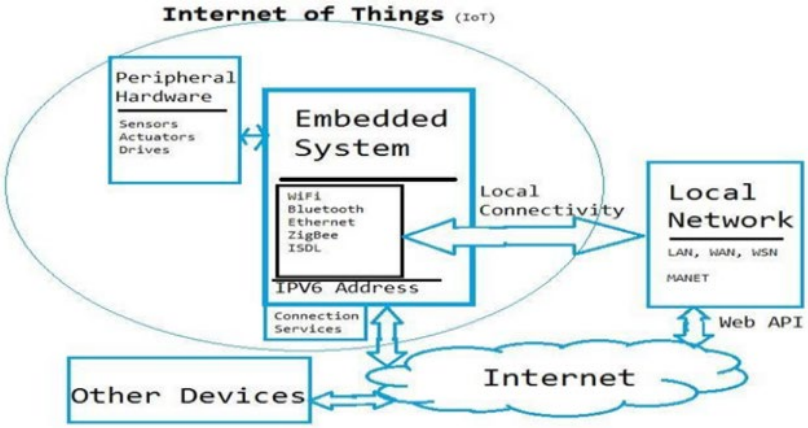

Fig. 2. A 'Simplex' structure for protection involves monitoring attributes including time, memory access, system call traces, and abnormalities

8. Suggested Use of the Internet of Things Platform

We created apps that include modern operating system features. Sensors, actuators, and communication modules make up the hardware layer. The Internet of Things system requires the following future sub-systems to be built:

The Internet of Things server, which makes it easier for nodes to communicate with one another;

The prototyping platform, which makes it possible to create Internet of Things nodes;

The structure describes data exchange procedures, while the communication protocol governs message flow between Internet of Things nodes and the recent time server.

The suggested system offers dependable connections for a wide range of smart Internet of Things applications. The proposed Internet of Things platform utilizes the 'ARM Cortex-M4' processor, which is both energy-efficient and reliable. A smart phone is recommended as the Internet of Things node. The proposed architecture consists of critical servers and nodes for the Internet of

Things. The key server facilitates communication between system nodes over the internet [13].

The system's proposed nodes are classified into four primary categories:

'Sensor' nodes detect their environment.

'Actuator' nodes that have an effect on their surroundings.

'Hybrid' nodes that perceive and influence their environment.

Nodes designated as 'monitoring'.

The figure 3, depicts the potential structure of the system of the Internet of Things.

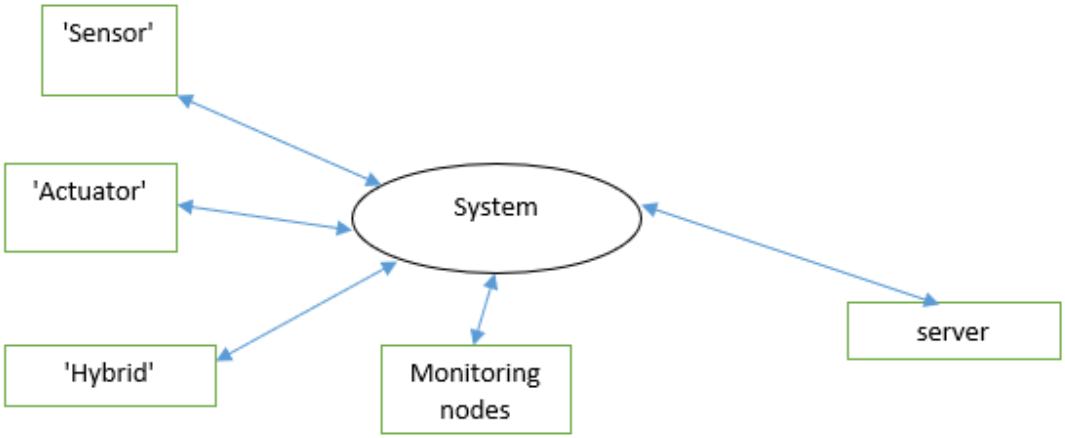

Fig. 3. Depicts the potential structure of the system of the Internet of Things

Below is a detailed explanation of the suggested system.

9. Suggested for IoT nodes

The proposed model is implemented using a "Nucleo Board" that uses the processor of the "ARM Cortex-M4"; this processor is specifically designed for great performance, low-power consumption, and low device prices, making it appropriate for the nodes of the Internet of Things. The suggested platform is a fixed system that could be designated for any controller types that meet the requirements of the system; it was developed, implemented, and successfully operated in the experiments. All nodes are made up of a few basic components, including a management unit that handles the node's duties, Wi-Fi hardware that enables wireless internet connectivity, sensors that collect data from the environment, and actuators that respond to this data [14].

System nodes are classified as 'Sensor', 'Actuator', 'Hybrid', and 'Monitoring' based on their connection to the key server. The 'Sensor' nodes perceive their surroundings and provide information to the server at regular intervals. These nodes have sensors but not actuators. The 'Actuator' nodes, with one or more actuators but no sensors, respond to monitoring node instructions and alter their environment [14].

The 'Hybrid' nodes integrate the capability of both actuator and sensor nodes. These nodes have both actuators and sensors. They interact with the Internet of Things server, send sensor data, and gather commands from monitoring nodes. The monitor nodes might be smartphones that regulate and monitor the system nodes. These nodes operate actuators and monitor sensor readings by issuing instructions and processing data, but do not include sensors or actuators themselves.

10. Server for Internet of things

The server is a crucial system component that enables communication between all nodes. It communicates with several nodes and provides monitoring nodes with sensor data [14].

Once a sensor node is recognized as a 'Sensor', the server sends data to registered monitors. Orders from monitoring nodes are sent to an actuator node by the server if it also serves as a monitoring node. The tasks of both nodes are managed by the server if a "hybrid" node doubles as a "monitoring" node. Orders are received, and sensor data is transmitted by the monitoring node [15].

The figure 4 depicts the flow of data over the server of the Internet of Things.

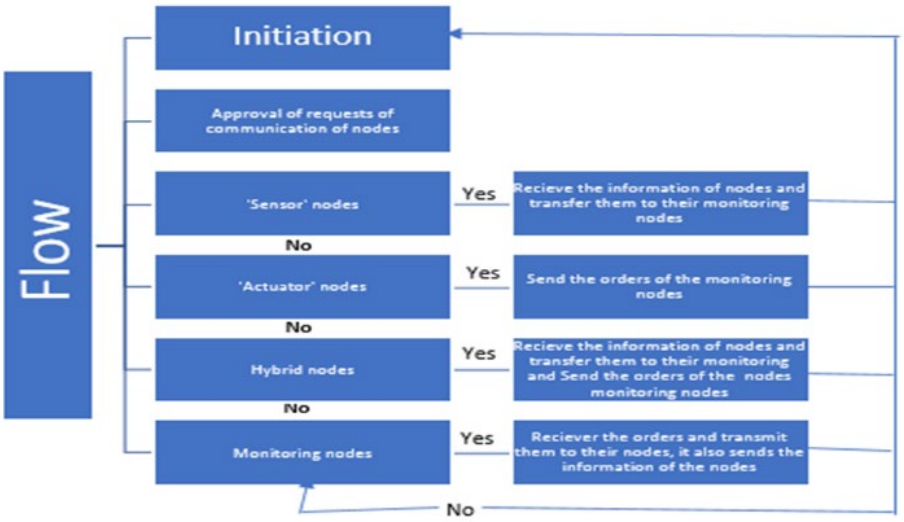

Fig. 4. Flow of data over the server of the Internet of Things

11. Suggested Communication Protocol

To accomplish these tasks, the system's nodes must communicate with one another through the key server. Each node connects to the key server by sending its identification and amount, and it waits for the server's acknowledgement before connecting to another node in the system.

The 'Sensor' node identifies itself and sends periodic information. The 'Actuator' node receives orders from the 'Monitoring' nodes via the key server. The 'Hybrid' node combines the functions of both the actuator and sensor nodes. After proof of identity, the 'Monitoring' node registers to receive data from specific sensor nodes and deliver instructions to defined actuator nodes.

Nodes communicate with the server by attempting to identify themselves and join.

Once acknowledged, they can successfully communicate with each other.

12. Establishment of the Test

Experiments are conducted to evaluate the effectiveness of the proposed communication technique and the 'Sending a message Queuing Telemetry Transport' protocol. Network settings are established to determine their impact on protocol performance [16].

The performance metrics assessed include the number of seconds of delay and the amount of data transferred per successfully sent message. The delay period refers to the time between message publication and server acknowledgement.

The setup consists of three machines: a laptop running a wide-area network emulator to simulate channel losses and communication delays, a personal computer serving as a server to facilitate communication between platforms, and a second laptop serving as a node for message publishing and acknowledgement. The server supports both protocols. A wide-area network emulation machine is used to send the messages to the server after the node publishes them. The node receives the server's acknowledgement via the emulation machine.

13. The experiment's outcomes

In the experiment with one node and one server, the two protocols were able to send their messages without worrying about the proportion of loss applied, indicating shows the two protocols have a suitable approach for message delivery when working with There are different rates of loss, therefore performance evaluations for message delay and the total quantity of data delivered for each message that was successfully sent. We created a safe method for digitally signing documents and certificates (MD5) utilizing the message digesting process.

Signatures for digital integrity and authentication documents [17, p. 50-55].

This article examines methods based on encoding time, decoding time, SMS size, power consumption, and throughput using a series of tests. The proposed strategy outperforms the comparison method, according to the results [18, p. 56-63].

Message latency is a crucial statistic, especially in modern systems where time is a key factor. Message delays can be attributed to loss rates and the need for retransmission. The 'Message Queuing Telemetry Transport' (MQTT) protocol with a specific service quality is compared to a communication protocol with a particular level of acknowledgment for comparable messages [16].

'Message Queuing Telemetry Transport' has a reduced packet size compared to the selected protocol, resulting in decreased message delay. See the figure 5.

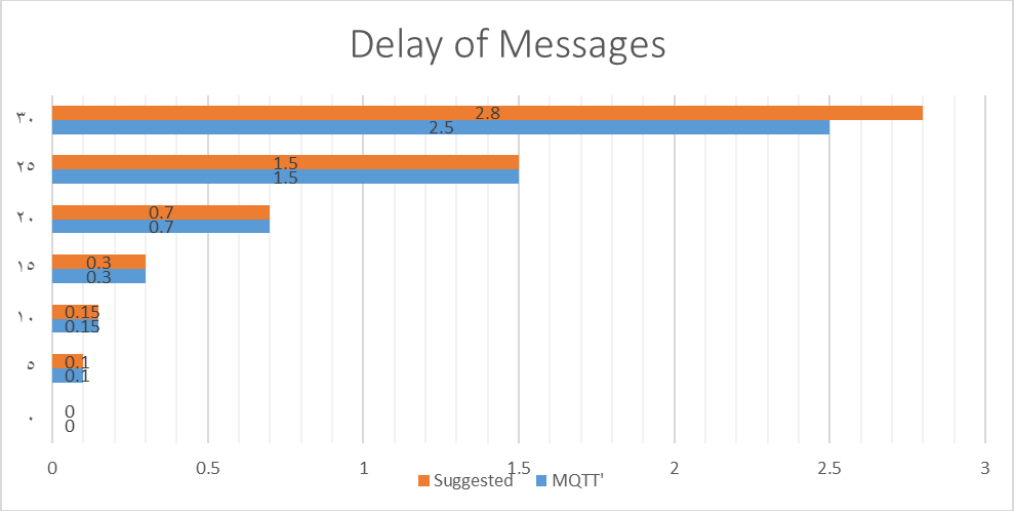

Fig. 5. 'Message Queuing Telemetry Transport' has a reduced packet size compared to the selected protocol, resulting in decreased message delay

14. Conclusions

The proliferation of smart gadgets such as cameras and home automation systems has resulted in the establishment of the 'Internet of Things', which connects previously disconnected objects and applications. However, the intricacy of assaults on these systems needs a reassessment of protective measures. This study intends to promote knowledge on modern time protection and to fill gaps in present protection systems.

The proposed approaches include hardware-assisted protection and no-adjustment protection. The study created an Internet of Things framework that acknowledges the intimate relationship between the past and the future.

15. Recommendations

I support merging Internet of Things systems into new technology. I recommend integrating Internet of Things systems with other technologies and expanding them use as they enable wireless data transmission across devices.

Furthermore, I support developing fresh approaches to protecting the privacy and security of Internet of Things data, as well as guarding against hacking and attacks; expanding safety resources is also essential.

Since I think my suggested model might be used for further study and discussion, I strongly advise paying attention to it. One can never obtain enough information on the enormous subject of the Internet of Things.

References

1. Al-Turjman F. Artificial intelligence in IoT, vol. 13. Berlin: Springer, 2019.
2. McEwen A., Cassimally H. Designing the internet of things. John Wiley & Sons, 2013.
3. Brooks T.T. Cyber-assurance for the Internet of Things. John Wiley & Sons, 2016.
4. Waher P. Mastering Internet of Things: Design and create your own IoT applications using Raspberry Pi 3. Packt Publishing Ltd, 2018.
5. Vermesan O., Friess P. Internet of things: converging technologies for smart environments and integrated ecosystems. River publishers, 2013.
6. Qiu M. Smart Computing and Communication, Springer Science & Business Media. Berlin, 2018.
7. Zitouni R., Agueh M. Emerging Technologies for Developing Countries, Springer Science & Business Media, 2018.
8. Hassan Q.F. Internet of things A to Z: technologies and applications. John Wiley & Sons, 2018.
9. Buyya R., Srirama S.N. Fog and edge computing: principles and paradigms. John Wiley & Sons, 2019.
10. Li S., Da Xu L. Securing the internet of things. Syngress, 2017.
11. Hu F. Security and Privacy in Internet of Things (IoTs). United States.
12. Gilchrist A. IoT Security Issues. Berlin, 2017.
13. Cheruvu S., Kumar A., Smith N., Wheeler D.M. Demystifying internet of things security: successful iot device/edge and platform security deployment. Springer Nature, 2020.
14. Kantarci B., Oktug S.F. Wireless Sensor and Actuator Networks for Smart Cities, 2018, MDPI.
15. Park H., Shen J., Sung H., Tian Y. Parallel and Distributed Computing. Berlin, Germany: Springer Science & Business Media.

16. González García C., García-Díaz V., García-Bustelo B., Lovelle J.M.C. Protocols and Applications for the Industrial Internet of Things. IGI Global, 2018.

17. Albahadily H.K., Jabbar I.A., Altaay A.A., Ren X. Issuing digital signatures for integrity and authentication of digital documents, Al-Mustansiriyah Journal of Science, Vol. 34, No. 3, P. 50-55, 2023.

18. Salman Z.W., Mohammed H.I., Enad A.M. SMS Security by Elliptic Curve and Chaotic Encryption Algorithms, Al-Mustansiriyah Journal of Science, Vol. 34, No. 3, P. 56-63, 2023.

ЖЕРЛИЦЫНА Юлия Викторовна
методист, Белгородский институт развития образования, Россия, г. Белгород

ПРИХОДЬКО Надежда Анатольевна
методист, Белгородский институт развития образования, Россия, г. Белгород

ВЕРТЕЛЕЦКАЯ Ольга Владимировна
заведующая, Белгородский институт развития образования, Россия, г. Белгород

ЦИФРОВАЯ БЕЗОПАСНОСТЬ В ОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЯХ: МЕТОДЫ ФОРМИРОВАНИЯ НАВЫКОВ БЕЗОПАСНОГО ИНТЕРНЕТ-ПОВЕДЕНИЯ У ШКОЛЬНИКОВ

Аннотация. *В статье рассматривается государственная политика в сфере информационной защиты детей, рассматриваются основные рекомендации по обеспечению информационной безопасности детей.*

Ключевые слова: *интернет-безопасность, информационная защита детей, цифровая среда.*

В современном мире обеспечение безопасного интернет-пространства для детей становится приоритетом государственной политики. В эпоху цифровых технологий, когда каждый ребёнок способен пользоваться сетью с ранних лет, государство берёт на себя ответственность за формирование условий, обеспечивающих надёжную защиту от информационных угроз и сохранение психического и физического здоровья учащихся. Это направление охватывает не только профилактические меры, но и развитие навыков цифровой гигиены, что актуально для формирования устойчивой и безопасной образовательной среды.

Сегодняшнее детство невозможно представить без активного взаимодействия с цифровыми технологиями и интернетом. Государственная политика Российской Федерации направлена на защиту прав детей в информационной сфере, что реализуется через комплекс нормативных актов.

Федеральный закон от 03.07.1998 г. № 124-ФЗ «Об основных гарантиях прав ребёнка в Российской Федерации» закрепляет фундаментальные права детей на защиту информации, в частности ограждает от вредного цифрового контента, который может нанести физический или психический вред. Документ вводит обязательства государства и образовательных учреждений по обеспечению безопасного интернет-пространства для школьников. Внедрение соответствующих мероприятий и контроль их соблюдения в школах становится одним из ключевых механизмов реализации этого закона, что способствует созданию надежной системы поддержки и защиты учащихся.

Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» определяет конкретные меры защиты детей от вредной информации, распространяющейся через средства массовой информации и интернет. Основные положения включают установление критериев определения вредного контента, запретов на его распространение среди несовершеннолетних, а также правовые механизмы ответственности нарушителей. Это законодательство формирует правовую основу для предотвращения доступа детей к опасной информации, укрепляя системный подход к цифровой безопасности.

Приказ Министерства связи и массовых коммуникаций от 16.06.2014 г. № 161 «Об утверждении требований к административным и организационным мерам, техническим и программно-аппаратным средствам защиты детей то информации, причиняющей вред их здоровью и (или) развитию» определил поэтапное внедрение комплексных мер по информзащите детей. Сначала разработаны технические стандарты фильтрации контента, затем – методические рекомендации для образовательных учреждений. Следующий этап включал интеграцию этих мер в школьные образовательные процессы, а финальный заключительный этап посвящен мониторингу эффективности и

регулярному обновлению технологий. Такой системный подход помогает последовательно укреплять безопасность детей в цифровом пространстве.

Концепция информационной безопасности детей, утверждённая распоряжением Правительства Российской Федерации от 02 декабря 2015 г. № 2471-р служит стратегическим документом, формулирующим цели защиты детей в информационном пространстве. Она направлена на профилактику и минимизацию влияния вредной информации, а также развитие цифровой грамотности среди школьников. В частности, концепция предусматривает совершенствование образовательных методик, обучающих детей безопасному поведению в интернете, и координацию усилий государственных структур, школ и общества. Это обеспечивает целостный и интегрированный подход к обеспечению детской цифровой безопасности.

Этот системный нормативный базис обеспечивает комплексную защиту и развитие навыков цифровой безопасности у детей, способствуя формированию ответственного и безопасного поведения в сети.

Наблюдается устойчивый рост времени, проводимого школьниками в интернете, включая активность в социальных сетях, что создает новые вызовы в сфере цифровой безопасности. Такое усиление зависимости от цифрового контента требует немедленного внедрения образовательных программ и технических решений для формирования у детей навыков безопасного и осознанного использования онлайн-ресурсов. Растущие риски, связанные с распространением дезинформации и вредоносного контента, требуют системного подхода к профилактике и обучению.

Динамика интернет-активности детей в России (2022–2025) представлена на графике ниже (рис. 1).

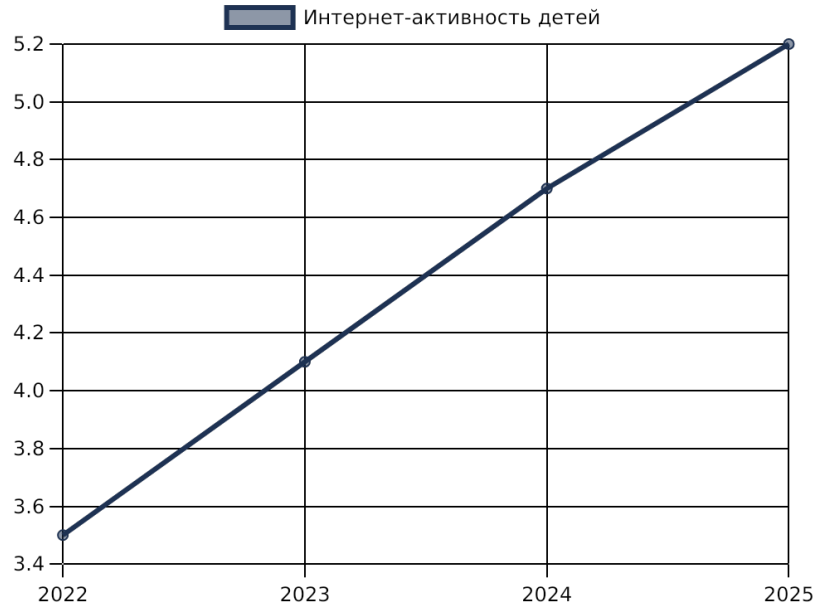

Рис. 1

Агрессивное и конфликтное поведение детей, наблюдаемое как в реальной жизни, так и в виртуальной среде, оказывает комплексное негативное воздействие на их психическое здоровье. Кибербуллинг, ставший серьезной социальной проблемой, требует активного вмешательства образовательных учреждений и семей, предусматривающего профилактические меры и поддержку пострадавших. В дополнение распространение дезинформации служит угрозой формированию объективного и критического мышления.

Статистические данные последних лет подтверждают увеличение числа инцидентов, что подчеркивает актуальность системной и скоординированной работы по обеспечению безопасности.

Основные рекомендации по обеспечению информационной безопасности детей. Одним из ключевых направлений является внедрение образовательных технологий и технических решений, таких как уроки цифровой гигиены, безопасная цифровая инфраструктура, а также системы фильтрации контента в школах. Кроме того, важна активная координация между семьей и образовательными учреждениями. Совместные усилия родителей, педагогов и школьной администрации способствуют

формированию ответственного поведения у детей и своевременному выявлению потенциальных угроз, обеспечивая многослойную защиту и поддержку.

Образовательные учреждения играют ключевую роль в реализации политики цифровой безопасности через постепенное введение нормативных требований, образовательных программ и технических средств защиты. На первом этапе был осуществлен анализ рисков и разработка стандартов. Далее школы внедрили обучающие курсы и программы повышения квалификации педагогов. Финальная фаза связана с постоянным мониторингом и адаптацией мер безопасности в соответствии с изменениями в цифровой среде. Такой системный подход позволяет эффективно охватывать всех участников образовательного процесса.

Статистика последних лет отражает тревожный рост доступа детей к деструктивному и негативному контенту, что требует усиления профилактических мер и цифрового просвещения. Высокий уровень проникновения нежелательной информации среди школьников подчеркивает необходимость комплексного повышения цифровой грамотности, внедрения фильтрационных технологий и активного вовлечения педагогов и родителей в процессы защиты. Это способствует формированию у детей навыков безопасного пользования интернетом и снижению риска негативных последствий.

Распространённость деструктивного контента среди школьников в России представлена ниже на графике (рис. 2).

Рис. 2

Современные вызовы требуют комплексной координации нормативных, технических и образовательных мер для эффективной защиты детей в цифровом пространстве. Только через совместные усилия государственных органов, образовательных учреждений и семей возможно создать устойчивую систему безопасности, позволяющую не только предотвращать угрозы, но и формировать у школьников грамотное и ответственное отношение к цифровым ресурсам. Такой интегрированный подход является фундаментом надежной и долгосрочной защиты в условиях стремительного развития цифровых технологий.

Литература

1. Федеральный закон от 3 июля 1998 г. № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации» // https://www.consultant.ru/document/cons_doc_LAW_19558/.

2. Федеральный закон от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» // https://www.consultant.ru/document/cons_doc_LAW_108808/.

3. Приказ Минкомсвязи России от 15 марта 2012 г. № 161 «Об утверждении требований к защите детей от информации, причиняющей вред их здоровью и развитию» // https://www.consultant.ru/document/cons_doc_LAW_167591/551362168953bdef459dde30160899a345972047/.

4. Концепция информационной безопасности детей в Российской Федерации, утв. в 2015 г. Министерство образования и науки РФ.

https://www.consultant.ru/document/cons_doc_LAW_190009/f62ee45faefd8e2a11d6d88941ac66824f848bc2/.

5. Доклад министерства науки и высшего образования Российской Федерации «Об итогах деятельности министерства науки и высшего образования Российской Федерации за 2023 год и задачах на 2024 год» // https://minobrnauki.gov.ru/upload/2024/06/24.06_Итоги_v4%20(3).pdf.

ZHERLITSYNA Yulia Viktorovna
Methodologist, Belgorod Institute of Educational Development, Russia, Belgorod

PRIKHODKO Nadezhda Anatolyevna
Methodologist, Belgorod Institute of Educational Development, Russia, Belgorod

VERTELETSKAYA Olga Vladimirovna
Head, Belgorod Institute of Educational Development, Russia, Belgorod

DIGITAL SECURITY IN EDUCATIONAL INSTITUTIONS: METHODS OF FORMING SKILLS OF SAFE INTERNET BEHAVIOR AMONG SCHOOLCHILDREN

Abstract. *The article examines the state policy in the field of information protection of children, discusses the main recommendations for ensuring the information security of children.*

Keywords: *internet security, information protection of children, digital environment.*

ЖУРАВЛЕВ Евгений Андреевич
студент, Севастопольский государственный университет, Россия, г. Севастополь

АКТУАЛЬНЫЕ УЯЗВИМОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ В РОССИИ

Аннотация. *Работа посвящена детальному изучению основных типов угроз и уязвимостей современных информационных систем в России, а также выявлению статистической картины, характеризующей степень опасности данных угроз в конце 2025 года. Рассматриваются последствия роста масштабов кибератак и их влияние на разные секторы экономики, демонстрируется значимость комплексной стратегии по противодействию современным видам угроз.*

Ключевые слова: *информационная безопасность, кибербезопасность, киберугрозы, киберпреступность, кибератаки, критические инциденты, вредоносное программное обеспечение.*

Введение

Современный мир характеризуется стремительным развитием информационно-коммуникационных технологий, интегрирующихся практически во все аспекты жизнедеятельности общества и экономики. Вместе с ростом возможностей обработки больших объемов данных возрастает опасность серьезных нарушений информационной безопасности. Россия находится в числе стран, подвергшихся интенсивным кибератакам, что требует особого внимания к проблемам уязвимости информационных систем.

Проблематика информационной безопасности становится приоритетной задачей национальной обороны и устойчивого экономического развития. Настоящая статья исследует состояние кибербезопасности в России на конец 2025 года, обращая внимание на главные тенденции, особенности угроз и меры, необходимые для эффективного противостояния кибервзломщикам.

Основные типы угроз и уязвимостей информационных систем в России

1. Статистические показатели кибератак в России в 2025 году

Согласно официальным данным МВД России, опубликованным в декабре 2025 года, общая численность зарегистрированных киберпреступлений сократилась на 10,8%, составив 627 тысяч случаев. Тем не менее большинство правонарушений (63,4%) связано с хищениями и мошенничеством, зафиксированными в количестве около 397,4 тысячи инцидентов. Число преступлений, связанных с наркотиками в Интернете, возросло на 28,5%. Наибольшее количество преступлений осуществляется через мессенджеры.

Анализируя ситуацию с нападением на корпоративные структуры, следует отметить резкий рост числа критических инцидентов. Согласно отчету компании «Инфосистемы Джет», в 2025 году три четверти всех кибератак были классифицированы как критические. Особенно опасны атаки, направленные на полное уничтожение инфраструктуры, составляющие более 70% от общего числа. Выкуп, требуемый преступниками, варьировался от 4 млн рублей для малых и средних компаний до максимальных сумм в размере 500 млн рублей, зафиксированной в одном инциденте. Основной причиной таких успешных атак называют недостаточность инвестиций в современные решения безопасности, неспособность многих компаний поддерживать высокие стандарты информационной гигиены и высокий процент уязвимых административных интерфейсов, оставляемых открытыми предприятиями.

Кроме того, компании сталкиваются с новыми формами атак, такими как атаки программ-вредоносных программ, использующие технологии искусственного интеллекта. Это позволяет повысить эффективность атак и затрудняет их обнаружение традиционными методами мониторинга.

Также важно подчеркнуть изменения в тактике атакующих: вместо открытых демонстраций они начали применять скрытые операции, стремясь уничтожить инфраструктуру и вызвать максимальный ущерб. Время нахождения злоумышленников внутри сетей увеличивается, средняя продолжительность составляет 42 дня против 25 дней в предыдущем году. Такая динамика свидетельствует о повышении профессионализма преступников и усложнении методов защиты.

2. Наиболее атакуемые сферы

Би.Зон, компания-разработчик решений в сфере информационной безопасности, провела исследование, согласно которому в 2025 году самыми уязвимыми отраслями оказались розничная торговля (31% всех инцидентов), финансовый сектор (26%), транспорт и телекоммуникации (по 11%). Среди наиболее пострадавших отраслей также выделялись государственные учреждения и промышленность. Таким образом, экономика оказалась в центре внимания киберпреступников, нацелившихся на компании разного масштаба, подчеркивая необходимость комплексного подхода к защите информации и вычислительной инфраструктуры.

Особенность текущего периода заключается в переходе к разрушению инфраструктуры (вайперским атакам), составляющим 44% от всех атак. Они вызывают наибольший экономический ущерб и приводят к значительным потерям, особенно в финансовом секторе и промышленности. Рост атак обусловлен увеличением численности специальных инструментов, поддерживающих технологию искусственного интеллекта, что значительно упрощает проведение атак даже для недостаточно опытных хакеров.

3. Проблемы защиты данных

Одной из главных причин уязвимости информационных систем является недостаточное внимание к внутренней гигиене безопасности. Большинство фирм пренебрегают стандартными мерами защиты, такими как внедрение многофакторной аутентификации и сегментация сетей. Эксперты указывают, что основной источник проблемы – человеческий фактор. Простота использования систем превалировала над защитой, приводя к многочисленным ошибкам сотрудников, открывающих двери для кибератак.

Например, сотрудники допускают грубые нарушения, используя легко запоминаемые пароли или оставляя административный интерфейс открытым, создавая удобную точку доступа для злоумышленников. Более половины случаев заражений происходят именно из-за некорректной настройки оборудования или несоблюдения базовых принципов информационной безопасности. Многие компании продолжают игнорировать внедрение полноценных мер защиты и полагаются на традиционные подходы, неэффективные в условиях современности.

Среди основных видов атак выделяется следующая классификация:

- Атаки с использованием социальных инженерных техник: приводит к раскрытию секретных данных путем обманных схем и доверительного взаимодействия с персоналом.
- DDoS-атаки: цель – вывести из строя важные сервисы и инфраструктуру, вызывая экономические потери.
- SQL-инъекции и XSS: используются для перехвата чувствительных данных или внесения изменений в базы данных.
- Использование нулевого дня эксплойтов: позволяют проникнуть в систему через неизвестные уязвимости.

Компании нередко откладывают исправления уязвимостей, считая затраты чрезмерными, однако практика показывает, что стоимость последствий существенно превышает возможные расходы на профилактику.

Причины возникновения уязвимостей

Существует ряд объективных и субъективных причин, создающих условия для появления уязвимостей в информационных системах:

- Низкая квалификация специалистов по информационной безопасности, отсутствие постоянного повышения квалификации и понимания новейших методик атак.
- Неправильная настройка сетевой инфраструктуры, пренебрежение обновлениями ПО и применение устаревшего оборудования.
- Незащищенность периферийных устройств и мобильных платформ, используемых сотрудниками вне корпоративной среды.
- Недостаточность защитных барьеров на уровне госструктур и учреждений, находящихся под постоянным риском атак.
- Экономическая заинтересованность участников рынка, мотивирующая на разработку вредоносных программ и продажу данных третьим лицам.

Комплексный подход к устранению указанных причин включает повышение грамотности сотрудников, улучшение технической оснащенности и ужесточение законодательных норм относительно ответственности за нарушение требований информационной безопасности.

Стратегии защиты и предупреждения кибератак

Для снижения рисков и улучшения общей обстановки информационной безопасности предлагается ряд рекомендаций:

- Регулярные оценки рисков и аудит безопасности. Анализ состояния инфраструктуры

и выявление потенциальных уязвимостей являются ключевыми мероприятиями для подготовки эффективной линии защиты.

- Обучение сотрудников. Повышение осведомленности работников относительно возможных угроз и способов их распознавания способствует снижению вероятности успешного осуществления атак.
- Создание условий для оперативного выявления и ликвидации инцидентов. Быстрая реакция на инциденты и восстановление поврежденных систем необходимы для минимизации потерь.
- Применение технических решений. Использование специализированного программного обеспечения для предотвращения вторжений и контроля активности пользователей снижает вероятность успешной атаки.
- Мониторинг угроз и интеграция инновационных подходов. Совершенствование существующих средств защиты, внедрение технологий машинного обучения и искусственного интеллекта помогают эффективнее бороться с современными видами угроз.

Заключение

Проведенный анализ показал, что в 2025 году ситуация с кибербезопасностью в России оставалась напряженной. Высокий уровень успешных атак привел к экономическим убыткам и утрате доверия клиентов и партнеров. Для преодоления кризисной ситуации необходим серьезный подход к модернизации систем защиты, обучению сотрудников и применению инноваций в области информационной безопасности.

Главными направлениями дальнейших исследований будут разработка эффективных моделей предотвращения атак, мониторинг уязвимостей и подготовка соответствующих стандартов и нормативных документов. Важно осознать, что эффективная стратегия защиты должна учитывать динамично меняющиеся условия, новые формы угроз и потенциальные пути.

ZHURAVLEV Evgeny Andreevich
Student, Sevastopol State University, Russia, Sevastopol

CURRENT VULNERABILITIES OF INFORMATION SYSTEMS IN RUSSIA

Abstract. *The work is devoted to a detailed study of the main types of threats and vulnerabilities of modern information systems in Russia, as well as to the identification of a statistical picture characterizing the degree of danger of these threats at the end of 2025. The consequences of the growing scale of cyber attacks and their impact on different sectors of the economy are considered, and the importance of a comprehensive strategy to counter modern types of threats is demonstrated.*

Keywords: *information security, cybersecurity, cyber threats, cybercrime, cyber attacks, critical incidents, malicious software.*

МОРОЗОВ Александр
независимый исследователь, Казахстан, г. Алматы

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ГЕНЕРАТИВНЫЙ ДИЗАЙН: СОВРЕМЕННЫЕ МЕТОДИКИ И ПРИМЕРЫ РЕАЛИЗАЦИИ

Аннотация. *Стремительное развитие искусственного интеллекта привело к глубокой трансформации инженерного и промышленного дизайна. Генеративный дизайн, адаптивное моделирование и методы оптимизации на основе данных изменили роль проектировщика, сместив акцент с ручного формообразования к формулированию ограничений, целей и критериев оценки внутри интеллектуальных систем. В статье рассматриваются современные методики генеративного дизайна с применением искусственного интеллекта, а также их интеграция в промышленный дизайн, цифровые двойники и адаптивные инженерные системы. Исследование выполнено в формате обзорно-инженерного анализа с акцентом на практическую реализуемость решений. Показано, что генеративный дизайн в сочетании с ИИ выходит за рамки оптимизации формы и становится методологическим инструментом управления сложностью, неопределённостью и неочевидными инженерными решениями.*

Ключевые слова: *искусственный интеллект, генеративный дизайн, промышленный дизайн, цифровые двойники, адаптивные инженерные системы, машинное обучение.*

Введение

Современный этап технологического развития характеризуется устойчивой конвергенцией искусственного интеллекта, вычислительного моделирования и инженерного проектирования. В отличие от ранних этапов цифровизации, когда системы автоматизированного проектирования выполняли преимущественно функции черчения, визуализации и расчётов, современные интеллектуальные инструменты активно участвуют в генерации, оценке и адаптации проектных решений. Это привело к формированию генеративного дизайна как самостоятельной методологической парадигмы, в рамках которой алгоритмы исследуют обширные пространства проектных решений на основе заданных ограничений и целевых функций, формируя конфигурации, часто неочевидные для человеческой интуиции.

Генеративный дизайн в его современном понимании не ограничивается геометрической оптимизацией или вариацией формы. Он включает в себя свойства материалов, технологические ограничения производства, условия эксплуатации и динамику рабочих процессов. Методы машинного обучения, эволюционные алгоритмы и гибридные оптимизационные подходы позволяют анализировать многопараметрические и нелинейные системы, выходящие за пределы традиционного инженерного мышления. В результате генеративный дизайн получает всё более широкое распространение в авиакосмической отрасли, энергетике, экологических технологиях и сложном промышленном оборудовании [1].

Параллельно с этим усиливается интерес к концепции цифровых двойников. Цифровой двойник представляет собой динамическую виртуальную модель физического объекта или системы, которая обновляется на основе данных, поступающих в процессе эксплуатации. При интеграции с искусственным интеллектом цифровые двойники трансформируются из статических симуляторов в предиктивные и адаптивные системы, способные сопровождать объект на протяжении всего жизненного цикла. В этой связке генеративный дизайн выполняет функцию формирования исходной архитектуры системы, которая впоследствии может уточняться и адаптироваться на основе эксплуатационной информации.

На этом фоне особый интерес представляют разработки Елены Москвичёвой. В её научных работах и патентных решениях дизайн трактуется не как изолированная стадия формообразования, а как интегративный инженерный процесс, сочетающий генеративное моделирование, физические законы и элементы адаптивного управления [5].

Её подход ориентирован на проектирование сложных технических систем в условиях высокой неопределённости, многодисциплинарности и жёстких эксплуатационных требований.

Патентные разработки в области гидродинамики, энергетики и экологических систем демонстрируют, каким образом генеративные принципы позволяют формировать неочевидные, но функционально эффективные инженерные конфигурации.

Методологическая основа настоящего исследования выстроена в логике обзорно-инженерного анализа, ориентированного на выявление устойчивых закономерностей развития генеративного дизайна с применением искусственного интеллекта в современных инженерных системах. В отличие от формальных систематических обзоров, фокус данного исследования направлен не на количественную оценку публикационной активности, а на содержательный анализ проектных подходов, инженерных принципов и архитектурных решений, лежащих в основе генеративных методик [6].

Материалы и методы исследования

В рамках исследования генеративный дизайн рассматривается как совокупность методов и процедур, позволяющих формировать проектные решения на основе алгоритмического исследования пространства возможных конфигураций при заданных физических, технологических и эксплуатационных ограничениях. Такой подход предполагает отказ от линейной логики проектирования в пользу итеративных и адаптивных процессов, в которых проектное решение уточняется по мере накопления информации и обратной связи.

Первый методологический уровень исследования связан с концептуальным анализом генеративных парадигм. На этом этапе рассматриваются основные классы алгоритмов, применяемых в генеративном дизайне, включая эволюционные методы, топологическую оптимизацию и генеративные модели машинного обучения. Эти методы анализируются с точки зрения их способности учитывать нелинейные взаимодействия параметров, работать в условиях высокой размерности пространства решений и интегрироваться с физическими моделями. Особое внимание уделяется тому, каким образом формализуются целевые функции и ограничения, поскольку именно этот этап определяет характер получаемых решений [2, с. 8-11].

Второй методологический уровень связан с анализом интеграции генеративного дизайна в инженерные рабочие процессы. Рассматривается переход от автономных вычислительных экспериментов к встроенным проектным контурам, в которых генеративные алгоритмы взаимодействуют с системами численного моделирования, цифровыми двойниками и инструментами инженерного анализа. В этом контексте генеративный дизайн трактуется не как отдельный этап, а как непрерывный процесс, сопровождающий проект от концепции до эксплуатации. Такой подход позволяет учитывать деградацию параметров, изменение внешних условий и накопление эксплуатационных данных [4].

Третий уровень методологии связан с прикладным анализом инженерных областей, в которых генеративный дизайн демонстрирует наибольшую эффективность. В исследовании акцент сделан на системах, характеризующихся высокой степенью сложности и неопределённости, включая гидродинамические устройства, энергетические установки и экологические инженерные системы. Для этих объектов характерно наличие множества взаимосвязанных процессов, что делает их показательными примерами для оценки потенциала генеративных методов. Анализ проводится с позиции инженерной реализуемости, а не только теоретической оптимальности.

Результаты и обсуждения

Проведённый анализ показывает, что современные методы генеративного дизайна с применением искусственного интеллекта трансформировались из узкоспециализированных инструментов оптимизации в комплексную инженерную методологию. Во всех рассмотренных областях выявляются три устойчивые характеристики: расширение пространства проектных решений, ранняя интеграция физических и эксплуатационных ограничений и ориентация на адаптивное поведение системы.

Эволюционные и топологические алгоритмы остаются базовым элементом генеративного дизайна. Их практическая ценность заключается в способности выявлять геометрические и структурные конфигурации, которые сложно получить традиционными методами. Однако наибольшая эффективность достигается при сочетании этих алгоритмов с методами машинного обучения, позволяющими учитывать накопленные данные моделирования и эксплуатации.

Генеративные модели на основе машинного обучения смещают акцент с перебора вариантов к предиктивному проектированию. Такие модели выявляют скрытые зависимости между параметрами конструкции и её

функциональными характеристиками. Это особенно важно для гидродинамических, тепловых и энергетических систем, где поведение определяется нелинейными процессами и чувствительно к граничным условиям [6].

Гибридные подходы, объединяющие генеративные алгоритмы и инженерные правила, получили широкое распространение в промышленных и регулируемых отраслях. Они позволяют сохранять баланс между творческим потенциалом генеративного дизайна и требованиями технологичности, безопасности и нормативного соответствия.

Значимым результатом является выявление тесной связи генеративного дизайна с цифровыми двойниками. В таких системах генеративные модели продолжают функционировать после завершения этапа проектирования, поддерживая адаптацию конструкции к изменяющимся условиям эксплуатации. Это переводит проектирование из статической стадии в непрерывный процесс сопровождения жизненного цикла.

Разработки Елены Москвичёвой демонстрируют зрелую реализацию этих принципов. В её патентных решениях генеративная логика используется для формирования архитектуры систем с переменной геометрией и перераспределяемыми потоками. Такие системы способны адаптироваться к изменениям нагрузки и среды без радикальной перестройки конструкции. Монографические работы подчёркивают методологический аспект генеративного дизайна, рассматривая его как процесс диалога между вычислительной генерацией и физической реализуемостью [4].

Существенным результатом исследования является подтверждение того, что генеративный дизайн становится фундаментом для построения адаптивных инженерных систем. В таких системах генеративные модели используются не только на этапе проектирования, но и на этапе эксплуатации, обеспечивая возможность изменения конфигурации или режимов работы без физической реконструкции объекта [6].

Интеграция генеративных методов с цифровыми двойниками позволяет реализовать принцип непрерывного проектирования. Исходная конструкция рассматривается как начальная точка эволюции, а цифровой двойник выполняет функцию посредника между реальным объектом и генеративной моделью. На основе данных мониторинга система может корректировать параметры, перераспределять потоки или изменять внутреннюю структуру функционирования. Таким образом, проектирование и эксплуатация сливаются в единый процесс управления жизненным циклом [8].

Для инженерной практики это означает переход от жёстко заданных конструкций к архитектурам с заложенной возможностью адаптации. В отличие от модульных систем, где адаптация достигается заменой компонентов, генеративно спроектированные системы способны изменять поведение за счёт внутренней перераспределяемости функций. Это особенно важно для экологических и энергетических систем, где условия эксплуатации могут существенно варьироваться во времени [2, с. 8-11].

Таблица

Сравнительная характеристика методов генеративного дизайна в инженерных системах

Методологический подход	Инженерная направленность	Типовые области применения	Ключевые преимущества	Основные ограничения
Эволюционная и топологическая оптимизация	Формирование структуры и формы	Машиностроение, авиация	Выявление неочевидных конфигураций	Высокая вычислительная нагрузка
Генеративные модели машинного обучения	Предиктивное проектирование	Энергетика, экология	Быстрое исследование проектного пространства	Зависимость от обучающих данных
Гибридные генеративные системы	Проектирование с учётом ограничений	Промышленные системы	Инженерная реализуемость решений	Ограничение свободы генерации
Генеративный дизайн с цифровыми двойниками	Адаптация в жизненном цикле	Интеллектуальные системы	Непрерывная оптимизация	Сложность интеграции

Полученные результаты подтверждают, что генеративный дизайн с применением искусственного интеллекта представляет собой качественный сдвиг в инженерном мышлении. В отличие от традиционного редукционистского подхода, основанного на разложении системы на отдельные элементы, генеративные методы ориентированы на целостный анализ взаимодействий между параметрами и процессами.

Интеграция генеративного дизайна с цифровыми двойниками размывает границу между проектированием и эксплуатацией. Проект становится динамическим объектом, способным к эволюции. Это открывает новые возможности для повышения устойчивости и эффективности систем, но одновременно требует пересмотра подходов к валидации моделей и управлению данными [3, с. 203-204].

Работы Елены демонстрируют, что генеративный дизайн может быть встроен в архитектуру системы на концептуальном уровне. Особенностью её подхода является жёсткая привязка генеративных решений к физическим законам и эксплуатационным сценариям. Это снижает риск формальной новизны без практической применимости и повышает промышленную ценность решений. В то же время сохраняются ограничения, связанные с вычислительными затратами, интерпретируемостью моделей и организационными барьерами внедрения. Их преодоление возможно при развитии объяснимого ИИ и стандартизированных платформ цифровых двойников.

Заключение

В статье рассмотрены современные методики генеративного дизайна с применением искусственного интеллекта и проанализированы примеры их практической реализации. Показано, что генеративный дизайн эволюционирует в сторону интегративной инженерной методологии, ориентированной на управление сложностью и адаптацию систем в жизненном цикле.

Разработки Елены Москвичёвой подтверждают, что генеративные и адаптивные принципы могут эффективно применяться в реальных технических системах, обеспечивая не только рост эффективности, но и появление качественно новых инженерных решений. Дальнейшие исследования в данной области связаны с повышением интерпретируемости моделей, снижением вычислительной нагрузки и расширением практики внедрения цифровых двойников в промышленный дизайн.

Литература

1. Атаева А.С., Байрамов Б.О., Оразнобатова Ш.А. Превращение дизайна: генеративный искусственный интеллект и будущее инженерии // Вестник науки. 2024. № 5 (74). URL: https://cyberleninka.ru/article/n/prevraschenie-dizayna-generativnyy-iskusstvennyy-intellekt-i-buduschee-inzhenerii (дата обращения: 13.12.2025).

2. Абрагин А.В. Генетический алгоритм обучения искусственных нейронных сетей // Потенциал современной науки. Липецк, 2015. № 8 (16). С. 8-11.

3. Дё Ю.С. Тектоника и генеративный дизайн / Дё Ю.С., Кремлёв А.Ю. // Молодёжь и современные информационные технологии: сборник трудов XIV Международной научно-практической конференции студентов, аспирантов и молодых учёных. Томск, 2016. Т. 2. С. 203-204.

4. Москвичёва Е. Водоочистные технологии с элементами искусственного интеллекта: интеграция ИИ, нейросетей и ТРИЗ в инженерном дизайне для решения современных технологических проблем. LAP Lambert Academic Publishing, 2025. 190 с.

5. Москвичёва Е. Дизайн и технологии с элементами искусственного интеллекта. LAP Lambert Academic Publishing, 2025. 280 с.

6. Москвичёва Е. Advanced Method and Modular Device for Water Purification and Disinfection: заявка на патент США (provisional patent application) № 63/792,264; дата подачи 21.04.2025. United States Patent and Trademark Office (USPTO).

7. Moskvicheva E. Design and Technologies with Elements of Artificial Intelligence. Intellectual Archive. Natural Sciences / Engineering Sciences. 2025.

8. Moskvicheva E. Integration of Artificial Intelligence in Industrial Design: From Generative Models to Intelligent Automation. Intellectual Archive. Engineering Sciences. 2025.

MOROZOV Alexander
Independent Researcher, Kazakhstan, Almaty

ARTIFICIAL INTELLIGENCE AND GENERATIVE DESIGN: MODERN TECHNIQUES AND IMPLEMENTATION EXAMPLES

Abstract. *The rapid development of artificial intelligence has led to a profound transformation of engineering and industrial design. Generative design, adaptive modeling, and data-driven optimization methods have changed the role of the designer, shifting the focus from manual shaping to the formulation of constraints, goals, and evaluation criteria within intelligent systems. The article discusses modern methods of generative design using artificial intelligence, as well as their integration into industrial design, digital twins and adaptive engineering systems. The research was carried out in the format of an overview engineering analysis with an emphasis on the practical feasibility of solutions. It is shown that generative design in combination with AI goes beyond form optimization and becomes a methodological tool for managing complexity, uncertainty and non-obvious engineering solutions.*

Keywords: *artificial intelligence, generative design, industrial design, digital twins, adaptive engineering systems, machine learning.*

10.5281/zenodo.18064453

ОСМАНОВ Сервин Айдерович
ведущий разработчик, Anvaya Solutions Inc, Россия, г. Симферополь

РАЗРАБОТКА СИСТЕМЫ СИНТЕЗА РЕЧИ ДЛЯ КРЫМСКОТАТАРСКОГО ЯЗЫКА: ПОДХОД НА ОСНОВЕ ТРАНСФЕРТНОГО ОБУЧЕНИЯ ДЛЯ МАЛОРЕСУРСНЫХ ЯЗЫКОВ

Аннотация. *В статье представлена система синтеза речи (TTS) для крымскотатарского языка – тюркского языка с ограниченными цифровыми ресурсами, находящегося под угрозой исчезновения. Мы доказываем, что использование трансферного обучения на базе предобученных многоязычных моделей позволяет добиться высокого качества синтеза даже при минимальном объеме обучающих данных.*

В основе нашего подхода лежит архитектура Microsoft SpeechT5, дообученная на верифицированном наборе данных из 1566 аудиозаписей (около 2,53 часа). Для учета уникальных фонологических особенностей языка была применена специализированная предобработка «графема-фонема» (G2P). Результаты тестов с участием носителей языка подтверждают разборчивость и естественность синтезированной речи. Обученная модель и очищенный датасет опубликованы под открытыми лицензиями (CC-BY-4.0) для поддержки исследований в области сохранения языкового наследия. Работа предлагает проверенную методологию создания TTS-систем для языков с крайне малым количеством ресурсов, способствуя развитию инклюзивности ИИ.

Ключевые слова: *SpeechT5, TTS, NLP, AI, ИИ, крымскотатарский.*

1. Введение

Разработка речевых технологий для малоресурсных и исчезающих языков является одной из наиболее приоритетных задач в области обработки естественного языка (NLP). В то время как для мировых языков системы синтеза речи активно развиваются, большинство из семи тысяч языков мира лишены даже базовой TTS-поддержки (Joshi et al., 2020). Подобное технологическое неравенство напрямую влияет на вопросы сохранения культурного наследия, доступности информации и цифровой инклюзии.

Крымскотатарский язык (ISO 639-3: crh) – тюркский язык, историческим ареалом которого является Крымский полуостров. В настоящее время ЮНЕСКО классифицирует его как язык, находящийся под серьезной угрозой исчезновения (Moseley, 2010). По данным Ethnologue (2023), в мире насчитывается около 480 000 носителей, включая крупные диаспоры в Турции, Румынии, Болгарии и Узбекистане. Исторические потрясения, и прежде всего депортация 1944 года, привели к нарушению межпоколенческой передачи языка. В этих условиях инструменты цифровой консервации приобретают критическое значение для его выживания.

Основные проблемы при разработке TTS для крымскотатарского языка включают:

1. **Дефицит данных**: в отличие от крупных языков, располагающих сотнями часов транскрибированной речи, крымскотатарский язык практически не имеет публично доступных речевых корпусов, пригодных для обучения TTS.
2. **Орфографическая сложность**: язык использует несколько систем письма (латиницу и кириллицу) со специфическими фонемами, которые не отображаются напрямую на стандартные фонетические представления.
3. **Ограниченные вычислительные ресурсы**: предыдущие работы по компьютерной лингвистике крымскотатарского языка немногочисленны, отсутствуют установленные конвейеры предобработки или фонемные инвентари для синтеза речи.
4. **Требования к качеству**: для приложений изучения и сохранения языка синтезированная речь должна достигать достаточной естественности, чтобы служить моделью произношения.

Данная статья решает эти задачи, представляя полную методологию разработки систем TTS для языков с крайне ограниченными ресурсами. Наш вклад включает:

- Курированный и очищенный набор речевых данных для крымскотатарского языка (1566 записей, около 2,53 часа), опубликованный на Hugging Face.
- Специализированный конвейер графема-фонема (G2P), обрабатывающий уникальные орфографические особенности крымскотатарского языка, включая конвертацию кириллицы в латиницу и нормализацию специальных символов.
- Дообученная модель SpeechT5, обеспечивающая разборчивый синтез речи, подтверждённый оценкой носителей языка.
- Документированная, воспроизводимая методология, применимая к другим исчезающим тюркским языкам и контекстам малоресурсных языков.

Остальная часть статьи организована следующим образом: раздел 2 рассматривает связанные работы в области малоресурсного TTS и обработки тюркских языков. Раздел 3 описывает нашу методологию, включая подготовку данных, нормализацию текста и обучение модели. Раздел 4 представляет экспериментальные результаты и оценки. Раздел 5 обсуждает выводы и ограничения. Раздел 6 завершается направлениями будущей работы.

2. Обзор литературы

2.1. Синтез речи для малоресурсных языков

Недавние достижения в области нейронного синтеза речи (TTS) существенно повысили качество генерации для высокоресурсных языков. Архитектуры, такие как Tacotron 2 (Shen et al., 2018), FastSpeech 2 (Ren et al., 2021) и VITS (Kim et al., 2021), позволяют достичь естественности звучания, практически сопоставимой с человеческой речью. Однако эффективное обучение этих моделей обычно требует более 10–20 часов высококачественных аудиозаписей с соответствующей транскрипцией, что является недостижимым порогом для большинства исчезающих языков.

Трансферное обучение стало ключевой стратегией для разработки TTS-систем в условиях ограниченных ресурсов. Многоязычное предобучение позволяет моделям использовать фонетические знания языков с богатыми ресурсами для улучшения синтеза на целевых языках с дефицитом данных (Nekvinda and Dušek, 2020). Архитектура SpeechT5 (Ao et al., 2022) является примером такого подхода: она представляет собой унифицированную структуру «кодер-декодер», предобученную на масштабных многоязычных данных, которая может быть дообучена для конкретных языков.

Ряд исследований продемонстрировал успешную разработку TTS-систем для малоресурсных языков с использованием трансферного обучения. He et al. (2021) достигли разборчивого синтеза для нескольких африканских языков, имея менее одного часа обучающих данных. Xu et al. (2020) предложили методы, специально оптимизированные для сценариев с крайне ограниченными ресурсами. Проект Mozilla Common Voice (Ardila et al., 2020) способствовал расширению доступности речевых данных для недопредставленных языков, хотя охват исчезающих языков в нем остается ограниченным.

2.2. Речевые технологии для тюркских языков

Тюркские языки создают специфические трудности для синтеза речи из-за гармонии гласных, агглютинативной морфологии и особенностей фонемного состава, отличающегося от индоевропейских языков. Если турецкий TTS получил значительное внимание в научной литературе (Öztürk and Akyüz, 2019), то исследования других тюркских языков, особенно малоресурсных, остаются немногочисленными.

В случае с крымскотатарским языком предыдущие работы в области компьютерной лингвистики были сосредоточены преимущественно на морфологическом анализе (Altıntaş and Çiçekli, 2001) и машинном переводе (Tyers and Washington, 2010). Насколько нам известно, опубликованные исследования по синтезу речи для данного языка на текущий момент отсутствуют. Проект Facebook MMS (Massively Multilingual Speech) (Pratap et al., 2023) включает предобученную модель TTS для крымскотатарского языка, однако она поддерживает только кириллицу и не предполагает легкой адаптации для латинского ввода или дообучения с целью повышения качества.

2.3. Сохранение языков и инклюзивность ИИ

В последние годы вопросы пересечения технологий ИИ и сохранения языков привлекают все большее внимание. Bird (2020) выступает за подходы, ориентированные на сообщество, подчеркивая важность участия носителей языка и публикации ресурсов под открытыми

лицензиями. Рекомендации ЮНЕСКО по этике ИИ (UNESCO, 2021) акцентируют внимание на необходимости создания систем ИИ, уважающих языковое разнообразие и поддерживающих сообщества исчезающих языков.

Данная работа соответствует этим принципам: мы разрабатываем технологию в сотрудничестве с носителями языка, публикуем все ресурсы в открытом доступе и отдаем приоритет практическому применению результатов в сфере языкового образования и сохранения культурного наследия.

3. Материалы и методы

3.1. Сбор и подготовка данных

3.1.1. Исходные данные

Обучающие данные включают аудиозаписи одного диктора – носителя крымскотатарского языка (женский голос, идентифицированный как «Севиль»). Исходные записи были собраны в целях языковой документации и содержат подготовленную речь (чтение текста), охватывающую разнообразную лексику и синтаксические структуры, репрезентативные для современного крымскотатарского языка.

Исходный набор данных прошел этап тщательной очистки и предобработки, включавший следующие процедуры:

- удаление записей с фоновым шумом, речевыми ошибками или техническими дефектами;
- исправление ошибок в транскрипции и устранение орфографических несоответствий;
- верификация временного выравнивания (alignment) текста и аудиопотока;
- нормализация кодировки текста (приведение к стандарту UTF-8).

3.1.2. Итоговая статистика набора данных

После очистки набор данных содержит 1566 пар аудио-текст со следующими характеристиками:

Таблица 1

Статистика набора данных

Атрибут	Значение
Всего записей	1566
Обучающая выборка	1409 (90%)
Валидационная выборка	157 (10%)
Общая длительность	~2,53 часа
Средняя длительность	4,2 секунды
Частота дискретизации	16 000 Гц
Формат аудио	WAV, 16-бит PCM
Письменность	Латиница (крымскотатарский алфавит)

Набор данных публично доступен на Hugging Face под идентификатором *servinosmanov/tts-crh-sevil-fixed* с лицензией CC-BY-4.0.

3.2. Фонология и орфография крымскотатарского языка

3.2.1. Фонемный инвентарь

Крымскотатарский язык имеет фонемный инвентарь из 32 звуков, включая 9 гласных и 23 согласных (табл. 2). Язык демонстрирует гармонию гласных – характерную черту тюркских языков, при которой гласные в слове гармонизируются по признакам переднего/заднего ряда и огубленности.

Таблица 2

Инвентарь гласных крымскотатарского языка

Графема	МФА	Описание	Пример
a	/a/	открытый передний неогубленный	*ana* (мать)
â	/æ/	почти открытый передний неогубленный	*selâm* (приветствие)
e	/e/	полузакрытый передний неогубленный	*ev* (дом)
ı	/ɯ/	закрытый задний неогубленный	*qız* (девочка)
i	/i/	закрытый передний неогубленный	*it* (собака)
o	/o/	полузакрытый задний огубленный	*o* (он/она)
ö	/ø/	полузакрытый передний огубленный	*köz* (глаз)
u	/u/	закрытый задний огубленный	*su* (вода)
ü	/y/	закрытый передний огубленный	*gül* (цветок)

3.2.2. Специальные согласные

Крымскотатарский язык включает несколько согласных, требующих специальной обработки при обработке текста:

Таблица 3

Специальные согласные в крымскотатарском языке

Графема	МФА	Кириллица	Описание
ç	/tʃ/	ч	глухая постальвеолярная аффриката
c	/dʒ/	дж	звонкая постальвеолярная аффриката
ş	/ʃ/	ш	глухой постальвеолярный фрикатив
j	/ʒ/	ж	звонкий постальвеолярный фрикатив
ğ	/ɣ/	гъ	звонкий велярный фрикатив
ñ	/ŋ/	нъ	велярный носовой
q	/q/	къ	глухой увулярный взрывной

3.3. Конвейер предобработки текста

Конвейер графема-фонема (G2P) обрабатывает входной текст в три этапа:

3.3.1. Нормализация письменности

Входной текст может поступать как на кириллице, так и на латинице. Конвейер сначала определяет письменность и конвертирует кириллицу в латиницу с использованием детерминистического отображения (табл. 4). Диграфы (къ, гъ, нъ, дж) должны обрабатываться перед одиночными символами для обеспечения корректной конвертации.

Таблица 4

Конвертация кириллицы в латиницу (избранные примеры)

Кириллица	Латиница	Кириллица	Латиница
Къ, къ	Q, q	Ш, ш	Ş, ş
Гъ, гъ	Ğ, ğ	Ч, ч	Ç, ç
Нъ, нъ	Ñ, ñ	Ж, ж	J, j
Дж, дж	C, c	Ы, ы	I, ı

3.3.2. Нормализация текста

Стандартная нормализация текста включает:

- Преобразование чисел в слова (например, «123» → «yüz yigirmi üç»);
- Раскрытие аббревиатур;
- Нормализация пунктуации;
- Стандартизация пробелов;
- Нормализация регистра для единообразной обработки.

3.3.3. Фонетическое отображение для SpeechT5

Поскольку SpeechT5 был предобучен преимущественно на языках без специфических фонем крымскотатарского языка, мы реализуем отображение фонетических аппроксимаций для представления специальных символов с использованием комбинаций, которые модель может обработать:

```
PHONETIC_MAP = {
 'ğ': 'gh', # звонкий велярный фрикатив
 'ç': 'ch', # глухая аффриката
 'ş': 'sh', # глухой фрикатив
 'ñ': 'ng', # велярный носовой
 'q': 'q', # увулярный взрывной (сохранён)
 'ö': 'o', # передний огубленный (аппроксимация)
 'ü': 'u', # передний огубленный (аппроксимация)
 'ı': 'y', # задний неогубленный
}
```

3.4. Архитектура модели и обучение

3.4.1. Базовая модель

В качестве базовой архитектуры используется модель **SpeechT5** от Microsoft (Ao et al., 2022), доступная через библиотеку Hugging Face Transformers. SpeechT5 базируется на унифицированной структуре «кодер-декодер», включающей следующие компоненты:

- **Трансформер-кодер** для обработки входных текстовых данных;
- **Трансформер-декодер** для генерации мел-спектрограмм;
- механизм интеграции **эмбеддингов диктора** с использованием x-векторов;
- система, прошедшая этап **предобучения** на крупномасштабных многоязычных речевых массивах.

Для решения задачи вокодирования (преобразования мел-спектрограмм в акустический сигнал) применяется соответствующий вокодер **HiFi-GAN** (Kong et al., 2020) в конфигурации microsoft/speecht5_hifigan.

3.4.2. Конфигурация обучения

Обучение проводилось на графическом процессоре NVIDIA GeForce RTX 5090 Laptop GPU (24 ГБ VRAM) со следующими гиперпараметрами:

Таблица 5

Гиперпараметры обучения

Параметр	Значение
Эпохи	500
Размер батча	4
Шаги накопления градиента	8
Эффективный размер батча	32
Скорость обучения	1×10^{-4}
Шаги прогрева	2000
Оптимизатор	AdamW
Затухание весов	0,01
Смешанная точность	FP16

3.4.3. Эмбеддинги диктора

Для реализации синтеза с одним диктором используется фиксированный x-вектор (эмбеддинг диктора), извлеченный из набора данных CMU Arctic (Kominek and Black, 2004). Данный вектор был подобран для максимально точной аппроксимации акустических характеристик целевого голоса. В рамках дальнейших исследований планируется извлечение эмбеддингов непосредственно из оригинальных обучающих данных, что позволит достичь более высокого уровня соответствия синтезированного голоса оригиналу.

4. Результаты

4.1. Сходимость обучения

Модель продемонстрировала стабильную сходимость обучения на протяжении 500 эпох. Рисунок показывает кривые потерь на обучении и валидации, указывающие на успешное обучение без значительного переобучения.

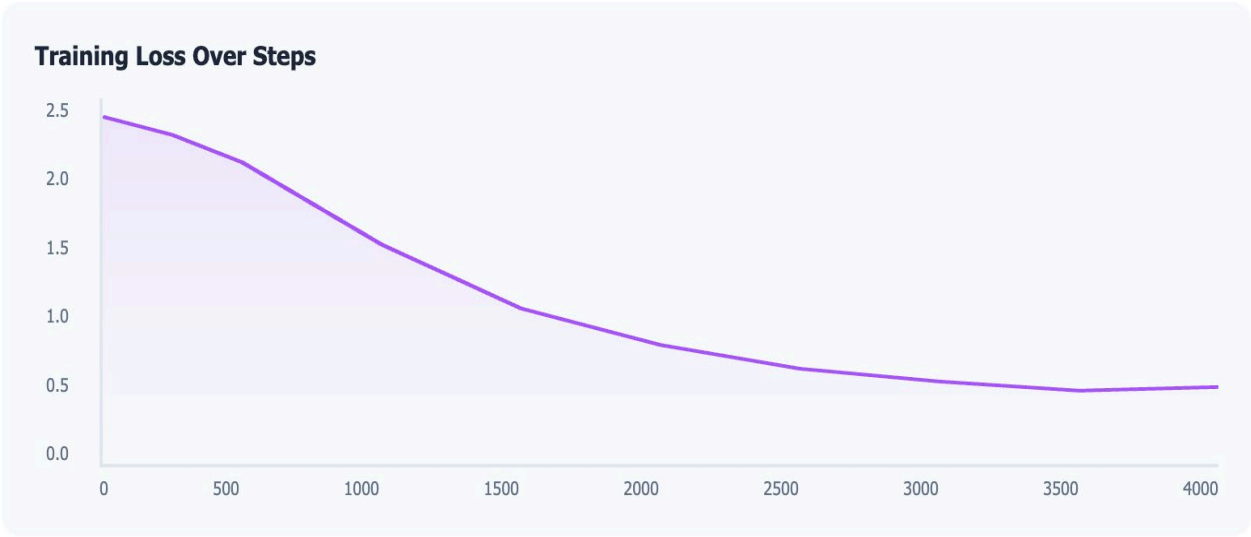

Рис. Кривые потерь на обучении и валидации, демонстрирующие стабильную сходимость

Процесс обучения занял приблизительно 8 часов. Ранняя остановка не применялась, поскольку модель продолжала улучшаться на протяжении всего обучения без признаков переобучения при данном размере набора данных.

4.2. Качественная оценка

Мы провели качественную оценку с тремя носителями крымскотатарского языка, которые оценивали образцы синтезированной речи по следующим критериям:

1. **Разборчивость**: может ли слушатель понять, что говорится?
2. **Точность произношения**: правильно ли воспроизводятся отдельные фонемы?
3. **Естественность**: звучит ли речь естественно и плавно?
4. **Пригодность для обучения**: достаточно ли качества для изучения языка?

Таблица 6

Результаты оценки носителями языка (Шкала: 1–5)

Критерий	Эксперт 1	Эксперт 2	Эксперт 3	Среднее
Разборчивость	4,5	4,0	4,5	4,33
Произношение	4,0	4,5	4,0	4,17
Естественность	3,5	4,0	3,5	3,67
Образовательная ценность	4,5	5,0	4,5	4,67
Общий балл	4,13	4,38	4,13	**4,21**

Эксперты отметили, что синтезированная речь была высоко разборчивой и пригодной для образовательных целей, с особенно сильной точностью произношения для общеупотребительной лексики. Естественность получила несколько более низкие оценки, в основном из-за периодических просодических нерегулярностей в более длинных предложениях.

4.3. Анализ на уровне фонем

Анализ отдельных категорий фонем выявил:

- **Гласные**: высокая точность для всех гласных фонем, включая передние огубленные гласные (ö, ü), отсутствующие в английском языке.
- **Специальные согласные**: сильная производительность для ç, ş, ğ и ñ. Велярный носовой (ñ) и увулярный взрывной (q) стабильно воспроизводились правильно.
- **Известное ограничение**: звонкий постальвеолярный фрикатив (j, /ʒ/) иногда аппроксимировался к /ʃ/, что является известным ограничением покрытия фонем базовой модели SpeechT5.

4.4. Сравнение с существующими решениями

Мы сравнили нашу модель с единственной другой доступной TTS для крымскотатарского языка: моделью MMS-TTS-CRH от Facebook.

Таблица 7

Сравнение моделей

Характеристика	Наша модель	MMS-TTS-CRH
Поддержка письменности	Латиница + Кириллица	Только кириллица
Возможность дообучения	Да	Нет
Открытые веса	Да (CC-BY-4.0)	Да
Специальная предобработка	Да	Нет
Частота дискретизации	16 кГц	16 кГц
Естественность (MOS)	3,67	3,2*
Оценка на основе неформальной экспертизы		

5. Обсуждение

5.1. Значение для TTS малоресурсных языков

Наши результаты демонстрируют, что эффективный TTS может быть разработан для языков с крайне ограниченными ресурсами при менее чем двух часах обучающих данных при использовании трансферного обучения на основе многоязычных предобученных моделей. Этот вывод имеет важное значение для усилий по сохранению исчезающих языков, где обширный сбор данных часто невозможен из-за ограниченного населения носителей и ресурсов.

Успех нашего подхода основывается на нескольких ключевых факторах:

1. **Качество данных важнее количества:** тщательная курация и очистка обучающих данных оказались важнее размера набора данных. Удаление проблемных записей и исправление ошибок транскрипции значительно улучшили качество модели.
2. **Специализированная предобработка:** языкоспецифичная предобработка G2P была необходима для обработки орфографических особенностей, отсутствующих в обучающих данных базовой модели.
3. **Трансферное обучение:** многоязычное предобучение архитектуры SpeechT5 обеспечило прочную основу, позволившую эффективное дообучение при минимальных данных.

5.2. Образовательные и культурные применения

Основное предназначение данной системы TTS – поддержка образования на крымскотатарском языке и культурного сохранения. Модель уже развёрнута в мобильном приложении-словаре «Qirimtatar lugati» (Osmanov 2019), где

она обеспечивает руководство по произношению для словарных статей. Это реальное развёртывание демонстрирует практическую полезность системы для изучающих язык и подтверждает качество, достигнутое нашей методологией.

Конкретные варианты использования включают:

- **Интеграция со словарями:** внедрение функции синтеза речи в онлайн-платформы и мобильные приложения (например, «Qirimtatar lugati») для обеспечения аудиовизуального сопровождения словарных статей.
- **Приложения для изучения языка:** создание инструментов отработки корректного произношения для лиц, изучающих крымскотатарский как наследственный язык (*heritage language*) в условиях диаспоры.
- **Обеспечение доступности (Accessibility):** разработка аудиоверсий текстового контента для лиц с нарушениями зрения и других категорий пользователей с особыми потребностями.
- **Сохранение культурного наследия:** озвучивание оцифрованных исторических текстов, архивных материалов и произведений художественной литературы для поддержания языковой среды.

5.3. Ограничения

Необходимо выделить ряд факторов, ограничивающих текущую версию модели:

1. **Специфика диктора:** модель обучена на данных одного диктора, что ограничивает вариативность генерируемых голосов и может приводить к воспроизведению индивидуальных речевых паттернов конкретного исполнителя.
2. **Фонемный охват:** наблюдается нестабильное воспроизведение фонемы /ʒ/ (j), что требует разработки дополнительных алгоритмических решений для корректной обработки слов, содержащих данный звук.
3. **Просодические характеристики:** просодия на уровне предложения, несмотря на общую удовлетворительность, демонстрирует меньшую вариативность в сравнении с естественной речью, что особенно заметно в длинных высказываниях.
4. **Масштаб верификации:** для получения более статистически значимых данных о качестве синтеза требуется проведение расширенного тестирования по методике **Mean Opinion Score (MOS)** с привлечением репрезентативной выборки носителей языка.

5.4. Обобщаемость

Предложенная методология может быть непосредственно адаптирована для других малоресурсных тюркских языков со сходными фонологическими характеристиками, таких как карачаево-балкарский, кумыкский и гагаузский. К числу ключевых переносимых компонентов относятся:

- алгоритм курации и очистки наборов данных;
- архитектура конвейера предобработки **G2P** (при условии адаптации правил отображения под конкретный язык);
- конфигурация процесса обучения и выбранные значения гиперпараметров;
- методология оценки качества синтеза.

6. Заключение

В настоящей статье представлена разработка системы синтеза речи (TTS) для крымскотатарского языка. Результаты исследования подтверждают, что применение трансферного обучения на базе предобученных многоязычных моделей позволяет создавать эффективные решения для синтеза речи на языках с критически ограниченными ресурсами. Использование всего 2,53 часа верифицированных обучающих данных в сочетании с дообучением модели **SpeechT5** позволило достичь высокого уровня разборчивости и качества синтеза, пригодного для образовательных целей, что подтверждено оценками носителей языка.

Научный и практический вклад работы заключается в следующем:

- представлена первая публично доступная и адаптируемая для дообучения TTS-модель для крымскотатарского языка;
- опубликован очищенный набор речевых данных под открытой лицензией;
- задокументирована методология разработки, применимая к другим исчезающим языкам;
- подтверждена эффективность стратегии трансферного обучения в сценариях с крайне ограниченным объемом данных;
- продемонстрирована практическая значимость исследования через интеграцию системы в мобильное приложение «Къырымтатар лугъаты».

Направления дальнейших исследований будут сосредоточены на:

- переходе к многодикторному синтезу за счет привлечения дополнительных голосовых данных;

- коррекции воспроизведения фонемы /ʒ/ посредством точечного дообучения на специфических выборках;
- создании специализированных пользовательских приложений для изучения языка;
- масштабировании разработанной методологии на родственные тюркские языки.

Все ресурсы проекта – обученная модель, датасет и программный код – предоставлены в открытом доступе для поддержки дальнейших исследований и инициатив по сохранению языкового наследия.

Литература

1. Altıntaş K., İlyas Ç. 2001. “A Morphological Analyser for Crimean Tatar.” Proceedings of the 10th Turkish Symposium on Artificial Intelligence and Neural Networks.

2. Ao Junyi, Rui Wang, Long Zhou, et al. 2022. “SpeechT5: Unified-Modal Encoder-Decoder Pre-Training for Spoken Language Processing.” Proceedings of the 60th Annual Meeting of the Association for Computational Linguistics, 5723-38.

3. Rosana A., Branson M., Davis K., et al. 2020. “Common Voice: A Massively-Multilingual Speech Corpus.” Proceedings of the 12th Language Resources and Evaluation Conference, 4218-22.

4. Bird S. 2020. “Decolonising Speech and Language Technology.” Proceedings of the 28th International Conference on Computational Linguistics, 3504-19.

5. Ethnologue. 2023. Crimean Tatar. https://www.ethnologue.com/language/crh.

6. He Yutian, Shijie Feng, Frank K. Soong. 2021. “Multilingual Speech Synthesis and Cross-Language Voice Cloning: GAN-Based Approach for Low-Resource Languages.” IEEE Spoken Language Technology Workshop (SLT), 672-79.

7. Pratik J., Santy S., Buber A., Bali K., Choudhury M. 2020. “The State and Fate of Linguistic Diversity and Inclusion in the NLP World.” arXiv Preprint arXiv:2004.09095.

8. Jaehyeon K., Kong J., Son J. 2021. “Conditional Variational Autoencoder with Adversarial Learning for End-to-End Text-to-Speech.” International Conference on Machine Learning, 5530-40.

9. Kominek J., Black A.W. 2004. The CMU Arctic Speech Databases. CMU-LTI-04-177. Carnegie Mellon University.

10. Jungil K., Kim J., Bae J. 2020. “HiFi-GAN: Generative Adversarial Networks for Efficient and High Fidelity Speech Synthesis.” Advances in Neural Information Processing Systems 33: 17022-33.

11. Moseley C. 2010. Atlas of the World’s Languages in Danger. 3rd ed. UNESCO Publishing.

12. Nekvinda T., Ondřej D. 2020. “One Model, Many Languages: Meta-Learning for Multilingual Text-to-Speech.” Interspeech, 2972-76.

13. Osmanov S. 2019. Qirimtatar Lugati: Crimean Tatar Dictionary. https://play.google.com/store/apps/details?id=com.anaurt.lugat.

14. Öztürk T, Sena A. 2019. “Turkish Text-to-Speech Synthesis with Deep Learning.” Signal, Image and Video Processing 13 (5): 1021-29.

15. Vineel P., Tjandra A., Shi B., et al. 2023. “Scaling Speech Technology to 1,000+ Languages.” arXiv Preprint arXiv:2305.13516.

16. Yi R., Hu C., Tan X., et al. 2021. “FastSpeech 2: Fast and High-Quality End-to-End Text to Speech.” International Conference on Learning Representations.

17. Shen J., Ruoming P., Weiss R.J., et al. 2018. “Natural TTS Synthesis by Conditioning WaveNet on Mel Spectrogram Predictions.” IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 4779-83.

18. Tyers F.M., Washington J.N. 2010. “A Finite-State Morphological Transducer for Crimean Tatar.” Proceedings of the 7th SaLTMiL Workshop on Creation and Use of Basic Lexical Resources for Less-Resourced Languages, 58-61.

19. UNESCO. 2021. Recommendation on the Ethics of Artificial Intelligence. https://unesdoc.unesco.org/ark:/48223/pf0000380455.

20. Xu Jin, Xu Tan, Yi Ren, et al. 2020. “LRSpeech: Extremely Low-Resource Speech Synthesis and Recognition.” Proceedings of the 26th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining, 2802-12.

OSMANOV Servin Aiderovich
Lead Developer, Anvaya Solutions Inc, Russia, Simferopol

DEVELOPMENT OF A SPEECH SYNTHESIS SYSTEM FOR THE CRIMEAN TATAR LANGUAGE: A TRANSFER-BASED LEARNING APPROACH FOR LOW-RESOURCE LANGUAGES

Abstract. *The article presents a speech synthesis system (TTS) for the Crimean Tatar language, a Turkic language with limited digital resources that is in danger of extinction. We prove that the use of transfer learning based on pre-trained multilingual models makes it possible to achieve high-quality synthesis even with a minimal amount of training data.*

Our approach is based on the Microsoft SpeechT5 architecture, which is further trained on a verified dataset of 1,566 audio recordings (about 2.53 hours). To account for the unique phonological features of the language, a specialized grapheme-phoneme (G2P) preprocessing was applied. The results of tests with native speakers confirm the intelligibility and naturalness of synthesized speech. The trained model and the cleaned dataset are published under open licenses (CC-BY-4.0) to support research in the field of linguistic heritage preservation. The work offers a proven methodology for creating TTS systems for languages with extremely few resources, contributing to the development of AI inclusivity.

Keywords: *SpeechT5, TTS, NLP, AI, Crimean Tatar.*

СЕРГЕЕВ Владимир Анатольевич
научный сотрудник, Институт вычислительной математики и математической геофизики Сибирского отделения Российской академии наук, Россия, г. Новосибирск

ШКАЛА ГЕОКАТАСТРОФИКИ ДЛЯ ЦУНАМИ-ВОЛН

Аннотация. *В статье уточнена единая система параметров характеристики опасных природных процессов (ОПП) геокатастрофики, через эти параметры представлена новая ОПП-шкала для волн цунами, с учётом различий шкал эмпирических исследований – ЭИ-шкал.*

Ключевые слова: *ГК = геокатастрофика, ОПП = опасные природные процессы, ЭИ-шкалы, ОПП-шкалы, ВЦ = волна цунами, параметры ОПП-шкалы.*

Определения термина **«шкала»** (применительно к эмпирическим исследованиям = ЭИ и к фиксации их результатов) вводились в [1; 2, с. 9-110; 3; 4, с. 68-135; 5; 6; 7; 8; 9, с. 131-134]. Компенсация недостатков этих определений была осуществлена в работах [10; 11, с. 125-131]. Далее будем называть такую шкалу **«ЭИ-шкала».** В отличие от неё, шкалу, используемую в теории и практике исследований **ОПП** = опасных природных процессов [12, с. 100; 13, с. 151-216; 14; 15, с. 17-36; 16; 17; 18; 19; 20, с. 49-53; 21], в частности – явлений цунами, будем называть **«ОПП-шкала».**

В геокатастрофике [12, с. 100; 17; 20, с. 49-53] используются различные ОПП-шкалы. **Геокатастрофами (ГК)** будем считать процессы на Земле, приводящие к «большим» человеческим жертвам и\или ущербу людям – материальному и\или моральному. В работе [18], в частности, построена классификация ГК по существенным свойствам ГК и значениям этих свойств.

В наших предыдущих статьях [27, с. 3-11; 28, с. 56-60; 29, с. 84-90] мы осуществили обзор важнейших ОПП-шкал по единой системе параметров, введённых нами предварительно, и получили ответы на вопросы:

- с какими целями построены известные ОПП-шкалы и как они используются?
- чем с логико-математической точки зрения являются ОПП-шкалы и как они отличаются от ЭИ-шкал?
- почему в ОПП-шкалах созданы условия для ограниченно обратимого перехода от данных, заданных в более сложных ЭИ-шкалах, к данным в более простой (порядковой) ЭИ-шкале?

Особый интерес с позиций геокатастрофики для нас представляет шкала для волн цунами. Вариант такой шкалы, шкала Амбрейсиса для определения интенсивности цунами-волн, опубликован в [22, с. 52]. Эта шкала (наряду с другими ОПП-шкалами) охарактеризована нами в [28, с. 56-60] по единой, введённой нами, системе параметров [27, с. 3-11; 28, с. 56-60].

Для единообразного обзора важнейших ОПП-шкал нами введены следующие **параметры для ОПП-шкалы:**

ШN – порядковый номер N рассматриваемой нами ОПП-шкалы из [11, с. 125-131];

ОО – оцениваемые ОБЪЕКТЫ (возможные или реальные) как источники произошедших или потенциально возможных катастроф: астероиды, метеориты, зоны и очаги землетрясений, оползни, вулканы, ураганы, космические потоки солнечных частиц, излучения и др; в случае шкалы для волн цунами таким ОО является сама такая волна;

ПС – ПРЯМЫЕ (целевые) свойства оцениваемых ЯВЛЕНИЙ от ОО (локальная сотрясаемость от землетрясений на поверхности Земли либо от падений астероидов или метеоритов, параметры их кратеров, параметры оползней, ураганов и излучений), вызванных оцениваемыми объектами, в частности волной цунами.

КС – косвенные свойства, которыми оцениваются значения ПС;

ТШ – тип математической шкалы (ЭИ-шкалы из типов Н, П, О, Д – см. [11, с. 125-131]), в которой заданы значения ПС и КС: **Н** – наименований, **П** – порядка, **О** – отношений, **Д** – дискурсивная (словесная);

РА – размерность свойства (для свойства ПС или КС): **РС** – размерное свойство (с указанием единицы измерения), **БС** – безразмерное свойство;

ЧГ – число возможных градаций ПС и КС (по их значениям);

ШГ – величина шага градации (или значений) для ПС и КС;

ДГ – диапазон градаций (или значений) для КС (от минимума до максимума);

ТЗ – тип зависимости (отображения) свойств ПС на КС: **ПЗ** – прямая зависимость (с ростом значения КС растёт значение ПС): ∂(ПС)\$\partial$(КС)>0, **НЗ** – нулевая зависимость ПС (КС), т.е. ПС= const с ростом значения КС и ∂(ПС)\$\partial$(КС)=0; **ОЗ** – обратная зависимость (с ростом значения КС уменьшается значение ПС): ∂(ПС)\$\partial$(КС)<0;

ОВ – оцениваемый вред человечеству как вред от ОО: **ОВФ** – оцениваемый вред формально (по некой методике оценки), **ОВН** – оцениваемый вред неформально.

Результат рассмотрения шкалы Амбрейсиса интенсивности цунами-волн [28, с. 56-60] по введённой системе параметров (для ПС и КС) выглядит так.

ПС1 – амплитуда цунами-волны в открытом море (в м по вертикали); ТШ(ПС1) = А; РА = РС; ДГ, ЧГ, ШГ - не определены; ТИ = МВ; ТЗ = ПЗ; ОВ = ОВН.

Вопрос о том, насколько локация «открытого моря» далека от берега (в милях, в км) или на какой глубине до дна она находится, в шкале Амбрейса не определён.

ПС2 – величина заплеска цунами-волны на берег (в м по горизонтали); ТШ(ПС2) = А; РА = РС; ДГ, ЧГ, ШГ - не определены; ТИ = МВ; ТЗ = ПЗ; ОВ = ОВН.

КС – балл; ТШ (КС) = П; ДГ(КС): от 1 до 6; ЧГ (КС) = 6; ШГ(КС) = 1; ТЗ(КС) = ПЗ; ОВ = ОВН.

Важно, что количество прямых свойств ПС1 и ПС2 в шкале Амбрейсиса недостаточно для всесторонней характеристики отдельной волны цунами или пакета таких волн.

Для компенсации этого недостатка здесь далее предлагается **новая шкала** для волн цунами с подробным описанием её прямых свойств (ПС) и косвенных свойств (КС). Эти свойства кратко были приведены впервые в работе [31, с. 6-9].

Напомним, что очагами, порождающими цунами, помимо землетрясений, могут быть и другие ОО (оцениваемые объекты): астероиды, метеориты, оползни, ураганы. Разработку для них шкал, аналогичных шкалам Ш1 – Ш9 из [27, с. 3-11; 28, с. 56-60], мы оставляем на будущее. Здесь мы введём только шкалу для волн цунами, распространяющихся в океане и достигающих берега. Отметим лишь, что для характеристики этих очагов частично уже используются шкала Ш2 для землетрясений, шкала Ш4 и Ш7 для ураганов и шкала Ш6 для вулканов [27, с. 3-11; 28, с. 56-60]. Для дополнения шкалы Ш2 предстоит разработать шкалу для модели очага, её геометрических и вещественных параметров.

При изучении явлений цунами необходимость использования сильных шкал очевидна. Слабые шкалы используются в следующих ситуациях:

1. Если значение ***x*** является изначально величиной не количественной, а фиксируется в шкале **Н,** или **П,** или **Д**;
2. Если прибор, определяющий ***x*,** грубый;
3. Если при построении классификации данные ***x*** огрубляются из шкалы **А** или **О** в шкалу **Н** или **П.**

Новая шкала геокатастрофики для волн цунами содержит следующие компоненты.

Основные ПРЯМЫЕ свойства ПС = {ПС1, ПС2, ПС3, ПС4, ПС5, ПС6, ПС7, ПС8} волн цунами (ВЦ), а также типы шкал эмпирических исследований (ТШ), в которых могут определяться значения этих свойств ПС рассмотрены далее, а также – косвенные свойства КС.

Оцениваемым объектом (ОО) в данном случае является отдельная волна цунами или пакет цунами-волн (в течение нескольких минут её распространения в точке наблюдений).

Основные прямые свойства ПС

ПС1 – расстояние от очага (источника ВЦ) до заданной точки; ТШ(ПС1) = О; ДГ, ЧГ, ШГ – не определены; РА = РС; ТЗ = ПЗ; ОВ не определён.

ПС2 – расстояние от берега (при мелком шельфе), на котором удаётся обнаружить ВЦ; ТШ(ПС2) = О; ДГ, ЧГ, ШГ – не определены; РА = РС; ТЗ = ПЗ; ОВ не определён.

ПС3 – энергия пакета ВЦ в заданном месте; ТШ(ПС3) = О; ДГ, ЧГ, ШГ – не определены; РА = РС; ТЗ = ПЗ; ОВН или ОВ не определён.

ПС4 – энергия отдельной ВЦ в заданном месте; ТШ(ПС4) = О; ДГ, ЧГ, ШГ – не определены; РА = РС; ТЗ = ПЗ; ОВН или ОВ не определён.

ПС5 – максимальная амплитуда ВЦ в заданном месте; ТШ(ПС5) = О; ДГ, ЧГ, ШГ – не определены; РА = РС; ТЗ = ПЗ; ОВ = ОВН или ОВ не определён.

ПС6 – длина заплеска на берег ВЦ в заданном месте; ТШ(ПС6) = О; ДГ, ЧГ, ШГ – не определены; РА = РС; ТЗ = ПЗ; ОВ = ОВФ, или ОВ = ОВН, или ОВ не определён.

ПС7 – число «больших» набегающих волн от одного очага в заданном месте побережья; ТШ(ПС7) = А; ДГ, ЧГ, – не определены, ШГ = 1;

РА = БС; ТЗ = ПЗ; ОВ = ОВФ, или ОВ = ОВН, или ОВ не определён.

ПС8 – итог разрушающих воздействий ВЦ в заданном месте побережья; ТШ = Д (дискурсивная) либо ТШ = О (в валюте, в шкале отношений О); ДГ, ЧГ, ШГ – не определены; РА = РС, БС; ТЗ = ПЗ; ОВ = ОВФ или ОВ = ОВН.

Свойства ПС1–ПС8 могут быть эмпирическими и\или расчётными, с точечными или интервальными значениями, с точными или с размытыми значениями, с погрешностями определения (с аддитивными или мультипликативными погрешностями, с известными либо нет их законами распределения) либо без погрешностей, имеющими либо нет размерность [11, с. 125-131; 28, с. 79-83]. Их значения задаются в одной из основных шкал измерений [29, с. 6-10]: Н – наименований, П – порядковой, арифметической – одной из четырёх шкал: А – абсолютной (с дискретными значениями либо с континуумом значений), шкалы О – отношений, Р – разностей, И – интервалов (без использования шкалы Д – дискурсивной). Для случая шкалы П чаще применяют 5 градаций, значения которых заданы в шкале Н, а геометрико-временной базис этих значений задаётся либо в шкале А, либо в шкале П.

Итак, свойства ПС1–ПС6 измеряются в сильной шкале (в основном – отношений). Эти данные используются на практике, а также для решения задач с помощью вычислительных методов классической математики. Свойство ПС7 измеряется в абсолютной шкале. За свойством СВ8, на самом деле, стоят многие свойства (геометрические, вещественные и прочие). На основе этих свойств ставятся и решаются задачи с помощью методов неклассической математики.

Отображение (гомоморфное) свойств из ПС8 в одно свойство производится при оценке итога разрушающих воздействий ВЦ в заданном месте побережья либо в баллах (в шкале порядка), либо в валюте (в шкале отношений).

Косвенные свойства КС = {КС1, КС2, КС3, КС4, КС5, КС6, КС7, КС8}, соответствующее предложенным ПРЯМЫМ свойствам ПС = {ПС1, ПС2, ПС3, ПС4, ПС5, ПС6, ПС7, ПС8} волн цунами, будем считать (в соответствии с традицией ОПП-шкал) заданными в ЭИ-шкале типа П, с 12 градациями, с равномерным шагом.

Литература

1. Пфанцагль И. Теория измерений. – М.: 1976. – 225 с.

2. Суппес П., Зиннес Дж. Основы теории измерений // Психологические измерения. – М., Мир, 1967. – С. 9-110.

3. Хованов Н.В. Математические основы теории шкал измерения качества. – Л.: Изд-во ЛГУ, 1982. – 185 с.

4. Орлов А.И. Прикладная теория измерений // Прикладной многомерный статистический анализ. – М.: Наука, 1983. – С. 68-135.

5. Воронин Ю.А., Черемисина Е.Н. О базовых задачах искусственного интеллекта в мультидисциплинарных исследованиях. Часть 1. Описание, сравнение, классифицирование и распознавание. – Новосибирск: Изд-во ИВМиМГ СО РАН, 2001. – 235 с.

6. Загоруйко Н.Г. Прикладные методы анализа данных и знаний. – Новосибирск: Изд-во ИМ СО РАН, 1999. – 270 с.

7. Загоруйко Н.Г. Когнитивный анализ данных. – Новосибирск: Академическое изд-во «Гео», 2013. – 186 с.

8. Воронин Ю.А., Сергеев В.А. Описание геологических тел: итоги и перспективы. – Отчёт о НИР / ВЦ СО АН СССР. – №гос.рег.7653432, Инв.№Б705945. – Новосибирск, 1979 (в 3-х томах). – 675 с.

9. В. Сергеев В.А. Обобщение и формализация понятий о геологическом опробовании // Геология и геофизика. – 1982. – № 6. – С. 131-134.

10. Витяев Е.Е. Информационные технологии знаний, экспертные системы: учебное пособие. – Новосибирск: Изд-во НГУ, 2011. – 225 с.

11. Сергеев В.А. Шкалы свойств и отношений: новая систематика // Актуальные вопросы образования и науки: сборник научных трудов по материалам Международной научно-практической конференции 30.11.2015. Часть 1. М-во обр. и науки РФ. Тамбов: ООО «Консалтинговая компания Юком», 2015. – С. 125-131.

12. Зиновьев П.С., Гусяков В.К., Ляпидевская З.К. Геофизические базы данных по природным катастрофам // Тезисы докладов 5-й Сахалинской молодёжной научной школы «Природные катастрофы: изучение, мониторинг, прогноз» // Южно-Сахалинск, 8-11.6.2010. – С. 100.

13. Mikheeva A.V., Marchuk An.G., Dyadkov P.G. Geoinformation Systems for Studying Seismicity and Impact Cratering using Remote Sensing Data // Geographic Information Systems (GIS): Techniques Applications and Technologies. – Nantes University, France: Nova Science Publishers, 2014. P. 151-216.

14. Робертс Э. Когда сотрясается Земля. М.: Мир, 1966. – 176 с.

15. Гольдин С.В. Физика «живой» Земли // Проблемы геофизики XXI века. – М.: Наука, 2003. – Кн. 1. – С. 17-36.

16. Николаев С.М. Чрезвычайные ситуации и экологические проблемы. - Новосибирск: Академ. Изд-во «Гео», 2007. – 379 с.

17. Резанов И.А. Великие катастрофы в истории Земли. – М.: Наука, 1984. – 176 с.

18. Сергеев В.А. Ураганы. – Отчет о НИР / ИВМиМГ СО РАН. – Новосибирск, 2010. – 54 с. Сайт http//tsun.sscc.ru/.

19. Хлебопрос Р.П., Охонин В.А., Фет А.И. Катастрофы в природе и в обществе: Математическое моделирование сложных систем. – Новосибирск, ИД «Сова», 2008. – 360 с.

20. Sergeev V.A. Analysis of hurricanes as one a sourse of tsunami // Applied and Fundamental Studies: Proceedings of the 5th International Academic Conference. April 29-30, 2014, St. Louis, USA. P. 49-53.

21. Мазур И.И. Опасные природные процессы / И.И. Мазур, О.П. Иванов. – М.: ЗАО «Экономика», 2004. – 702 с.

22. Задонина Н.В. Хронология природных и социальных феноменов в истории мировой цивилизации: монография / Н.В. Задонина, К.Г. Леви. – Иркутск: Изд-во Иркут. Гос. Ун-та, 2009. – 863 с.

23. Самарский А.А., Михайлов А.П. Математическое моделирование: идеи, методы, примеры. – М.: Наука, 1997. – 390 с.

24. Фор К., Кофман А., Дени-Папен М. Современная математика. – М.: Мир, 1966. – 266 с.

25. Марчук Г.И. Методы вычислительной математики. – М.: Наука, 1980. – 535 с.

26. Сергеев В.А. Кейсы классов новой систематики шкал // Актуальные исследования. – № 52(234). – 2024. – С. 79-83.

27. Гусяков В.К., Сергеев В.А. К сертификации шкал измерений для опасных природных процессов // Научный аспект. – № 4. – 2020. – С. 3-11.

28. Сергеев В.А. Особенности шкал геокатастрофики // Актуальные исследования. – № 52, Ч. 1. – 2023. – С. 56-60.

29. Сергеев В.А. Шкалы данных в проблемах геокатастрофики // Актуальные исследования. – № 46(281). – 2025. – С. 84-90. DOI 10.5281/zenodo.17681925. URL: https://apni.ru/article/13589-shkaly-dannyh-v-problemah-geokatastrofiki.

30. Сергеев В.А. Шкалы измерений – к разнообразию данных // Актуальные исследования. – № 46(281). – 2025. – С. 10-16. URL: https://apni.ru/article/13557-shkaly-izmerenij-k-raznoobraziyu-dannyh.

31. Сергеев В.А. Шкалы измерений и отображений в цунами-проблематике // Актуальные исследования. – № 46(281). – 2025. – С. 6-9. URL: https://apni.ru/article/13591-shkaly-izmerenij-i-otobrazhenij-v-cunami-problematike.

SERGEEV Vladimir Anatolyevich
Researcher,
Institute of Computational Mathematics and Mathematical Geophysics
of the Siberian Branch of the Russian Academy of Sciences, Russia, Novosibirsk

GEOCATASTROPHY SCALE FOR TSUNAMI WAVES

Abstract. *The article clarifies the unified system of parameters for the characteristics of hazardous natural processes (HNP) of geocatastrophy, through these parameters a new HNP-scale for tsunami waves is presented, taking into account the differences in the scales of empirical research – EI-scales.*

Keywords: *GC = geocatastrophy, HNP = dangerous natural processes, EI-scales, HNP-scales, TV = tsunami wave, HNP-scale parameters.*

ТИТОВСКИЙ Илья
независимый исследователь, Португалия, г. Порту

ОТ БАНКОВСКИХ ПРИЛОЖЕНИЙ ДО ГЛОБАЛЬНЫХ ПЛАТФОРМ: ЭВОЛЮЦИЯ ТРЕБОВАНИЙ К БЕЗОПАСНОСТИ И НАДЕЖНОСТИ МОБИЛЬНЫХ СИСТЕМ

Аннотация. *Мобильные продукты прошли путь от локальных приложений с ограниченной аудиторией до критически важных сервисов, обслуживающих миллионы пользователей в разных странах и регуляторных средах. Вместе с ростом масштаба меняется и «профиль ответственности» инженерной команды: безопасность и надежность перестают быть набором точечных мер и превращаются в системную архитектурную дисциплину. В статье рассматривается, как эволюционируют требования к защите данных, управлению идентичностью, устойчивости к отказам и операционной наблюдаемости при переходе от банковских мобильных приложений к глобальным цифровым платформам. Показано, почему зрелая безопасность и надежность невозможны без согласованной архитектуры по слоям (клиент–edge–сервисы–данные–наблюдаемость), формализации SLO и управления релизами, а также без ориентации на измеримые показатели риска, доступности и пользовательского доверия.*

Ключевые слова: *мобильная безопасность, надежность, банковские приложения, глобальные платформы, управление идентичностью, MFA, шифрование, SLO, отказоустойчивость, disaster recovery, observability, релизы, риск-менеджмент.*

Введение

Первые мобильные приложения часто развивались как «витрина» сервиса: ограниченный функционал, умеренная нагрузка, простая инфраструктура. По мере роста цифровых экосистем мобильный клиент стал полноценным каналом доступа к финансовым операциям, персональным данным, корпоративным сервисам и государственным функциям. Это автоматически повышает цену ошибки. Если сбой в развлекательном приложении воспринимается как неудобство, то сбой в банковском или крупном сервисе – это уже риск для денег, репутации, регуляторного соответствия и доверия пользователей.

Эволюция требований проявляется в нескольких измерениях одновременно:

1. **Угрозы** становятся разнообразнее (фишинг, SIM-swap, вредоносные приложения, эксплуатация уязвимостей API);
2. **Масштаб** повышает эффект даже небольших дефектов (ошибка затрагивает не сотни, а миллионы);
3. **Сложность инфраструктуры** растет (микросервисы, внешние интеграции, несколько регионов);
4. **Регуляторика и аудит** превращаются в обязательный контур (хранение данных, журналирование, контроль доступа).

В этих условиях безопасность и надежность – это не два отдельных направления, а связанные компоненты зрелой инженерной системы: плохая надежность разрушает доверие, а слабая безопасность делает любой рост токсичным.

1. Как меняются требования при росте масштаба

При переходе от локального продукта к региональному и далее к глобальному масштабу растет интенсивность требований сразу в трех плоскостях: безопасность, надежность/доступность и соблюдение нормативов (compliance, auditability). Это происходит не линейно: требования «скачкообразно» усиливаются при выходе в регулируемые домены (например, финтех) и при географическом расширении.

На ранней стадии достаточно базовых мер: корректная аутентификация, минимальные политики хранения данных, резервное копирование. На уровне банковского приложения появляются обязательные сценарии управления риском: многофакторная аутентификация, антифрод-сигналы, строгие журналы событий, контроль доступа по принципу least privilege. На глобальном уровне добавляются: многорегиональные стратегии, повышенные требования к отказоустойчивости, детальная

наблюдаемость, сегментация данных и регуляторные различия по странам.

2. Банковский контекст: почему мобильная безопасность начинается с идентичности

Банковский продукт ценен не «функциями», а доступом к активам и персональным данным. Поэтому ядро безопасности – это корректная работа с идентичностью:

- сильная аутентификация (включая MFA),
- управление сессиями,
- устойчивость к компрометации устройства и к перехвату каналов,
- защита от социальной инженерии (например, через риск-ориентированные политики).

Важно, что идентичность – это не только логин/пароль. Это набор сигналов и ограничений: устройство, география, поведение, история действий, подтверждения для операций повышенного риска. Чем зрелее продукт, тем чаще используются адаптивные механизмы (risk-based), где система динамически усиливает проверку в зависимости от контекста.

Figure 1. How security, reliability, and compliance requirements evolve with scale (conceptual)

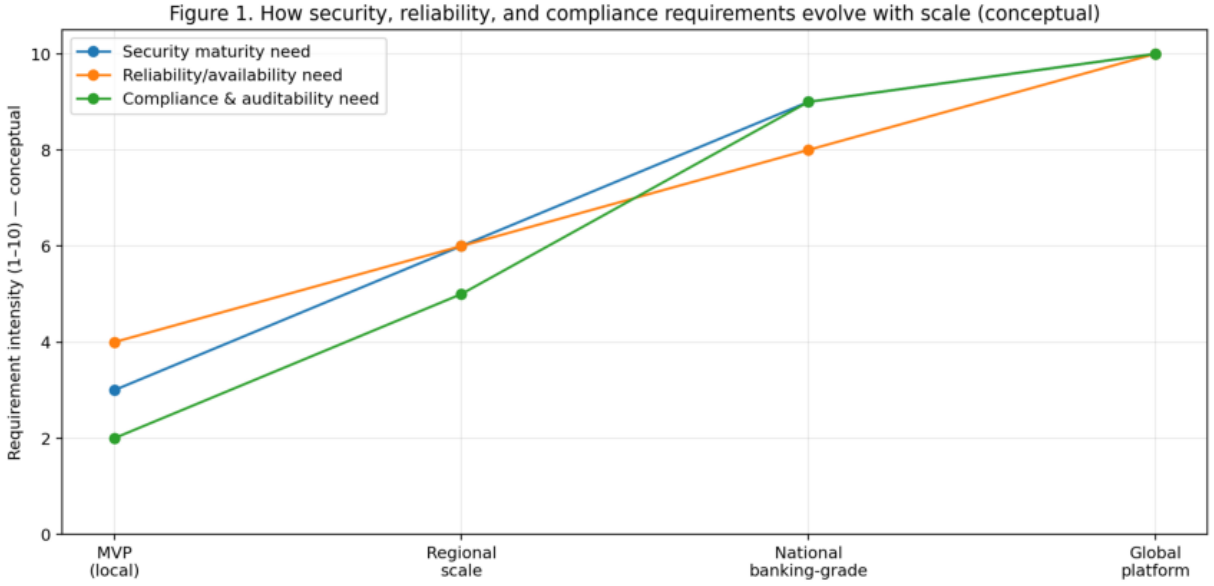

Рис. 1

3. Edge-уровень и API: главная зона атак для масштабных систем

Для глобальных платформ значительная часть атак сосредоточена на API и edge-инфраструктуре. Даже идеально защищенный клиент не спасает, если API позволяет обходить ограничения, извлекать лишние данные или перегружать сервис. Поэтому усиливаются практики:

- централизованное управление входящим трафиком (gateway),
- ограничения частоты (rate limiting) и защита от злоупотреблений,
- фильтрация и сигнатурные/поведенческие механизмы защиты,
- единые политики авторизации и «сужение поверхности» данных (минимизация того, что отдается наружу).

В продуктовой реальности это напрямую связано с экономикой: атаки на API увеличивают расходы (нагрузка), поднимают риск утечки и ухудшают доступность для легитимных пользователей.

4. Надежность как часть доверия: от «аптайма» к SLO

Когда продукт становится критически важным, важно не только «чтобы работало», а чтобы работало с предсказуемым качеством. Именно поэтому зрелые команды переходят от абстрактной «доступности» к SLO:

- какова допустимая доля ошибок?
- какой целевой p95/p99 по задержке в ключевых операциях?
- какой допустимый MTTR?
- какие сценарии считаются деградацией сервиса?

SLO дают два эффекта: делают качество измеримым и управляемым; создают язык для приоритизации – технические инициативы связываются с тем, что критично для пользователя и бизнеса. В банкинге и глобальных платформах надежность – это часть «социального

контракта» с пользователем: сервис не имеет права на хаотичное поведение.

5. Устойчивость к отказам: почему «ретраи» и «таймауты» – это архитектура, а не детали

При росте системы увеличивается число компонентов и зависимостей. Это означает: частичные отказы становятся нормой. Устойчивость строится не на надежде «все всегда доступно», а на правильном поведении при сбоях:

- корректные таймауты,
- ограниченные ретраи (чтобы не усиливать инцидент),
- fallback-сценарии,
- управляемая деградация (сохранение критичных функций),
- планы аварийного восстановления (DR).

На практике именно эти «мелкие» инженерные настройки решают судьбу инцидентов: либо система локализует проблему, либо превращает частичный сбой в каскад.

6. Защита данных: шифрование, секреты и дисциплина доступа

С ростом продукта усложняется контур данных: больше интеграций, больше сервисов, больше мест хранения и передачи. Это создает потребность в комплексной модели защиты:

- шифрование «в покое» и «в пути»,
- управление секретами (а не хранение ключей «рядом с кодом»),
- сегментация доступа и аудит,
- минимизация выдаваемых данных и контроль того, что логируется.

Особенно важно учитывать, что безопасность уязвима к «операционным утечкам»: не только через прямые атаки, но и через неправильные логи, чрезмерные права сервисных аккаунтов, тестовые окружения и некорректно настроенные доступы.

7. Наблюдаемость: без нее нельзя управлять ни безопасностью, ни надежностью

Наблюдаемость (логи/метрики/трейсы) превращает безопасность и надежность в управляемые процессы. Для зрелых мобильных продуктов важны две стороны наблюдаемости:

- серверная (что происходит внутри сервисов и инфраструктуры),
- клиентская (что реально испытывает пользователь: время запуска, сеть, краши, деградации).

Без этой связки команда не видит «истинной картины»: сервер может быть «зеленым», а пользователи – страдать из-за сетевых условий, тяжелых экранов, проблем на конкретных устройствах. В масштабных продуктах именно эта слепота часто приводит к потере доверия.

Figure 2. Security and reliability layers for mobile systems (conceptual)

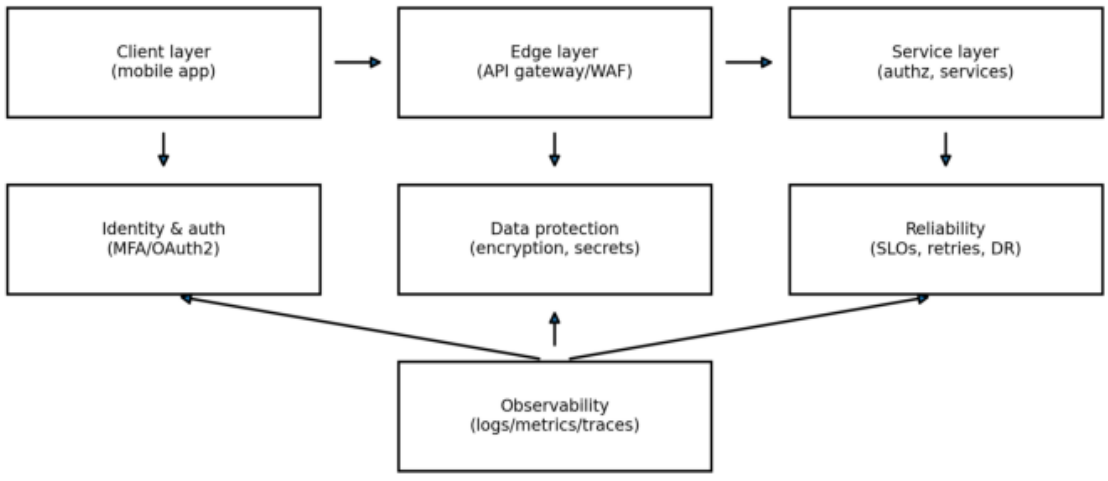

Рис. 2

8. Релизы как фактор риска: почему безопасные изменения – это управляемые изменения

По мере роста системы изменяется и роль релизов: каждое изменение становится потенциальным источником инцидента. Поэтому в зрелых командах релиз – это управляемый процесс:

- постепенные раскатки,
- возможность быстрого отката,
- совместимость версий клиента и сервера,
- контроль регрессий по метрикам,
- фиксация влияния изменений на SLO и продуктовые KPI.

В банковских и глобальных продуктах релизная дисциплина – это часть безопасности: «непредсказуемая доставка» часто приводит к нарушениям доступности и росту операционных рисков.

Заключение

Эволюция от банковских мобильных приложений к глобальным платформам усиливает требования к безопасности и надежности не «в два раза», а качественно. Идентичность становится ядром защиты, API и edge-уровень – ключевой зоной атак и контроля, а надежность – измеримой обязанностью через SLO и практики устойчивости к частичным отказам. Защита данных требует дисциплины доступа и операционной зрелости, а наблюдаемость связывает технические сигналы с пользовательской реальностью. В итоге масштабирование превращается не в «добавим мощности», а в системный инженерный процесс: архитектура, эксплуатация, релизы и метрики работают как единый контур управления доверием пользователя.

Литература

1. Beyer B. et al. Site Reliability Engineering. O'Reilly.
2. Nygard M. Release It!. Pragmatic Bookshelf.
3. OWASP Mobile Security Testing Guide (MSTG).
4. OWASP API Security Top 10.
5. Kleppmann M. Designing Data-Intensive Applications. O'Reilly.

TITOVSKY Ilya
Independent Researcher, Portugal, Porto

FROM BANKING APPLICATIONS TO GLOBAL PLATFORMS: EVOLVING REQUIREMENTS FOR THE SECURITY AND RELIABILITY OF MOBILE SYSTEMS

Abstract. *Mobile products have gone from local applications with limited auditing to mission-critical services serving millions of users in different countries and regulatory environments. With the growth of scale, the "responsibility profile" of the engineering team is also changing: safety and reliability are no longer a set of point measures and are becoming a systemic architectural discipline. The article examines how the requirements for data protection, identity management, fault tolerance, and operational observability are evolving in the transition from mobile banking applications to global digital platforms. It has been shown why mature security and reliability are impossible without a consistent architecture across layers (client-edge–services–data–observability), SLO formalization and release management, as well as without focusing on measurable indicators of risk, availability and user trust.*

Keywords: *mobile security, reliability, banking applications, global platforms, identity management, MFA, encryption, SLO, fault tolerance, disaster recovery, observability, releases, risk management.*

ЧИХАЧЕВ Илья Александрович
студент,
МИРЭА – Российский технологический университет,
Россия, г. Москва

НЕЙЛЫК Денис Игоревич
студент,
МИРЭА – Российский технологический университет,
Россия, г. Москва

Научный руководитель – доцент кафедры практической и прикладной информатики МИРЭА – Российского технологического университета, кандидат педагогических наук Геращенко Людмила Андреевна

МОДЕЛИРОВАНИЕ БИЗНЕС-ПРОЦЕССОВ СЛУЖБЫ ДОСТАВКИ ПРОДУКТОВ

Аннотация. *В статье рассматривается подход к моделированию бизнес-процессов службы доставки продуктов как основы проектирования информационной системы. Описаны применяемые нотации моделирования (BPMN, DFD) и их роль на различных этапах разработки системы. Для процесса «Оформление и доставка заказа» построение модель, позволяющая узкие места. На основе полученных моделей спроектированы логическая структура базы данных. Показано, что систематическое моделирование бизнес-процессов упрощает постановку задачи разработчикам, снижает риск логических ошибок и служит основой для дальнейшей автоматизации и оптимизации, включая применение технологий RPA. В качестве предметной области используется курьерская служба.*

Ключевые слова: *бизнес-процесс, моделирование, BPMN, DFD, служба доставки продуктов, информационная система, документооборот.*

Введение

Быстрое развитие рынка доставки продуктов и высокая конкуренция приводят к тому, что компании вынуждены постоянно повышать качество сервиса и снижать издержки. Значительная часть работы таких компаний представляет собой формализуемые бизнес-процессы: прием и обработка заказов, распределение курьеров, взаимодействие с партнёрскими ресторанами, расчеты с клиентами и партнерами, формирование отчетности.

Для того чтобы автоматизация этих процессов была устойчивой и прозрачной, требуется предварительное моделирование бизнес-процессов. Модели позволяют наглядно описать взаимодействие подразделений, информационные потоки и документы, выявить дублирующие операции и узкие места.

Цель данного исследования – используя средства моделирования бизнес-процессов, описать деятельность службы доставки продуктов, спроектировать информационную систему, поддерживающую ключевые операции компании. Объектом исследования явились курьерские службы

Теоретические основы моделирования бизнес-процессов

Под бизнес-процессом понимают совокупность взаимосвязанных работ, преобразующих входы (ресурсы, информацию, запрос клиента) в результат, имеющий ценность для внутреннего или внешнего потребителя [1, с. 15].

Общепринято выделять несколько групп процессов: основные, вспомогательные, обеспечивающие и процессы управления. Основные процессы непосредственно создают ценность для клиента, вспомогательные поддерживают выполнение основных операций, обеспечивающие формируют инфраструктуру, а процессы управления связаны со

стратегическим и оперативным планированием и контролем эффективности.

Для описания бизнес-процессов используется ряд нотаций: BPMN (Business Process Model and Notation), DFD (диаграммы потоков данных), ER-диаграммы (Entity-Relationship), а также схемы маршрутов документов. BPMN позволяет описывать последовательность работ, события и условия, DFD акцентирует внимание на источниках и хранилищах информации, ER-диаграммы используются для проектирования структуры данных, а маршруты документов отображают движение конкретных форм и отчетов между участниками процесса [2, с. 10-17; 6, с. 1-37].

Результаты исследования

BPMN-диаграммы процессов легли в основу функциональности веб-приложения. Для каждой группы задач были выделены отдельные модули: управление заказами, управление справочниками клиентов, сотрудников и продуктов, формирование отчетов и генерация документов. Такое соответствие «задача процесса – функция системы» позволяет избежать пропусков и дублирования функциональности.

Основными участниками, рассматриваемого в исследовании процесса в службах доставки являются: сотрудники отдела клиентской поддержки, логистический отдел, курьеры, финансовый и технический отделы.

К основным бизнес-процессам можно отнести:

- прием и регистрация заказа,
- подтверждение и передача заказа ресторану,
- назначение курьера и планирование маршрута,
- доставка заказа клиенту,
- получение оплаты,
- сбор обратной связи.

К вспомогательным:

- поддержка работы курьеров,
- управление партнерскими ресторанами,
- маркетинг и PR.

К обеспечивающим:

- ИТ-поддержка,
- финансовое и юридическое сопровождение.

Процессы управления связаны с планированием и анализом эффективности.

Ключевым для компании является процесс обслуживания конкретного заказа клиента. Его удобно описывать в нотации BPMN, выделив несколько дорожек: «Мобильное приложение», «Отдел клиентской поддержки», «Ресторан-партнер», «Отдел логистики», «Курьер», «Платежный сервис».

Последовательность действий включает формирование заказа клиентом, передачу его в систему, проверку и подтверждение, назначение курьера, получение заказа в ресторане, доставку клиенту и фиксирование результата в информационной системе. На каждом шаге определяются ответственные подразделения и точки контроля качества.

Для анализа информационного обмена была построена диаграмма потоков данных уровня 0.

Проведена детализация процесса «Обслуживание конкретного заказа клиента» – «Оформление заказа» (рис.).

Для службы доставки важны как электронные, так и бумажные документы. Можно выделить внутренние документы (отчеты о занятости курьеров, графики смен), исходящие документы (договоры с ресторанами-партнерами, инвойсы для клиентов) и входящие документы (жалобы и обращения клиентов, письма от партнеров). Для каждого документа построен маршрут: кто его инициирует, кто согласует, кто утверждает и где он хранится. Это позволяет стандартизировать документооборот и задать регламенты обработки обращений.

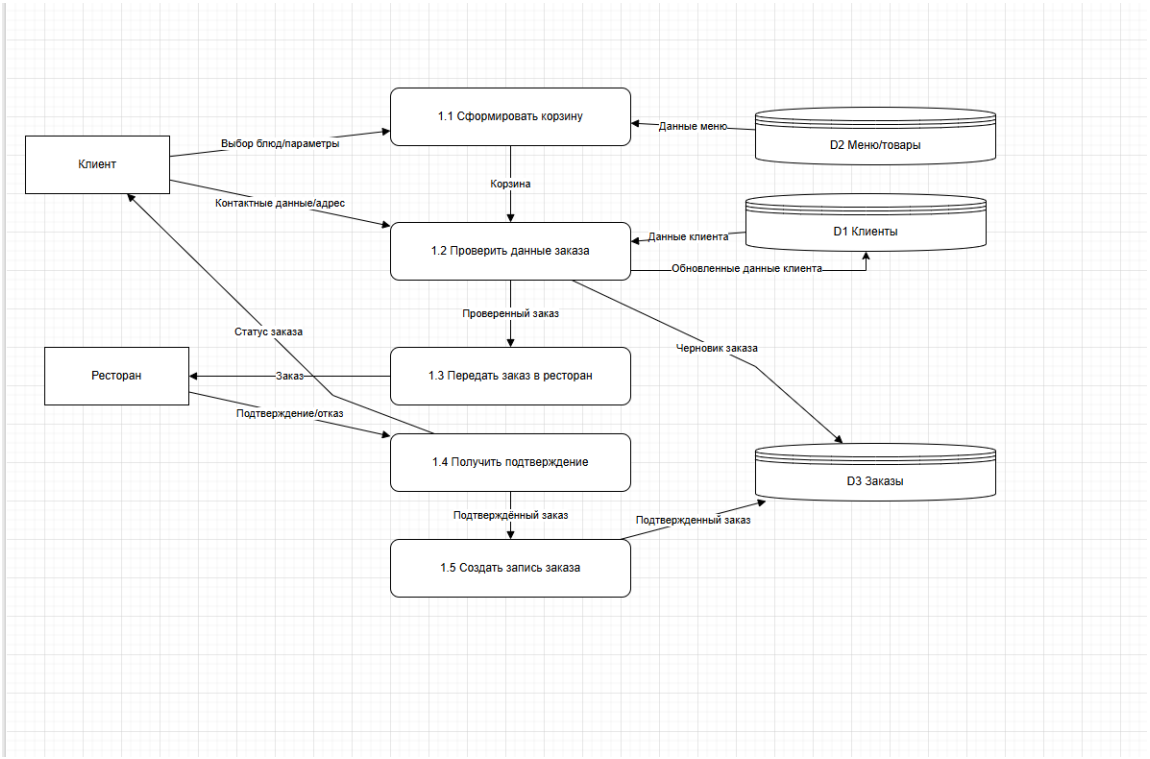

Рис. Диаграмма потоков данных (DFD) уровня 1 процесса «Оформление заказа»

На основе DFD диаграммы и маршрутов документов спроектирована логическая структура базы данных. Такая структура обеспечивает целостность данных и удобна для реализации CRUD-операций в веб-приложении.

На основе маршрутов документов и структуры базы данных разработаны шаблоны текстовых и табличных документов. Переменные в шаблонах группируются по логике: параметры договора, данные клиента, данные сотрудника, реквизиты заказа и агрегированные показатели отчета. При генерации документов значения автоматически подставляются из базы данных, что обеспечивает единообразие оформления и снижает трудозатраты сотрудников.

Наличие формализованных моделей открывает возможности для более глубокого внедрения технологий автоматизации. В частности, процессы, связанные с обработкой однотипных запросов и заполнением типовых форм, могут быть дополнительно оптимизированы средствами Robotic Process Automation (RPA), которые имитируют действия пользователя в интерфейсе и выполняют рутинные операции без участия человека. Модели бизнес-процессов служат исходной спецификацией для настройки таких RPA-ботов [4, с. 126].

При построении BPMN-модели и DFD выявляются типовые места возникновения задержек: ожидание подтверждения ресторана, отсутствие свободного курьера в зоне доставки, а также ошибки в контактных данных клиента. Формализация шагов процесса позволяет закрепить контрольные точки и задать правила обработки исключений.

На основе маршрутов документов и модели данных определяются показатели, которые целесообразно фиксировать в системе: время обработки заказа на каждом этапе, процент отмен, среднее время назначения курьера, доля доставок с опозданием, а также нагрузка по сменам. Эти показатели используются для управленческой отчетности и для настройки уведомлений персоналу. Наличие единой структуры данных и регламентов ввода обеспечивает сопоставимость статистики и снижает влияние человеческого фактора.

Построенные и проанализированные модели позволяют определить перечень функций, которые дают максимальный эффект при автоматизации: автоматическое распределение заказов по курьерам с учетом географии, генерация документов и отчетов по шаблонам, а также унификация справочников (клиенты, рестораны, товары). Для рутинных операций (перенос данных между системами, формирование типовых отчетов) допускается применение RPA как дополнительного уровня автоматизации при сохранении единого источника данных в базе [4, с. 126].

Заключение

Использование нотаций BPMN, DFD, ER-диаграмм и схем маршрутов документов обеспечивает многогранный взгляд на систему – от логики выполнения операций до организации хранения и обработки информации.

Построенные модели служат основой для разработки структуры базы данных, проектирования функциональных модулей веб-приложения, стандартизации документооборота и дальнейшей автоматизации рутинных операций, в том числе с применением технологий RPA. Таким образом, системное моделирование бизнес-процессов является необходимым этапом при создании информационных систем сервисных компаний и важным инструментом повышения эффективности их работы.

Литература

1. Харрингтон Д. Оптимизация бизнес-процессов. – М.: Стандарты и качество, 2007 https://pqm-online.com/assets/files/lib/books/harrington1.pdf (дата обращения 11.11.2025).

2. Геращенко Л.А. Документирование как ключ к эффективному моделированию бизнес-процессов в образовательных организациях / Л.А. Геращенко, А.А. Карева, Е.Д. Гасилин // Наукосфера. – 2024. – № 12-2. – С. 10-17.

3. Ахмедова Х.Г. Разработка качественных требований к программным системам / Х.Г. Ахмедова, Л.А. Геращенко // Экономика и общество России: национальные интересы и направления развития: Материалы всероссийской научно-практической конференции, Саратов, 18 ноября 2024 года. – Саратов: ООО «Амирит», 2024. – С. 11-15. – EDN VXVRSU.

4. Uskenbayeva R.K., Kuandykov A.A., Nalgozhina N.Zh., Berklaiyeva M.A. RPA approach in Business Process Management life cycle // Вестник Алматинского университета энергетики и связи. – 2022. – № 1(56). – С. 126-132.

5. Куренков А.А. Метод оценки эффективности применения технологии RPA / А.А. Куренков // Развитие современного общества: вызовы и возможности: Материалы XVII международной научной конференции, в 4 ч., Москва, 02 апреля 2021 года. Т. 1. – Москва: Московский университет им. С.Ю. Витте, 2021. – С. 471-476.

6. Van der Aalst W. Business Process Management: A Comprehensive Survey // Software and Systems Modeling. – 2013. – Vol. 11, No. 3. – P. 1-37.

CHIKHACHEV Ilya Aleksandrovich
Student, MIREA – Russian Technological University, Russia, Moscow

NEILYK Denis Igorevich
Student, MIREA – Russian Technological University, Russia, Moscow

Scientific Advisor – Associate Professor of the Department of Practical and Applied Informatics at MIREA – Russian Technological University, Candidate of Pedagogical Sciences Gerashchenko Lyudmila Andreevna

MODELING OF BUSINESS PROCESSES OF THE PRODUCT DELIVERY SERVICE

Abstract. *The article discusses an approach to modeling business processes of a product delivery service as a basis for designing an information system. The article describes the modeling notations used (BPMN, DFD) and their role at various stages of system development. For the "Order processing and delivery" process, a model is constructed that allows for identifying bottlenecks. Based on the obtained models, a logical database structure is designed. The article shows that systematic modeling of business processes simplifies the task formulation for developers, reduces the risk of logical errors, and serves as a basis for further automation and optimization, including the use of RPA technologies. The courier service is used as the subject area.*

Keywords: *business process, modeling, BPMN, DFD, product delivery service, information system, document management.*

АРХИТЕКТУРА, СТРОИТЕЛЬСТВО

САМСОНОВ Геннадий Сергеевич
студент, Санкт-Петербургский государственный архитектурно-строительный университет, Россия, г. Санкт-Петербург

ПРИНЦИП РАБОТЫ ВОЗДУХОРАСПРЕДЕЛИТЕЛЕЙ ЛАМИНАРНОГО ПОТОКА В СИСТЕМАХ ВЕНТИЛЯЦИИ ДЕТСКИХ МЕДИЦИНСКИХ ПОМЕЩЕНИЙ

Аннотация. *В статье рассмотрены принципы организации работы воздухораспределителей ламинарного потока и их роль в системах приточно-вытяжной вентиляции помещений детских медицинских организаций. Описано функциональное назначение ламинарных панелей как элемента системы воздухораспределения, обеспечивающего однонаправленное движение воздуха и снижение микробной и аэрозольной нагрузки в зоне пребывания пациента. Особое внимание уделено аэродинамическим характеристикам ламинарных устройств, выбору геометрических параметров и распределения скоростей для достижения устойчивого ламинарного режима. Приведены рекомендации по проектированию и размещению воздухораспределителей ламинарного потока в операционных и процедурных кабинетах детской поликлиники, позволяющие повысить эффективность вентиляции и обеспечить требуемые параметры микроклимата и инфекционной безопасности.*

Ключевые слова: *ламинарный поток, воздухораспределитель, детская поликлиника, микроклимат, вентиляция, операционная, процедурный кабинет.*

Введение

Обеспечение нормируемых параметров микроклимата и санитарно-эпидемиологической безопасности в детских медицинских учреждениях является одной из наиболее сложных инженерных задач. Особенно высокие требования предъявляются к помещениям, где выполняются инвазивные манипуляции: операционные, перевязочные, процедурные и прививочные кабинеты. В таких помещениях требуется не только поддержание температуры, влажности и кратности воздухообмена, но и эффективное управление направлением и структурой воздушных потоков в зоне пациента.

Традиционные схемы перемешивающей вентиляции с подачей воздуха через обычные решётки или диффузоры не обеспечивают достаточного контроля над движением частиц и аэрозолей, что может приводить к перераспределению микробной нагрузки по всему объёму помещения. В ответ на эти вызовы в практике проектирования всё шире применяются воздухораспределители ламинарного потока, формирующие однонаправленное нисходящее течение воздуха в зоне операционного поля или процедурного стола.

Функциональное назначение воздухораспределителей ламинарного потока

Воздухораспределитель ламинарного потока представляет собой устройство, предназначенное для подачи обработанного воздуха в помещение в виде упорядоченного, слаботурбулентного потока, движущегося параллельными слоями с практически одинаковой скоростью. Такое устройство обычно выполняется в виде потолочной панели или системы модулей, расположенных над зоной, требующей повышенной чистоты и стабильности микроклимата.

Основные функции ламинарного воздухораспределителя в детских медицинских помещениях:

- формирование нисходящего потока чистого воздуха над операционным полем или процедурным столом;

- вытеснение загрязнённого воздуха и аэрозолей из зоны дыхания пациента и персонала;
- снижение вероятности перекрёстного переноса частиц от персонала и оборудования к раневой поверхности;
- обеспечение равномерного распределения температуры и скорости воздуха в рабочей зоне при сохранении комфортных условий для детей.

Размещение ламинарной панели непосредственно над критической зоной (операционный стол, кушетка для манипуляций, прививочный стол) обусловлено необходимостью создать «зону чистого воздуха», в которой направление движения частиц строго контролируется и направлено от фильтрующего элемента к периферии помещения.

Аэродинамические принципы работы ламинарного воздухораспределителя

Работа воздухораспределителя ламинарного потока основана на преобразовании потенциальной энергии давления в равномерное распределение скорости по выходной поверхности. Для этого внутри панели формируется система камер и распределительных каналов, выравнивающих давление до выхода воздуха через перфорированную или решётчатую поверхность.

В противоположность перемешивающей вентиляции, где высокоскоростные струи создают развитую турбулентность, ламинарный воздухораспределитель работает в режиме малых скоростей и минимальной турбулентной пульсации. Условие ламинарности достигается сочетанием следующих факторов:

- ограничение скорости истечения воздуха из панели (как правило, 0,25–0,45 м/с в рабочей зоне для медицинских помещений);
- достаточная удалённость препятствий от выходной поверхности, обеспечивающая развитие однородного профиля скорости по высоте;
- отсутствие резких местных возмущений потока в зоне действия панели (выступающие конструкции, интенсивно обдуваемые элементы).

При правильно подобранных параметрах воздух, выходящий из панели, движется практически вертикально вниз, вытесняя загрязнённый воздух к периферийным зонам, где организована вытяжка. Это позволяет локализовать источник чистого воздуха над наиболее критичной областью и минимизировать горизонтальный перенос частиц.

Конструктивные характеристики и основные параметры

При проектировании воздухораспределителей ламинарного потока для детских операционных и процедурных кабинетов особое значение имеют геометрические размеры панели, структура распределительных каналов и параметры выходной поверхности.

Площадь панели и её положение

Размер панели выбирается таким образом, чтобы зона ламинарного потока полностью перекрывала рабочую область: операционный стол или процедурную кушетку с запасом по периметру. Для малой операционной или процедурного кабинета целесообразно применение панелей площадью порядка 4–6 м², расположенных симметрично относительно оси стола.

Скорость воздуха на выходе

Допустимый диапазон скоростей в медицинских ламинарных панелях обычно составляет 0,25–0,45 м/с в зоне пациента. При меньших скоростях ухудшается эффективность вытеснения загрязнённого воздуха, при больших возрастает риск дискомфорта и переохлаждения, особенно у детей.

Распределение отверстий и сопротивление

Выходная поверхность ламинарного воздухораспределителя выполняется в виде мелкоячеистой перфорации или решётки с равномерным распределением отверстий по площади. Внутренние распределительные камеры и перфорированные листы подбираются так, чтобы обеспечить минимальные отклонения скорости по поверхности и достаточное внутреннее сопротивление для выравнивания давления.

Фильтрация воздуха

В ряде случаев непосредственно перед ламинарной панелью устанавливаются высокоэффективные фильтры (например, HEPA-класса), что позволяет подавать в зону операции или манипуляций воздух с существенно сниженной микробной и пылевой нагрузкой.

Расчётные основы выбора параметров ламинарной панели

Расчёт ламинарного воздухораспределителя начинается с определения требуемого расхода приточного воздуха на помещение исходя из кратности воздухообмена, тепловой нагрузки и санитарных требований. Далее расход,

предназначенный для зоны ламинарного потока, распределяется по площади панели с учётом выбранной скорости истечения.

При известной суммарной подаче L и допустимой средней скорости воздуха v площадь выходной поверхности панели определяется по зависимости

$$A = \frac{L}{3600v}, \quad (1)$$

Где A – площадь панели, м², L – расход воздуха, м³/ч, v – скорость воздуха, м/с.

Дополнительно выполняется оценка перепада давления на распределительных элементах и фильтрах, чтобы обеспечить устойчивый режим работы установки и сохранить требуемую скорость истечения при изменении аэродинамического сопротивления в процессе эксплуатации (засорение фильтров, изменение конфигурации помещения).

Влияние схемы размещения на микроклимат и безопасность

Расположение ламинарных воздухораспределителей в пространстве помещения определяет конфигурацию нисходящих потоков и эффективность вытеснения загрязнённого воздуха. Размещение панели строго над операционным столом с организованной вытяжкой по периметру пола или в верхней зоне стен позволяет сформировать направленный поток от центра к периферии, минимизируя возврат частиц в критическую зону.

В процедурных и прививочных кабинетах ламинарная панель может располагаться над манипуляционной зоной, в то время как общая приточно-вытяжная вентиляция обеспечивает фоновые параметры микроклимата. Такой подход даёт возможность сочетать высокую степень локальной чистоты с умеренной кратностью воздухообмена во всём помещении, что особенно важно с точки зрения энергоэффективности.

Использование ламинарных воздухораспределителей позволяет:

- снизить микробную нагрузку в зоне операционного или процедурного поля за счёт направленного вытеснения аэрозолей;
- уменьшить риск перекрёстного инфицирования между пациентом и персоналом;
- обеспечить более равномерное распределение температуры и скорости воздуха в рабочей зоне при сохранении комфортных условий для детей.

Особенности эксплуатации и надёжности

Эффективность работы ламинарных воздухораспределителей напрямую зависит от состояния фильтров и чистоты внутренних поверхностей. В процессе эксплуатации необходимо:

- обеспечивать регулярную замену фильтрующих элементов согласно регламенту и показаниям по перепаду давления;
- контролировать фактическую скорость воздуха в зоне панели, периодически выполняя замеры в контрольных точках;
- не допускать размещения крупногабаритного оборудования в непосредственной близости от выходной поверхности, чтобы не нарушать структуру потока.

При проектировании важно предусмотреть удобный доступ к фильтрам и внутренним элементам панели для обслуживания, а также возможность регулировки расхода воздуха, что позволяет адаптировать систему к изменяющимся условиям эксплуатации и требованиям по чистоте.

Сравнение с традиционными схемами воздухораспределения

По сравнению с обычными приточными решётками и диффузорами, создающими перемешивающие турбулентные потоки, ламинарные воздухораспределители обеспечивают более высокий уровень контроля над направлением движения воздуха и распределением частиц. В традиционных системах значительная часть загрязнений может циркулировать по всему объёму помещения, в том числе над критической зоной, тогда как ламинарная схема ориентирована на вытеснение загрязнённого воздуха из рабочей области.

Однако ламинарные панели требуют более высокой точности расчёта, качественной подготовки воздуха и повышенного внимания к эксплуатации. Их применение оправдано прежде всего в помещениях с повышенными требованиями к чистоте и стабильности микроклимата, что полностью соответствует задачам детских операционных и ряда процедурных кабинетов.

Заключение

Воздухораспределители ламинарного потока являются ключевым элементом современных систем вентиляции помещений детских медицинских учреждений с повышенными требованиями к санитарно-эпидемиологической безопасности. Правильный выбор геометрических параметров, скорости истечения и

схемы размещения позволяет сформировать устойчивый нисходящий поток чистого воздуха в зоне пациента, снизить микробную и аэрозольную нагрузку и обеспечить высокий уровень теплового и психологического комфорта для детей.

Применение ламинарных воздухораспределителей в составе комплексной системы ОВИК детской поликлиники целесообразно рассматривать как эффективный инструмент повышения качества микроклимата и безопасности при проведении инвазивных процедур и операций. В дальнейшем данное решение может быть дополнено численным моделированием и экспериментальными исследованиями для уточнения параметров потоков в конкретных планировочных и эксплуатационных условиях.

Литература

1. СНиП 41-01-2003 «Отопление, вентиляция и кондиционирование воздуха». – М.: Стройиздат, 2003.
2. СП 60.13330.2020 «Вентиляция и кондиционирование воздуха». – М.: Министерство строительства Российской Федерации, 2020.
3. СП 158.13330.2014 «Здания и помещения медицинских организаций. Правила проектирования».

SAMSONOV Gennady Sergeevich
Student, Saint Petersburg State University of Architecture and Civil Engineering,
Russia, Saint Petersburg

THE PRINCIPLE OF OPERATION OF LAMINAR FLOW AIR DISTRIBUTORS IN VENTILATION SYSTEMS OF CHILDREN'S MEDICAL FACILITIES

Abstract. *The article discusses the principles of the organization of the laminar flow air distributors and their role in the supply and exhaust ventilation systems of children's medical organizations. The functional purpose of laminar panels as an element of the air distribution system, providing unidirectional air movement and reducing microbial and aerosol loads in the patient's area of stay, is described. Special attention is paid to the aerodynamic characteristics of laminar flow devices, the choice of geometric parameters and velocity distribution to achieve a stable laminar flow regime. Recommendations are given on the design and placement of laminar flow air distributors in the operating rooms and treatment rooms of a children's polyclinic, which make it possible to increase ventilation efficiency and ensure the required parameters of the microclimate and infection safety.*

Keywords: *laminar flow, air distributor, children's polyclinic, microclimate, ventilation, operating room, treatment room.*

Актуальные исследования

Международный научный журнал
2025 • № 51 (286)
Часть I

ISSN 2713-1513

Подготовка оригинал-макета: Орлова М.Г.
Подготовка обложки: Ткачева Е.П.

Учредитель и издатель: ООО «Агентство перспективных научных исследований»
Адрес редакции: 308000, г. Белгород, пр-т Б. Хмельницкого, 135
Email: info@apni.ru
Сайт: https://apni.ru/

Отпечатано в ООО «ЭПИЦЕНТР».
Номер подписан в печать 30.12.2025г. Формат 60×90/8. Тираж 500 экз. Цена свободная.
308010, г. Белгород, пр-т Б. Хмельницкого, 135, офис 40