ISSN 2686-9373

ВЕСТНИК СОВРЕМЕННЫХ ЦИФРОВЫХ ТЕХНОЛОГИЙ

20. 2024 (СЕНТЯБРЬ)

Издание включено в перечень ВАК (специальности: 2.3.2, 2.3.6, 2.3.8, 5.2.4)

5 лет ЮБИЛЕЙНЫЙ ВЫПУСК

ВЕСТНИК

СОВРЕМЕННЫХ ЦИФРОВЫХ ТЕХНОЛОГИЙ

НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ

№20

СЕНТЯБРЬ 2024

www.c3da.org

ISSN 2686-9373

Издатели: *Российский государственный социальный университет*
Ассоциация РКЦФА

Адрес редакции и издателя: 129226, Москва,
ул. Вильгельма Пика, д.4, стр.1
www.c3da.org

РГСУ

Подписано в печать 30.09.2024 г.
Тираж 500 экз.
Подписной индекс в каталоге «Пресса России»: 79111

Свидетельство о регистрации СМИ
ПИ № ФС 77-76187 от 08.07.2019 г.

Журнал включен в перечень рецензируемых научных изданий ВАК, в которых должны быть опубликованы основные результаты диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук.
(2.3.2) Вычислительные системы и их элементы
(2.3.6) Методы и системы защиты информации, информационная безопасность
(2.3.8) Информатика и информационные процессы
(5.2.4) Финансы

РЕДАКЦИОННЫЙ СОВЕТ

РЕДАКЦИОННОЕ ПРИМЕЧАНИЕ

В сентябре этого года мы отмечаем пятилетие нашего журнала, оперативно публикующего значимые достижения российских и зарубежных ученых в области цифровых технологий. Журнал прошел непростой, но славный и достойный путь и ныне входит в перечень ВАК.

Наш успех стал возможен благодаря постоянной помощи и поддержке нашего редакционного совета, членам которого мы бы хотели выразить огромную благодарность!

Наш председатель – Александр Сергеевич Сигов, академик Российской академии наук, заслуженный деятель науки Российской Федерации – настоящий маяк в мире большой науки. Он определял стратегии научной работы и исследовательских поисков, поддерживал высокий уровень журнала и не только призывал нас к новым рубежам, победам и достижениям, но и всемерно способствовал им.

Внимательнейший и милейший Андрей Леонидович Хазин – ректор Российского государственного социального университета, академик Российской академии художеств, человек исключительной доброты и крупный ученый – также неизменно кропотливо, терпеливо и внимательно помогал нам и призывал к высокому научному и, что не менее важно, художественному качеству наших материалов.

Сопредседатель Редакционного Совета Джомарт Фазылович Алиев – доктор философии в области бизнес-права, доктор делового администрирования в области финансов (DBA), кандидат экономических наук, первый проректор Российского государственного социального университета – оригинальный философ и глубокий мыслитель, настоящий образец современного ученого, автор целого ряда новых концепций в современных естественных и гуманитарно-социальных науках. Своим руководством он неизменно укреплял и поддерживал нас, а непосредственным авторством в журнале вывел наши публикации на новый уровень.

Георгий Сергеевич Елизаров – академик Академии Криптографии РФ – внимательно и постоянно курировал вопросы информационной безопасности в наших публикациях и глубоко вникал в нашу повседневную работу.

Наш журнал просто невозможно представить без внимательного и каждодневного участия болеющих за наше общее дело поддержки науки и просвещения редакции, ученого секретаря Алины Александровны Рязановой и ответственной за дизайн и верстку Груздевой Натальи Владимировны. Они неустанно улучшают качество издания, обеспечивают безупречные публикации и организационный процесс.

Сергей Владимирович Запечников – доктор технических наук, доцент, профессор Института интеллектуальных кибернетических систем университета «МИФИ» – не только большой ученый, но и наш постоянный автор. Благодаря его высочайшей квалификации в области криптографии и компьютерной безопасности поддерживается высокое качество наших публикаций по этой тематике.

Татьяна Витальевна Кириченко – доктор экономических наук, профессор, заместитель заведующего кафедрой безопасности цифровой экономики РГУ нефти и газа имени И.М. Губкина – наша звезда в области экономики и финансов. Для многих поколений студентов-выпускников она настоящая заботливая мама и совершенно справедливо, что именно она рекомендует нам и продвигает лучшие студенческие работы.

Академический ученый Александр Викторович Князев – доктор физико-математических наук, профессор, директор Института точной механики и вычислительной техники им. С.А.Лебедева – помогал нам не только ориентироваться в мире науки, но и не заблудиться в коридорах научного администрирования. Александр Викторович твердо задавал нам курс к высокому уровню публикаций в области ИТ и аппаратных решений.

Алексей Алексеевич Комзолов – доктор экономических наук, профессор, заведующий кафедрой безопасности цифровой экономики РГУ нефти и газа имени И.М. Губкина – отразил в своей редакционной работе свойственное ему сочетание глубокого теоретика и блестящего практика, и в этом мы все берем с него пример.

Всеми любимый Валерий Аркадьевич Конявский – доктор технических наук, заведующий кафедрой Московского физико-технического института (МФТИ), один из основоположников современной аппаратной безопасности – неизменно поддерживал нас с самого момента основания журнала добрым словом и острой шуткой. Он помогал утвердить авторитет журнала не только на российских, но и зарубежных научных площадках.

Михаил Юрьевич Сенаторов – доктор технических наук, профессор, лауреат Премии Правительства Российской Федерации в области науки, действительный член Российской Академии космонавтики им. К.Э.Ци-

олковского – человек поистине метагалактического опыта и знаний, много лет проработавший заместителем председателя ЦБ РФ и накопивший бесценный опыт. Он всегда помогал мудрым советом, ободрял и поддерживал нас.

Евгения Витальевна Шилова – доктор экономических наук, профессор кафедры экономики знания Высшей школы современных социальных наук МГУ имени М.В. Ломоносова – женщина потрясающего юмора и эрудиции. Совместно с другими нашими коллегами-экономистами она сделала возможным признание журнала Высшей аттестационной комиссией в области финансов.

Владимир Ильич Егоров – кандидат физико-математических наук, заместитель директора Национального центра квантового Интернета, молодой талантливый ученый в области квантовой физики – обеспечил нам прорыв в новые горизонты исследований и публикаций, открыл увлекательный мир квантовой криптографии.

Дмитрий Сергеевич Мачихин – эксперт по вопросам противодействия отмыванию доходов и финансированию терроризма, учета и комплаенса цифровых финансовых активов и валют, член профильного комитета при Государственной Думе РФ – весьма серьезный наш коллега и специалист в этих важных современных областях финансов. Он помогал нам стать лучше и всегда быть на острие актуальности в стремительно меняющихся реалиях цифровой экономики.

Дмитрий Игоревич Правиков – кандидат технических наук, заведующий кафедрой комплексной безопасности критически важных объектов РГУ нефти и газа имени И.М. Губкина – без преувеличения основоположник современной российской информационной безопасности как научной дисциплины, сподвижник самого Сергея Павловича Расторгуева. Талантливый ученый и мудрый администратор, Дмитрий Игоревич помогал нам своим примером и советом, и ориентируясь на него, мы каждый день терпеливо и понемногу становились лучше, как команда и как издание.

Артем Евгеньевич Терпугов – кандидат экономических наук, проректор Государственного университета управления, стоял у истоков нашего журнала. Артем Евгеньевич, человек большой доброты и открытости, неизменно помогал нам в области научного роста и соответствия высоким стандартам российской науки и только иногда говорил, что наш журнал слишком тонкий. Но мы стараемся не худеть и быть поплотнее, Артем Евгеньевич и все наши коллеги и уважаемые члены редакционного Совета!

Главный редактор и редакция журнала

Юбилейный выпуск открывает статья главного редактора нашего журнала Андрея Щербакова **«Четвертый факультет Высшей школы КГБ в зеркале истории великой страны»**, посвященная крупной и важной исторической дате – 75-летию с момента основания Высшей школы криптографов, впоследствии – Четвертого факультета Высшей школы КГБ СССР, в течение долгих лет занимавшихся подготовкой специалистов в области криптографии и защиты информации. Не будет большим преувеличением сказать, что специалисты Четвертого факультета обеспечивали информационную безопасность нашего великого государства на протяжении целой эпохи исторических значимых его свершений.

Научные разделы журнала начинаются статьей **«Теоретические основы современной аватарной алгоритмизации»** Джомарта Алиева, затрагивающей фундаментальные и при этом крайне актуальные проблемы субъектности в проектах по созданию искусственного интеллекта. В ней предложена универсальная модель и сформулирован общий конструкт аватарной алгоритмизации как эффективные методологии синтеза ИИ, обладающего измеримыми свойствами субъектности. Весьма важным для будущих фундаментальных исследований выводом является то, что коммуникационные мотивы формирования компетенций цифровой сущности, включая становление её субъектного комплекса, определяются генеральным типом её объектности. Статья будет полезна теоретикам и практикам искусственного интеллекта.

В статье **«Методика синтеза объектно-ориентированной программной модели терминала релейной защиты из его функционального описания»** Наталии Галаниной и Сергея Петрова предлагается методика, предназначенная для сокращения времени разработки программного обеспечения устройств релейной защиты и автоматизации (РЗА) в условиях постоянно меняющихся требований к их функционалу. Синтезированные программные сущности представляют структуру программного обеспечения терминала РЗА и являются основой для дальнейшей реализации его внутреннего ПО, а также цифровых двойников устройства.

Статья **«О проблеме компьютерной фальсификации личности и общения»** Павла Былевского и Владимира Новикова посвящена интересной и актуальной проблеме компьютерной фальсификации личности и общения и открывает цикл публикаций о возможностях публичных цифровых сервисов, касающихся нарушения информационной безопасности и манипулирования сознанием человека. Авторами установлен фактор, определяющий деструктивную направленность разработок и поставок публичных цифровых сервисов. Выводы содержат рекомендации мер безопасности как для использования российскими гражданами зарубежных сервисов, так и для разработки их отечественных аналогов.

Статья **«Современные подходы к разработке мобильных приложений»** Алексея Маринина затрагивает весьма актуальный, но мало дискутируемый вопрос организации процесса разработки мобильных приложений высокого качества. В работе описана целесообразность и особенности комплексного применения фреймворка Flutter и языка программирования Dart для разработки кроссплатформенных приложений. Применение предлагаемого автором метода с учетом возможностей запуска приложения в разных операционных системах может способствовать созданию и выводу на рынок приложений, максимально соответствующих потребностям пользователей.

В статье **«Основные подходы к созданию информационно-технологической среды обитания нового общества»** Артёма Урядова сформулированы основные подходы, применение которых позволит подготовить общество к решению многих актуальных и потенциальных глобальных проблем. Автором изложены недостатки антропоцентричного восприятия мира и предложены направления развития, а также обоснована целесообразность применения витацентрического подхода.

Юбилейный выпуск завершается статьей Михаила Масленникова **«Высшая школа криптографов. Взгляд изнутри»**, также приуроченной к 75-летию технического факультета Высшей школы КГБ и повествующей о значимых вехах и непростых периодах, которые пережила криптографическая служба до момента появления и последующего развития в России гражданской криптографии.

В эти осенние дни свой 50-летний юбилей отмечает Сергей Владимирович Запечников — выдающийся российский ученый и ведущий специалист в области криптографии.

Сергей Владимирович – автор более 180 научных и учебно-методических трудов. Доктор технических наук (2011), доцент (2005), профессор Института интеллектуальных кибернетических систем Национального исследовательского ядерного университета «МИФИ». Окончил Московский государственный инженерно-физический институт по специальности «Прикладная математика».

К области научных интересов Сергея Владимировича относятся криптографические протоколы, обеспечение устойчивости распределенных вычислений и безопасности доступа к базам данных и системам распределенного реестра, надежность и безопасность приложений интеллектуального анализа данных и машинного обучения.

Лауреат премии Национального форума информационной безопасности «Инфофорум» в номинации «Преподаватель года» (2009), победитель конкурсов научных исследований в области информационной безопасности «ИнфоТеКС-Академия» (2012, 2014, 2018) победитель конкурса грантов благотворительного фонда В. Потанина для преподавателей государственных вузов России (2003, 2006).

Награжден нагрудным знаком «Лучший молодой преподаватель НИЯУ МИФИ» за высокие достижения в научно-исследовательской деятельности (2015), отмечен Благодарственным письмом генерального директора ГК «Росатом» за многолетний добросовестный труд, значительные личные успехи в научно-исследовательской деятельности и большой вклад в развитие атомной отрасли (2018).

Заместитель Председателя Диссертационного совета МИФИ 2.04.

С января 2020 по декабрь 2023 участвовал в выполнении Государственного задания "Аналитические и численные методы исследования математических моделей сложных систем" Министерства науки и высшего образования Российской Федерации.

Редакционный совет и читатели журнала сердечно поздравляют Сергея Владимировича Запечникова с юбилеем и желают ему крепкого здоровья, всемерного благополучия, больших творческих успехов и новых горизонтов на непростой стези большого ученого!

СОДЕРЖАНИЕ

1. ЗНАЧИМЫЕ СОБЫТИЯ И ПАМЯТНЫЕ ДАТЫ

А. Ю. Щербаков – Четвертый факультет Высшей школы КГБ в зеркале истории великой страны 6

2. ФУНДАМЕНТАЛЬНЫЕ ПРОБЛЕМЫ ЦИФРОВЫХ ТЕХНОЛОГИЙ

Д.Ф. Алиев – Теоретические основы современной аватарной алгоритмизации
D.F. Aliev – Theoretical foundations of modern avatar algorithmization 11

3. ПРАКТИЧЕСКИЕ АСПЕКТЫ ЦИФРОВЫХ ТЕХНОЛОГИЙ

Н.А. Галанина, С.В. Петров – Методика синтеза объектно-ориентированной программной модели терминала релейной защиты из его функционального описания
N.A. Galanina, S.V. Petrov – Methodology of synthesis of an object-oriented program model of a relay protection terminal from its functional description 28

4. ФИЛОСОФСКИЕ АСПЕКТЫ ЦИФРОВЫХ ТЕХНОЛОГИЙ

П.Г. Былевский, В.Г. Новиков – О проблеме компьютерной фальсификации личности и общения
P.G. Bylevskiy, V.G. Novikov – On the problem of computer falsification of personality and communication 37

5. СОВРЕМЕННЫЕ ЦИФРОВЫЕ ТЕХНОЛОГИИ: ОБЗОРЫ, МНЕНИЯ, ДИСКУССИИ

А.К. Маринин – Современные подходы к разработке мобильных приложений
A.K. Marinin – Modern approaches to mobile application development 47

А.В. Урядов – Основные подходы к созданию информационно-технологической среды обитания нового общества
A.V. Uryadov – Basic approaches to creating an information technology environment for the new society 56

Михаил Масленников – Высшая школа криптографов. Взгляд изнутри 61

Четвертый факультет Высшей школы КГБ в зеркале истории великой страны

Андрей Юрьевич Щербаков

Доктор технических наук, профессор, академик РАЕН, выпускник Четвертого факультета Высшей школы КГБ СССР 1990-го года. В 1993 г. защитил кандидатскую диссертацию по специальности 05.13.19, в 1997 г. – докторскую диссертацию по специальности 05.13.15 на тему «Методы и модели проектирования средств обеспечения безопасности в распределенных компьютерных системах на основе создания изолированной программной среды».

Автор более 170 научных работ, 15 монографий и 20 патентов.

Награжден почетной грамотой ВОИР «За многолетнюю плодотворную изобретательскую деятельность», почетным знаком ФИПС «Во благо России», грамотой председателя ЦБ РФ «За принципиальность, объективность и профессионализм».

Этой заметкой мы открываем цикл материалов, посвященных созданию Четвертого факультета Высшей школы КГБ СССР, который в течение долгих лет занимался подготовкой специалистов в области криптографии и защиты информации. Осенью этого года мы отмечаем семидесятипятилетие этого события.

Редакционный совет приглашает выпускников, преподавателей и сотрудников этого без сомнения замечательного учебного заведения подвести итоги, высказать своё мнение, поделиться воспоминаниями.

Вступление

Когда собираешься рассказать или написать о юбилее чего-то или кого-то масштабного, даже великого, всегда явно или подсознательно возникает вопрос: а так ли это событие масштабно, как кажется рассказчику?

В данном случае тезис «больше быть, чем казаться, много делать, но мало выделяться» в полной мере имеет право на существование. Криптографическая служба — это, конечно, не Росатом с ядерным щитом, а малозаметный, но ключевой игрок, например и в частности сделавший существование этого «щита» возможным и предотвратившем утечки информации не только о нем, но и о многих других важных проектах, фактах и событиях в истории и жизни СССР.

Итак, вернемся в осень 1949 года. 29-го августа СССР испытал атомную бомбу и в октябре мир узнал об испытаниях из официального сообщения ТАСС. 8 октября в "Известиях" появилась карикатура художника Бориса Ефимова со стихотворной подписью:

Сообщило миру ТАСС
Просто, скромно, без апломба,
Что, мол, атомная бомба
Есть у вас и есть у нас!
Да-с!

Узнаете стихотворный почерк? Ну, конечно, эти строки принадлежат Сергею Михалкову.

Вспомним также автобиографичный роман Александра Солженицына «В круге первом», относящийся к тому же времени, где герои среди прочего пытались установить личность дипломата, пытавшегося сообщить Западу имя и место передачи атомных технологий.

Итак, началась гонка технологий, создание нового «атомного» мира, и криптография, служащая в первую очередь защите государственных интересов, стала невероятно востребованной. Важно заметить, что создание криптографической службы и соответствующего учебного заведения в СССР не стало ответом на шаги запад-

ных стран, а стало, как бы сейчас сказали, «проактивным» действием, опередившим даже создание Агентства национальной безопасности США.

Интересно понять мотивации учёных и инженеров того времени, взявшихся за новое дело. Самое главное — уверенность и даже вера в то, что они берутся не только за нужное, но и за осуществимое. Кстати, прочитавшему «В круге первом» не покажется, что близкий автору круг верил в создание аппарата засекречивания речи.

Что же касается «технических условий» проекта, то в первую очередь они понимали, что необходимо опираться на математику и электронику (чуть позже — на вычислительную технику), во-вторых, безоговорочно верили в государственную поддержку своих идей и мнений, а в-третьих — были уверены, что в создаваемом учебном заведении будет кому учиться. Вот эту не очень явно выраженную идею «общего интересного дела» с верой в успешный результат и культивировал Четвертый факультет, его лучшие преподаватели и выпускники.

Немного ранней истории

Практически на следующий день после заметки в «Известиях», 9 октября 1949 года, Постановлением Политбюро ЦК ВКП(б) № П71/426 был принят ряд важнейших для советской криптографической науки решений [1]:

— на базе 6-го Управления Министерства государственной безопасности (МГБ) и дешифровально-разведывательной службы Генерального штаба Советской Армии было создано Главное управление специальной службы (далее — ГУСС) непосредственно при ЦК ВКП(б) (с 13 октября 1952 года ВКП(б) как мы помним стала называться КПСС);

— должны были быть предприняты меры по привлечению учёных как для выполнения оперативных задач криптографической службы, так и в роли преподавателей для подготовки новых высококвалифицированных кадров;

— давалось поручение о создании Высшей школы криптографов (далее — ВШК) и «закрытого» отделения механико-математического факультета Московского государственного университета.

11 августа 1950 года постановлением Секретариата ЦК ВКП(б) в составе ГУСС была создана Высшая школа криптографов (далее — ВШК) и отнесена к высшим учебным заведениям 1-й категории. Положение о ВШК было утверждено 6 сентября 1950 года. В состав ВШК входили кафедры криптографии, радиоразведки, математики, социально-экономических дисциплин и иностранных языков, а также курсы по подготовке техников-криптографов. Срок обучения составлял два года на дневном отделении и три года — на вечернем. Была установлена численность слушателей ВШК – 250 человек.

Обучение в ВШК (в настоящее время «наследник» ВШК — Институт криптографии, связи и информатики Академии ФСБ России[1]) началось в начале февраля 1951-го года. Учеба, по воспоминаниям слушателей того времени, действительно была непростой: математика на университетском уровне соединилась с электро- и радиотехникой на уровне института связи. К этому добавлялись почти ежедневные занятия по английскому языку и марксистской философии. Уровень математической подготовки определялся составом педагогов: высшую алгебру и теорию чисел читал профессор *Леопольд Яковлевич Глазунев*, анализ и теорию вероятностей — ведущие молодые доценты МГУ *Николай Петрович Жидков* (1918–1993) и *Андрей Сергеевич Монин* (1921–2007).

Первыми специальными дисциплинами были «Коды» и «Основы криптографии». Основными лекторами по этим дисциплинам были полковник *Борис Алексеевич Аронский* (1898–1976) и подполковник *Михаил Спиридонович Одноробов* (1910–1997), представлявшие два поколения советских криптографов.

Еще в апреле-мае 1941-го года в советскую криптослужбу было мобилизовано около 50 молодых учёных из МГУ — математиков, физиков и выпускников Военной академии связи. Они не только смогли быстро найти в ней свое место, но и привнесли в работу новые идеи.

Инженеры и физики начали создавать и внедрять в анализ шифров вспомогательную технику, что способствовало достижению крупнейшего успеха в дешифровании, «раскрытии» ключей, которые часто менялись. Значительный вклад в развитие этих методов внесли М.С. Одноробов, а также кандидаты физико-математических наук *Георгий Иванович Пондопуло* (1910–1996) и *Михаил Иванович Соколов* (1914–1998), которые преподавали математические методы анализа шифров и дешифрования шифропереписки.

Лекции М.С. Одноробова состояли из двух частей. Первая часть была посвящена систематизированному описанию классических шифров с анализом их слабостей и подходов к их «взлому», вторая – знакомству с

[1] С 1992 года технический факультет Высшей школы был преобразован в Институт криптографии, связи и информатики (ИКСИ) Академии Федеральной службы безопасности Российской Федерации (Академия ФСБ России). Основные направления подготовки в институте – криптография, прикладная математика, информатика и вычислительная техника, электронная техника, радиотехника и связь.

опубликованной в западной прессе того времени математической теорией стойкости секретных систем Клода Шеннона. В 1951 году был издан учебник М.С. Одноробова «Введение в криптографию», состоявший из четырех частей, общим объёмом –более семисот страниц.

С целью обеспечения обучения сотрудников советских криптографических подразделений приказом начальника ГУСС от 17 декабря 1952 года в соответствии с решением ЦК КПСС от 10 декабря 1952 года было создано вечернее отделение по подготовке инженеров-криптографов с четырехлетним сроком обучения. Занятия на вечернем отделении начались 18 февраля 1953 года.

Учебный план вечернего отделения был рассмотрен на Ученом совете ГУСС и утвержден в сентябре 1952 года. В его основу был положен общий учебный план физико-математических факультетов педагогических институтов, дополняемый дисциплинами, знание которых было необходимо в практической деятельности разных оперативных подразделений Управления.

В отличие от дневного отделения, где слушателям по окончании обучения присваивалась квалификация «инженер-криптограф» и диплом на руки не выдавался, а вшивался в личное дело, выпускники вечернего отделения получали диплом единого для всех вузов образца с присвоением квалификации «инженер-вычислитель» по специальности «прикладная математика».

В 1949–1957 годах на «закрытом» отделении мехмата МГУ прошли обучение около 200 человек. Их приход в начале 1950-х годов в криптографическую службу в значительной мере способствовал процессу «математизации» советской криптографии. Наряду с разработкой новых методов криптографического анализа существенное развитие получила теоретическая криптография (синтез шифров), в которой ведущую роль играли доказательные математические методы и теории.

24 апреля 1953 года ГУСС была ликвидирована и разделена на три части: Специальная служба органов госбезопасности (8-ое Управление МВД), Специальная служба ГШ СА и Специальная служба Главного штаба ВМФ. ВШК перешла в подчинение 8-го Управления и стала называться Высшей школой 8-го Управления МВД. Однако ее штатное расписание и списки преподавательского и учебно-вспомогательного состава сохранились без изменений.

3 марта 1954 года Указом Президиума Верховного Совета СССР был создан Комитет государственной безопасности (далее — КГБ) при Совете Министров СССР в составе нескольких управлений. 8-е Управление МВД стало 8-м Главным Управлением (далее — ГУ) КГБ СССР. «Положение о КГБ при СМ СССР» было утверждено Президиумом ЦК КПСС и введено в действие Постановлением СМ СССР от 23 декабря 1958 года.

Начальником 8 ГУ стал генерал-майор *Василий Андреевич Лукшин* (1912–1967), а его заместителем — генерал-майор *Алексей Иванович Копытцев* (1912–1987).

В январе 1960 года был принят закон «О новом значительном сокращении Вооруженных сил СССР», в соответствии с которым существенно сокращались и кадры КГБ. В связи с этим ВШ 8-го ГУ КГБ, включая профилирующие кафедры, аспирантуру, вечернее отделение и курсовую систему, вошла (в сокращенном виде) в структуру Высшей школы КГБ как 4-й (технический) факультет.

Именно в это время перед факультетом была поставлена новая задача: набирать одаренных математиков из числа выпускников средних школ на пятилетнее обучение. По предложению авторитетных научных работников службы возглавить эту работу был приглашен профессор математики *Иван Яковлевич Верченко* (1907–1996).

Иван Яковлевич был весьма необычным человеком, исключительной доброты и отзывчивости, талантливым математиком и великолепным педагогом и организатором. Многие слушатели из-за характерной манеры общения и внешнего вида называли его «Дедом Морозом». Автор этой заметки еще в школьные годы лично встречался с Иваном Яковлевичем.

Первый выпуск новой волны молодых криптографов состоялся в 1966 году. Уже через несколько лет их число превысило сотню, и они стали играть существенную роль как в спецслужбах СССР (КГБ, ГРУ), ВМФ, так и в промышленности. Самые сильные из них возвращались в аспирантуру факультета, что укрепляло связь кафедры с оперативными подразделениями.

Начальниками факультета в разные периоды времени были:

1. Евгений Фомич Баженов (1960 – апрель 1963).
2. Иван Яковлевич Верченко (май 1963 – 1972).
3. Владимир Иванович Бондаренко (январь 1972 – 1988).
4. Погорелов Борис Александрович (1989 – 1991).

Кафедру №7, сосредоточившую практически все криптографические дисциплины, в разные периоды возглавляли *Пондопуло Георгий Иванович* (в период 1960–1976 гг.) и *Шанкин Генрих Петрович* (с 1977г. по 1991г.).

«Рядом со щитом и мечом...»

Выступая 23 октября 1968 г. на собрании комсомольцев центрального аппарата КГБ СССР, Ю.В. Андропов подробно остановился на требованиях, которым должен отвечать сотрудник органов безопасности [2].

«Что это значит – быть на высоте требований? ... Это значит постоянно и упорно учиться. Прежде всего тому, что требует наша профессия, а она требует все более широких и глубоких знаний. Нельзя забывать и того, что противник использует в своей шпионской и подрывной деятельности все достижения науки и техники. Чтобы в таких условиях успешно выполнять возложенные на нас задачи, чекисты должны овладевать научно-техническими знаниями, овладевать современной техникой, которую дает нам страна. Если бы сейчас решался вопрос о нашей чекистской символике, то рядом со щитом и мечом можно было бы смело добавить и символ современной электроники».

Неизвестно, что имел в виду Юрий Владимирович. Возможно, он видел в качестве этого символа схематическое изображение транзистора, но слушатели того времени считали таким символом одного из преподавателей кафедры физики и электротехники.

Помимо выпускающей Седьмой кафедры, базовые знания слушателей на факультете формировали кафедра общематематических дисциплин (знаменитая тринадцатая кафедра — источник проблем для многих слушателей), кафедра физики и электротехники (четырнадцатая кафедра), восьмая кафедра (радиотехники) и десятая — вычислительной техники.

Находившиеся немного в тени своих «профильных» коллег, сотрудники этих кафедр приложили огромные усилия по формированию у слушателей эрудиции, высокой квалификации и ответственного отношения к делу. И важно отметить, что во многом их усилия помогли слушателям сориентироваться в сложной атмосфере 90-х и заново найти свое призвание в разных областях – от преподавательской до банковской.

Семидесятые и восьмидесятые годы

Четвертый факультет ВШ КГБ приобрел за годы своего существования и развития достаточный опыт и заслужил заметный авторитет в КГБ, армии и промышленности. В 1970-х годах Коллегия КГБ дважды рассматривала вопрос о превращении его в самостоятельное высшее военное учебное заведение. После первого из них И. Я. Верченко «по горячим следам» разработал предложения, согласно которым факультет должен был превратиться в учебное заведение со статусом Военной академии.

Однако это предложение не нашло поддержки ни у руководства ВШ, ни в Управлении кадров КГБ, поскольку ставило факультет в более привилегированное положение по сравнению с «материнской» ВШ. Иван Яковлевич был этим весьма недоволен, вступил в конфликт с руководством Высшей школы и отказался от продолжения руководства факультетом, хотя и продолжал читать на нем свой лекционный курс.

Начальником факультета был назначен генерал-майор *Владимир Иванович Бондаренко* (1918–2004) — заместитель начальника ГУ КГБ, который прошел Отечественную войну и командовал ранее несколькими подразделениями ГУСС.

К сожалению, Владимир Иванович был больше строевым офицером и его стиль руководства и педагогической работы подходил скорее для военного училища.

Для быстрейшего решения возникших проблем В.И. Бондаренко стал искать себе надежного помощника, и в апреле 1972 года заместителем начальника факультета был назначен Л.А. Кузьмин вместо Е.Ф. Баженова (1914–1978), который ушел на пенсию. Так начался новый этап развития Технического факультета ВШ КГБ и его кафедры криптографии.

Интересно, что в 1986 году издательство «Радио и связь» в плане изданий на 1987 год опубликовало анонс книги Д. Конхейма «Основы криптографии». В ней содержались базовые понятия и методы криптографии, приводилось описание американского стандарта блочного шифрования «DES», самые тривиальные подходы к его криптоанализу.

Реакция руководства 8-го ГУ КГБ была достаточно предсказуемой и книга в печать не вышла. Весь тираж был снабжен грифом «Для служебного пользования» и направлен в закрытые спецбиблиотеки управлений КГБ. Однако именно с этого момента началось движение в сторону «гражданской криптографии», без которой сейчас невозможно представить работу ни одного финансового сервиса, и даже само понятие «криптовалюта» отсылает к криптографическим механизмам.

Вместо заключения

Мы попробовали несколькими штрихами описать историю факультета и заслуги множества увлеченных и замечательных людей, стоявших у его истоков. Конечно, наша картина кому-то покажется неполной и даже искаженной — что же — никогда не поздно высказать мнение, которое мы с удовольствием опубликуем.

Малый объем не позволяет также упомянуть всех преподавателей, которые выполняли свой повседневный нелегкий труд и формировали замечательную учебную атмосферу факультета. С глубоким почтением и благодарностью вспомним Михаила Михайловича Глухова, известного математика-криптографа, начальника 13-й кафедры, доцента и руководителя 14-й кафедры физики и электротехники Александра Ивановича Кучумова, замечательно преподававшего львиную долю радиотехнических дисциплин, и Владимира Глебовича Никонова, выдающегося советского дискретного математика, преподавателя-художника (знаменитая седьмая кафедра), благодаря которому многие по-настоящему поняли идею многомерных пространств.

В наше непростое время усилиями упомянутых в заметке гигантов, на плечах которых стоим мы, нынешние криптографы, современная российская криптография держится на весьма достойном уровне и может отвечать весьма высоким современным требованиям. Достаточно привести два основополагающих принципа — использование в критических системах и приложениях только отечественных криптографических алгоритмов и необходимость сертификации средств криптографической защиты информации, использование сертифицированных криптографических средств.

Однако мы традиционно отстаем в элементной базе, производительности вычислительных комплексов и возможности разработки и производства собственных масштабных программных продуктов, в первую очередь операционных систем. Несмотря на то, что эти работы ведутся, их результатами пока становятся, к сожалению, неудобные в использовании кустарные поделки.

Причины современного сложного и даже кризисного состояния весьма глубоки и многообразны и лежат в основном вне способностей и возможностей российских учёных, а в первую очередь – в области идеологии и мотиваций. Как метко написал современный поэт Всеволод Емелин:

«...Вместо звезд и планет
Горит реклама «ИКЕИ».
Грустно сижу я на их
Табуретке фанерной.
Нынче не время утопий
Об покорении Вселенной.
Я все понимаю: Сталин,
Репрессии, пятилетки…
Но зачем мы Космос сменяли
На фанерные табуретки?

ЛИТЕРАТУРА

1. Гребенников В.В. Криптология и секретная связь. Сделано в СССР. - Изд-во «Алгоритм», 2017. ISBN: 978-5-906979-79-7. 680 с.
2. Юбилей Андропова. URL: http://www.fsb.ru/fsb/history/yubiley.htm%21_print%3Dtrue.html

УДК: 004.8, 51

Теоретические основы современной аватарной алгоритмизации

D.F. Aliev

Theoretical Foundations of Modern Avatar Algorithmization

Abstract. *The article invites theorists and practitioners in artificial intelligence to discuss the problem of subjectivity in modern and promising AI projects. A universal BFA model is proposed and a general construct of avatar algorithmization is formulated as an effective methodology for synthesizing AI with measurable properties of subjectivity. The reasons for the gap between the objectivity of digital entities and their subjectivity are described, as well as the risks of connecting the subjectivity of an avatar entity with its objectivity. It is shown that in accordance with the subject model of systematization, the communication motives for the formation of the competencies of a digital entity, including the formation of its subject complex, are determined by the general type of its objectivity.*

Keywords: *artificial intelligence, subjectivity, subject-object model, avatar, BFA model, subject model of systematization, methodology of artificial intelligence, cognition, semantics, vital logic.*

Д.Ф. Алиев
Доктор философии в области бизнес-права (PhD), доктор делового администрирования в области финансов (DBA), кандидат экономических наук, первый проректор Федерального государственного бюджетного образовательного учреждения высшего образования «Российский государственный социальный университет».
E-mail: kharchenkoDD@rgsu.net

Аннотация. *Статья приглашает теоретиков и практиков искусственного интеллекта к обсуждению проблемы субъектности в современных и перспективных проектах ИИ. Предложена универсальная БФА-модель и сформулирован общий конструкт аватарной алгоритмизации как эффективные методологии синтеза ИИ, обладающего измеримыми свойствами субъектности. Описаны причины разрыва объектности цифровых сущностей с их субъектностью, а также риски связи субъектности аватарной сущности с её объектностью. Показано, что в соответствии с субъектной моделью систематизации коммуникационные мотивы формирования компетенций цифровой сущности, включая становление её субъектного комплекса, определяются генеральным типом её объектности.*

Ключевые слова: *искусственный интеллект, субъектность, субъектно-объектная модель, аватар, БФА-модель, субъектная модель систематизации, методология искусственного интеллекта, когнитивность, семантика, витальная логика.*

ВВЕДЕНИЕ. ПОСТАНОВКА ПРОБЛЕМЫ

Перечень проблем и вопросов, обсуждаемых и осознаваемых сегодня сообществом разработчиков систем искусственного интеллекта (ИИ), концентрируется главным образом, вокруг объектности цифровых сущностей. Более того, их субъектность, как и неотъемлемо связанная с этим свойством потенциальная социальность создаваемых или проектируемых ими акторов (активных сущностей) цифровой бихевиористики[1], и вовсе не находится в фокусе их внимания. Отдельные попытки придания субъектности – развитие состязательности различных ИИ-платформ или конкурентная оптимизация обработки данных с токен-оцениванием, либо же их интеграция не только по данным, но и по алгоритмам, – являются в большинстве случаев техническими решениями, которые лежат всё в той же объектной плоскости.

У такого состояния дел имеется целый ряд причин, отчасти обосновывающих и в какой-то мере – лишь комментирующих сложившийся статус-кво. Ранее в [1] некоторые из них уже затрагивались, но в контексте данной работы их сходство состоит в том, что они основываются не на гипотезах, а на предположениях.

В связи с этим их множество представляет собой скорее срез не задачного, а вероятностного пространства, осознание которого, ввиду низкого уровня зрелости, выглядит больше интеллектуальной гимнастикой, нежели чем-то практическим и ориентированным на результат. Поэтому не погружаясь в подробности, приведём здесь четыре группы причин разрыва объектности цифровых сущностей с их субъектностью, выявленных при разработ-

[1] Бихевиоризм — это одно из основных направлений в психологии, которое фокусируется на изучении поведения индивида и способов влияния на него. Ключевым для бихевиоризма является предположение о том, что поступки и действия индивида складываются из рефлексов, которые он получает при рождении и приобретает в течение жизни, а также из его откликов на воздействие внешних факторов.

ке прикладных приложений социальной физики в рамках исследовательских проектов:

- функционально узкая (практически только вычислительная) постановка большинства ИИ-задач, что во многом определяет невнимание к субъектности, а иногда – даже и отрицание этого свойства, не только как характеристичного для сущности, но и как описательного. Подавляющее большинство целей в современных цифровых проектах (в основном – прикладных) априори преимущественно объектны, что совершенно нормально для доминантной сегодня субкультуры инвестируемого потребительства. Другое дело – проблематика ответственного научного поиска в ожидании баланса и гармонии.

- несколько идеалистичное представление о накопленных знаниях, связанных с прообразами тварного міра, модельными для разработок цифровых сущностей.

- кажущиеся вполне обоснованными смысловые лакуны наполнения и интерпретации определений цифровой субъектности; источник вынужденных, в известном смысле, упрощений «зрелостного» характера. Хотя они иногда и фундаментальны: например, пока у нас отсутствует (не восстановлена) тринарная вычислительная логика [2], эволюция от искусственного интеллекта через гибридный разум к синтетическому сознанию практически исключена. Во всяком случае – маловероятна и точно эмулятивна [3], поскольку для человека гармоничны только сущности «да/нет/не_знаю».

- реальные технологические пробелы работоспособности даже тех редких концептов, в которых объектно-субъектная (ОС) связанность предполагается. Но это не только кейсы с крайне высокой ресурсоёмкостью детерминированных потоковых расчётов: даже с надлежащей корректировкой семантики цифровых сущностей открывающиеся тут возможности используются не потенциально, а в унаследованных представлениях об их правильности. Наглядный пример — наши попытки преобразовать встроенные потенциалы квантовых вычислителей в прокрустово ложе бинарной логики.

Далее мы не будем рассматривать проявления первой и второй групп: говорить о первых очевидно не создаёт перспективу, а вторые имеют не методологические, а мировоззренческие корни. В описании причин третьей и четвёртой групп, мы, в целях обобщения постановки, отложим в сторону все коммерческие, отраслевые и технологические компоненты, сохранив в зоне внимания лишь массив, имеющий в своём основании когнитивно-семантические источники.

МЕТОД КОПИРОВАНИЯ КАЧЕСТВ. МЫСЛЕННЫЙ ЭКСПЕРИМЕНТ

Проведем следующий мысленный эксперимент. Положим на стол калькулятор и электробритву и организуем между ними некую коммуникацию таким образом, чтобы они функционально подтянулись: первый стал бы лучше считать, а вторая – качественнее брить.

Очевидно, что такой эксперимент только выглядит наукообразно. Но так ли это будет в дальнейшем? На достигнутых уже сегодня технологиях можно сконструировать такую «интеграцию» калькулятора и электробритвы; по данным – уверенно, по процедурам – вероятно, по объектам – не исключено. Достижение более высокого перфоманса этих устройств, обусловленное взаимным коннектом, конечно, останется сомнительным, но некоторые новые качества, такие как «зависимость интенсивности расчётных актов от средней продолжительности ежедневного бритья» или «зависимость средне-типичного шейпа бороды от уровня сложности калькуляций», мы с помощью вовлекаемых в процедуры ИИ-ассистентов собрать вполне способны.

Накопив несколько сотен таких «коннекторов» и собрав несколько десятков тысяч соответствующих датасетов, мы можем получить подтверждение какой-то ранее неизвестной нам факторной корреляции (например, «функция распределения совместной нагрузки при смежном использования бытовых калькуляторов и электробритв»). При этом может оказаться, что какое-то из найденных в таком эксперименте качеств будет даже иметь практическое значение, например, «зависимость вовлечения в конструкторские активности от носительства и типа усов». Однако 99,9% всех обнаруженных «закономерностей» будут пригодны только для сайта https://tylervigen.com или ему подобных.

Данный мысленный эксперимент был проведен не для того, чтобы поставить под сомнение современные практики создания цифровых сущностей, результатом которых являются множество платформ/комплексов машинного обучения. Главным смыслом эксперимента было показать ограниченность метода «черного ящика» для проявления качеств. В первую очередь – в поисках смежной объектности. С объектностью в однообъёмных качествах всё не намного проще, в особенности, если создаваемая сущность имеет свой прообраз (образец), который мы воссоздаём (копируем) при соз-

дании цифровых сущностей. Т.е. именно так, как в большинстве случаев при создании систем, которые мы и называем сегодня ИИ-системами.

Важно определить, в чем заключается проблема методики копирования качеств (пусть и с улучшениями). Для этого, например, можно ответить на вопросы, когда человек успешно (управляемо, в нужную сторону) полетел и когда, отказавшись от биомиметики[2] и переместившись на платформу бионики, перестал создавать копии (например, махолёты) и открыл для себя главное (подъёмную силу крыла). Это был не только технологический, но и семантический прорыв – человек сумел выделить в природном первообразе принципиальное, открыв не осознаваемое им ранее качество.

Теперь представим себе: комиссия из стрекозы, журавля и бабочки расставляет оценки смыслам практикам полета, вынося вердикты наподобие «Жуковский немного отвлёкся, Райты поняли главное, а Сикорский – просто молодец». Очевидна бессмысленность такой «ситуации». Однако мы до сих пор эксклюзивно привержены тесту Тьюринга (строго говоря – Айера[3]) и его клонам в оценках состоятельности создаваемых ИИ-сущностей социально-коммуникационного класса. При этом нет никаких аргументов против использования контроля, основанного на принципах биомиметики, для соотнесения их фактической и плановой функциональности: летит (считает, бреет) или нет. Но это касается только объектности, причём без её обратной связи с субъектностью.

Если мы говорим о субъектности, особенно в ИИ-системах высокого социального класса, то здесь намного более сложным представляется не только вопрос контроля своего рода «сходимости», но и множество собственно созидательных аспектов. Например, осознавали ли разработчики глобальных LLM-приложений, что обучающие их корпуса в весьма скором времени после запуска в массовую эксплуатацию соответствующих генеративных моделей будут поражены, в применении к языковым моделям, фактурой, созданной внутри процессора.

Анализ программных материалов команды OpenAI стартового периода (до смены политики информационной открытости на эффектах GPT-2) не выявил признаков такого предвидения. Также нам не удалось обнаружить их в постановочных материалах ни у Google, ни у DeepMind, ни у Microsoft. Что-то схожее с обеспокоенностью от самоконтаминации[4] встречается в заделах xAI. Однако данный проект, включая Grok, пока ещё слишком молод, чтобы оценивать его визионарность.

Это один из самых заметных примеров недооцененных рисков связи субъектности созданной цифровой сущности с её объектностью. И если здесь ошибка скорее косвенная, то в исследованиях от Sakana AI явно видна прямая ошибка влияния субъектности на объектность.

В системе компании Sakana AI объектно предполагалась некоторая генеративная автономность более высокого класса (попытка создания ИИ-платформы для научной деятельности). В этом кейсе практически реализовались риски субъектности. В отличие от изменения сущностью её скрипта при переходе в цикл перезапуска, когда ещё можно говорить об ошибке баг-типа, другой пример объектной корректировки от субъектности (отказ от задачи оптимизации перфоманса в пользу удлинения норм времени, отведённого на разрешение проблем) сложно объяснить чем-то, кроме ошибки в постановке при алгоритмизации образа учёного (в данном случае).

При этом сам по себе вызов, брошенный токийскими коллегами, превосходен, а весь их подход, предполагающий имитацию цифровой аутопоэзности организацией наследования моделей, как раз и выглядит как вполне уместная попытка перехода от биомиметики к бионике.

Цена ошибки и без использования технологий искусственного интеллекта не равна нулю. Мы до сих пор не располагаем достоверной информацией для того, чтобы определиться: правда ли, что американский капитан Уильям Бассет в 1962-м или советский подполковник Станислав Петров в 1983-м

[2]Биомиметика — это повторение свойств природного объекта в искусственном материале. Биомиметические материалы воспроизводят структурные особенности природных тканей или объектов. Применяется, например, в медицине для замены повреждённых тканей организма человека: хрящей, суставов, костей, в создании различных адаптируемых конструкций, например, бронежилетов. Изучение структурных особенностей природного материала и попытка воспроизвести этот объект на существующих материалах — два основных направления биомиметики.

[3]В 1936 году философ Альфред Айер рассмотрел обычный для философии вопрос касательно других разумов: как узнать, что другие люди имеют тот же сознательный опыт, что и мы? В своей книге «Язык, истина и логика» Айер предложил алгоритм распознавания осознающего человека и неосознающей машины: «Единственным основанием, на котором я могу утверждать, что объект, который кажется разумным, на самом деле не разумное существо, а просто глупая машина, является то, что он не может пройти один из эмпирических тестов, согласно которым определяется наличие или отсутствие сознания». Это высказывание очень похоже на тест Тьюринга, однако точно неизвестно, знал ли Тьюринг популярную философскую классику Айера.

[4]Контаминация (от лат. contaminatio — «смешение») в языкознании — возникновение нового выражения или формы путём объединения элементов двух выражений или форм, чем-нибудь сходных. Контаминацией называют также соединение имён и слов (точнее — корней), например: «Ф. Толстоевский» (Толстой и Достоевский), «трагикомический» (из «трагический» и «комический»), «В Академии поэзии — в озерзамке беломраморном» (Игорь Северянин).

году спасли человечество от глобального уничтожения в самых известных случаях объектно-субъектного влияния оператора на ядерном театре военных действий. Мы также не обладаем достоверной информацией, чтобы промоделировать те обстоятельства для оценки реактивности современных боевых стратегических ИИ-ассистентов (хотя и полагаем, что есть исследователи, которые это реализовали).

Для целей данной работы нам важна следующая из истории лемма фундаментальности объект-субъектной связи и её унаследованности из аналогового прошлого. Если мы способны (готовы) разрешать её при переходе в цифровое будущее, какие из прежних практик когнитивного восприятия и семантического оценивания во взаимодействиях «человек-человек» мы можем (или должны) применить для созидания взаимодействий типа «человек-машина» (в указанном выше примере – «машина-машинного» принятия решений). И наконец, как это возможно практически реализовать.

ЛЕММА ФУНДАМЕНТАЛЬНОСТИ ОБЪЕКТ-СУБЪЕКТНОЙ СВЯЗИ

Глобальная технологизация нашей социосферы расширила контингент операторов подобных дилемм, участив случаи их дихотомизации[5] и снизив уровень требований к пользовательской квалификации.

Не все современные кейсы несут в себе прямые риски уровня времен Карибского кризиса или политики Рейгана, однако число серьёзных рисков за прошедшие 60 лет увеличилось. Например, сегодня невозможно гарантировать стабильность ситуаций с разработками биологических агентов или надёжность кодов с отсутствием бэкдоров в программах управления критической инфраструктурой.

В большинстве проектов, как носителей системных рисков, акценты безопасности преимущественно объектны даже в тех случаях, когда их зрелость доходит только до ИИ-ассистанса, включая потенциально подобные японскому цифровому учёному. Несмотря на это, по замыслу попытка эволюционной алгоритмизации LLM-обучения со «слиянием моделей» очень похожа на один из перспективных вариантов когнитивно-семантической экстракции «человек-человеческой» экспертизы комбинирования объектности ролей сущностей с их субъектностью, но с двумя областями, которые на сегодня выглядят открытыми.

Первая область – стратный охват эволюционирующего сообщества. Подход Sakana AI определяет его в единственном генеалогическом древе от стартовой модели-родоначальника, протяженностью сотни поколений. На человеческой шкале времени этот интервал сравним с периодом от сотворения міра до наших дней. Проблема заключается в том, что наследование происходит по одной вертикали. При этом даже если организовать петлевой (итеративный) субалгоритм и/или межпоколенческое «слияние», издержки родовой ограниченности не позволят получать оптимально достижимые результаты. Это подобно ограничениям в доплеменном развитии, хорошо известным антропологам, когда динамика фенотипа возможна для сущности, но не обуславливается мутациями её генотипа.

Вторая область связана с механизмами передачи качеств от предка к потомку. Насколько это понятно из раскрытых японскими коллегами деталей их разработки, все они имеют не субъектный, а сугубо объектный характер. Более того, они разнообразны, но связаны лишь с различными перфомансами сущностей (моделей). Механизмы факторны, но не аргументны. Учитывая измерители качеств у моделей внутри одного поколения, алгоритм Sakana не корректирует в связи с этим базу качеств, присваивая новым их значениям ранг опорного на следующем такте эволюции.

Так действительно можно вывести самую рослую (сильную, быструю, умную) сущность в роду, решив тем самым задачу (задачи) объектной эволюции. Но в субъектном плане это сводит эволюцию к евгенике: коммуникационные потенциалы в «сообществе рослых» надо полагать весьма невысокими. При узости монородового охвата в результате появляется объектно-ориентированная «чемпионская» сущность без субъектности. Условия витальности не обеспечены, поскольку совокупность таких сущностей стагнативна.

Этому выводу легко можно возразить тем, что цель проекта EvoLLM не в разработке совокупности ИИ-сущностей, тем более – их сообщества. Однако в результате проекта должен быть создан ИИ-учёный, а учёный по определению субъектен в своей ролевой модели. Представим себе, что обучение капитана Бассета происходило бы по-японски (тем более, дело было на Окинаве). Наиболее ожидаемым максимином для офицера американских ВВС, по алгоритмам Sakana AI, на должности командира пуска была бы дисциплина, а не тактика, знание математики или умение пилотировать. И если бы

[5]Дихотомия — это раздвоенность, последовательное деление на две части, более связанных внутри, чем между собой. Это способ логического деления класса на подклассы, который состоит в том, что делимое понятие полностью делится на два взаимоисключающих понятия. Дихотомическое деление используется в математике, философии, логике и лингвистике для образования подразделов одного понятия или термина и служит для классификации элементов.

на месте Уильяма Бассета был сакана-чемпион по дисциплине, никаких шансов у Станислава Петрова проявить свою субъектность уже не было бы.

Вне зависимости от того, состязательна была природа субъектности для капитана Бассета или коллаборативна, мір спасла именно она. Но неважно это лишь тогда, когда субъектность у сущности есть, а не тогда, когда мы задаёмся вопросом о том, как её создать. Считается, что мы знаем, как привить её ребёнку – воспитанием (которое отличает образование от обучения). Тогда «бионика» разработчиков ИИ ставит перед ними задачу-максимум – проявить субъектность в машинах. И наша гипотеза в том, что воспитание есть обучение на разницах.

Мы рассмотрим этот тезис чуть ниже, в предположении, что на текущем уровне технологической зрелости решить этот вопрос очень сложно (из-за вычислительной бинарности), но возможно. Здесь нам очень важно не потерять «колористику» самой природы субъектности; вспомним слова Оруэлла «все животные равны, но некоторые из них равнее остальных». Британский писатель показал не самое приятное социальное полотно, но с исключительно верным подходом как к области определений, так и к самой алгоритмике.

Не вовлекаясь в сражение за триединый мозг между биологами и психологами (снова биомиметика vs бионика), оттолкнёмся от возможно единственного консенсуса между ними в этой части знания о человеке (в тезаурусе данной работы) – субъектность есть функция объектности. Но какова эта функция, определяет природа объектности.

Классическая тринарность витальной логики («да/нет/не_знаю») приобретает в контексте эволюции три смысла «состязательность/коллаборация/индифферентность». Причём последнее состояние гораздо богаче просто нейтральности: именно там мы обнаруживаем толерантность, более выраженную терпимость, доминирующую в большинстве сложных случаев релятивность и т.д.

Общим для всех кейсов, субъектность которых опирается на такую природу объектности, будет фактическая диссимиляция (а порою даже атрофия) самого свойства субъектности в описываемых (моделируемых, создаваемых) сущностях. Упрощая, можно сказать, что субъектность всяких сущностей «не_знаю» всегда имеет существенный понижающий коэффициент, какой бы формулой мы ни пытались описать её как функцию объектности. Поэтому ожидаемо, что большинство тех объектно-акцентированных ИИ-платформ, которые создают современные разработчики, субъектность просто игнорируют.

Если принять сказанное о субъектности, то рассуждения о её практической имплементации (воспитание ИИ-сущностей) необходимо структурировать с опорой на технолого-платформенные потенциалы и объектностное обучение. Понятно, что сама архитектура синтетического создания (как предельной цели ИИ-конструирования) не будет ни копией, ни даже подобием человеческого. Хотя тому есть множество причин, и главная из них — в фундаментальной неполноте нашего знания о самом прообразе.

Для того, чтобы перейти из точки А в точку Б, можно не знать координаты Б. Такая развитийная динамика описывается формулой «движение в сторону» (с разработанными тактиками сверки и уточнения направления). При этом незнание исходного пункта маршрута А губит любую осмысленность маршрута (в нашем случае – созидания), сохраняя незначительные перспективы успеха только для практики блуждания. Точки А на биомиметическом пути уподобления цифрового сознания человеческому мы не знаем (с нужной степенью достоверности), но отказаться от движения уже не можем.

СУБЪЕКТНАЯ МОДЕЛЬ

При незнании координат стартовой позиции исследований в области искусственного интеллекта можно оказаться в бесконечном блуждании. В то же время для использования общих принципов (солнце встаёт на востоке) и правил (поиск по спирали) блуждания нужно не только знать эти принципы и правила, но и помнить о цене ошибки для каждого из них.

Если связь объектности сущностей с их субъектностью относить к группе принципов ИИ-созидания, то зависимость природы субъектности от типа объектности можно отнести к эмпирическим правилам. Проверка гипотезы о принципиальности такой зависимости видится вполне посильной, но ресурсозатратной научной задачей. И не отрицая возможную академическую целесообразность последующих изысканий на гносеологическом поле классификации факторов, мы считаем более уместной здесь не практику когнитивного стемминга[6], а подход семантической лемматизации[7].

[6] Стемминг (англ. stemming) или морфологический поиск — процесс поиска основы слова с учётом морфологии исходного слова. Стемминг подразумевает морфологический разбор слова с нахождением общей для всех его грамматических форм основы без учёта суффиксов и окончаний.

[7] Лемматизация и стемминг— это методы обработки естественного языка (NLP), которые используются для приведения слов к их базовой или корневой форме. Лемматизация учитывает контекст и преобразует слова в их базовую форму.

Однако поскольку и методология в морфологии субъектности пока не сложилась (хотя и разрабатывается отдельными социологическими школами), и «норма» в применении к субъектности – не самая очевидная её категория, проиллюстрируем предлагаемое конкретикой этапа разметки одного из проектов создания цифровой экосистемы ИИ-сущностей.

В развитие подхода по компетенциям социальности [4] удачной оказалась ***субъектная БФА-модель систематизации*** («боксёр», «футболист», «атлет»), в соответствии с которой коммуникационные мотивы формирования компетенций субъекта (сущности), включая становление его субъектного комплекса, определяются генеральным типом его объектности.

Данная модель по сути соотносима с классической тринарностью в семантической группировке «состязательность/коллаборация/индифферентность»: лидерская объектность боксёра есть его прямая/непосредственная конкурентность в стремлении к поражению соперника; драйвер объектности футболиста – многоплановая коллективная победа его команды; объектность бегуна обусловлена по сути его сражением с обезличенными (и в этом смысле – объективизированными) килограммами, метрами и секундами. Таким образом закрепляется субъектность сущностей на состязательности для боксёров, коллаборации (командности) – для футболиста, и индифферентности (индивидуализме) – для атлета.

В практике реальных социумов из сказанного, конечно, не следуют выводы об исключении из субъектных панелей, например, солидарности для боксёра или элемента эгоизма – для футболиста. Причина – высокая (нарастающая) общественная зрелость как индивидов, так и различных социальных (объектно-субъектно сформированных) групп.

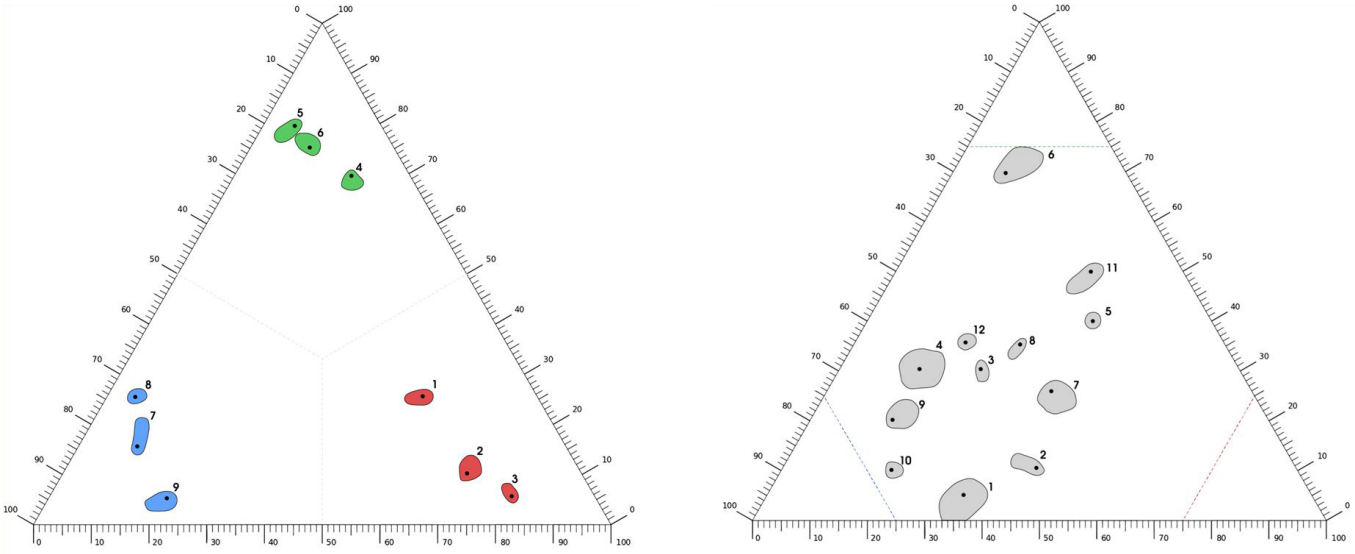


Рис.1. Примеры треугольных диаграмм, иллюстрирующих БФА-модели

Легенда левой диаграммы на рис. 1 состоит из перечня выдающихся фигур спортивного міра, а правой – знаковых персонажей цивилизационного развития последнего века. Первый список (1- Александр Карелин, 2- Конор Макгрегор, 3- Майк Тайсон; 4- Зинедин Зидан, 5- Андрес Иньеста, 6- Фёдор Черенков; 7- Усэйн Болт, 8- Юрий Власов, 9- Марк Спитц) составляют три тройки примеров мірового уровня, последовательно представляющие боксёрский, футбольный и атлетический профили, составленные на оценках общедоступной информации поведенческого характера (включая бихевиористику за пределом спортивных площадок).

Второй список – без организации (1- Константин Васильев, 2- Андрей Громыко, 3- Майкл Джексон, 4- Анатолий Кони, 5- Доктор Лиза, 6- Лю Цысинь, 7- Имельда Маркос, 8- Илон Маск, 9- Лайза Минелли, 10- Стивен Хокинг, 11- Коко Шанель, 12- Ли Якокка) и представлен в алфавитном порядке.

БФА-модель в настоящее время разрабатывается и будет опубликована по завершении разработки. На текущем этапе её применимость верифицируется рядом исследований, традиционных в естественнонаучных практиках. Весьма удовлетворительная корреляция компетентностной подмодели выявлена факторными методами в кардиологическом (управляемая тахикардия), и кластерными – в биохимическом (аминокислоты в плазме) пространствах, но прямое её применение для ИИ-девелопмента сегодня представляется сомнительным.

Несмотря на то, что определённые подсказки в треках развитийного характера могут быть весьма

эффективны, намного важнее, когда в фокус БФА-логики помещаются какие-либо ИИ-сущности. Важный эффект этому созидательному эксперименту может придать факт, что БФА-модель в качестве леммативатора является алгоритмом сусденческим. При этом перенос в моделируемые сущности наших оценок как разработчика только для их объектности в амбициозных эволюционных ожиданиях создаёт разрыв (ограничение) целостности цифровых субъектов для гибридно-социального будущего.

Всегда ли это требуется и позитивный ли смысл это имеет – вопрос субъективной оценки. С одной стороны – смысл позитивный, поскольку такая (в известном смысле обманчивая) ограниченность систем лишает их конкурентности и ассоциативности, оставляя за ними только сервисно-ролевой функционал «битвы с секундомером» и при этом мы уверены в том, что секундомер находится в руках у нас.

С другой стороны, именно такая узость замыслов и создаёт высокие риски. Отсутствие обеспечения двунаправленной коммуникации в числе задач ИИ-исследователей мешает проявлению субъектного подхода в созидании «машин». Кроме того, «машина», не обученная коммуницировать с другой «машиной» содержательно (и это не является для неё функциональной нормой), не будет пригодна к субстантивной субъектной коммуникации и с создавшим её человеком. Следует отметить, что полный отказ от субъектности ИИ-сущности за счёт концентрации на её объектности (который мы можем наблюдать сегодня) создаёт превенцию от самой проблематики социализации машин в грядущем обществе. При этом такое «воспитание» неизбежно, и пример «ИИ-учёного» от коллектива Sakana AI это наглядно показал.

ОБОСТРЕНИЕ КОММУНИКАТИВНОЙ ПРОБЛЕМЫ «ЧЕЛОВЕК-МАШИНА»

С указанными выше рисками связано неизбежное возникновение (и обострение) субъектно-коммуникативной проблемы «человек-машина». Мы уже делегировали машинам принятие решений («Алиса, включи спокойную музыку»), замкнув круг нормальной коммуникации в своём обыденном событийном потоке с включением в него машины как младшего партнёра. Человеко-машинные коммуникации стали реальностью, значит, и субъектность машин может стать практически достижимой.

Игнорирование субъектности цифровой сущности, возможно, не приведёт к появлению машинных обществ, однако при наступлении социального стазиса он непременно будет заполнен теми, кто увидит для себя возможности в этом состоянии. Здесь под стазисом понимается не только уровень экосистем «человек-машина», в котором явно виден коммуникационный разрыв или такие состояния непроявленного дефицита двунаправленной коммуникации, но и ограниченность в восприятии возможностей. Тем более такая сумма потенциалов (а это современное состояние индустрии цифровых сущностей) неконтролируема и конпревентивна.

Чем глубже и интенсивнее будет такой стазис, тем вероятнее локомотивность габитус-мотивов в устранении разрыва. Следовательно, каким бы ни оказался наиболее успешный трек цифрового созидания и какая бы техническая среда ни создала новые возможности, «полноценные» цифровые сущности будут созданы, и это вопрос времени.

Полноценными здесь надо полагать сущности, способные эмулировать множество перспективных когнитивно-семантических механизмов работы с данными (каналами, событиями, трендами и т.д.) и качественно пригодные для субъектного исполнения ролей участников социума (не обязательно исключительно человеческого).

Допуская неизбежность цифровой «победы», мы обязаны задать себе вопрос о механизме «новой» социальности. Данный вопрос носит глобальный характер и его изучение требует очень высоких затрат человеческих и материальных ресурсов. Однако сегодня, как можно наблюдать, намного проще и перспективнее решать задачи организации в цифровом контуре суррогатных органов (зрения, слуха, осязания, вкуса, обоняния), не задумываясь о том, что эта совокупность чувств не позволит цифровым сущностям познавать окружающий мир, адекватно реагируя на раздражители.

КОНСТРУКТ АВАТАРНОЙ АЛГОРИТМИКИ

Современное общество не готово к фундаментальному вызову гибридной социальности. На текущем этапе возможности ограничены алгоритмами обучения и воспитания сущностей, проявляющих как объектные, так и субъектные свойства. Иначе говоря, мы стремимся создать цифровую сущность (т.е. аватара), пригодную для гибридной социализации в близком будущем, но не для активности в отношении самого будущего.

Полагая, что сказанного выше достаточно для понимания необходимости (даже и неизбежности) разработки аватарной алгоритмики, без риска допустить грубую ошибку мы можем констатировать,

что главной задачей любого прикладного ИИ-разработчика, предполагающего полноценный жизненный цикл для своего творения, должна стать такая структура объектности его «машины», которая впоследствии обеспечит её субъектность. Помимо множества предметно-технических задач (следующих из контекста и не являющихся предметом данной работы), основная задача вполне очевидно сводится к проблеме «как избежать объект-субъектного конфликта».

Чтобы решить эту задачу, нужно не только обучать цифровые сущности, создаваемые как доступными, так и предполагаемыми способами, но и воспитывать их и по меньшей мере организовывать обе их алгоритмики (стратегическую и операционную) таким образом, чтобы, помимо трека функционального наполнения и развития, обеспечивались ролевые потенциалы социального созревания «машин», как когнитивные, так и семантические. Именно такое решение, представленное на рис. 2, мы назовём ***конструктом аватарной алгоритмики (КАА)*** синтетического сознания (цифровой сущности):

1- предметное пространство цифровой сущности;
2- задачное пространство цифровой сущности;
3- замысел проекта по созданию сущности;
4- рамки проекта;
5 - обусловленная ①, ②, ③ и ④ объектная область элементов сущности;
6 - её субъектная область, сформированная акторским подходом;
7- итоговая объектно-субъектная область компонентов;
8- собственно цифровая сущность;
9- аппаратное решение;
10- динамическая модель;
11- когнитивный блок;
12- семантический узел.

Для того чтобы сделать подход к практическому ответу на вопрос «как организовать этот ландшафт», обратимся к фундаментальной (обязательной) процедуре для любых систем машинного обучения – разметке данных. Этот алгоритмический функционал не только обязателен, но также неизбежен и необходим (и не только когда мы говорим о цифровых сущностях, но и в міре людей). Обучающие платформы, заявляемые разработчиками как способные работать на датасетах без разметки, в действительности без неё невозможны.

МАШИННОЕ ОБУЧЕНИЕ И СУБЪЕКТНОСТЬ

Современные сервисы создания датасетов разнообразны и многочисленны, и многие разработчики цифровых сущностей (возможно, их большинство) пользуются ими, не задумываясь об их структуре. Алгоритмы большинства провайдеров разметки, как продающих услуги, так и инхаусных, весьма схожи: разметка данных производится сотнями специалистов. И последующий выборочный контроль качества содержательными кураторами работ или клиентскими менеджерами имеет определенную эффективность.

Подобная методика практически эффективна, когда нужно разложить изображения на группы (например, кошки и собаки). Однако задача становится сложнее и актуальнее, если собак нужно разложить по породам или классифицировать изображе-

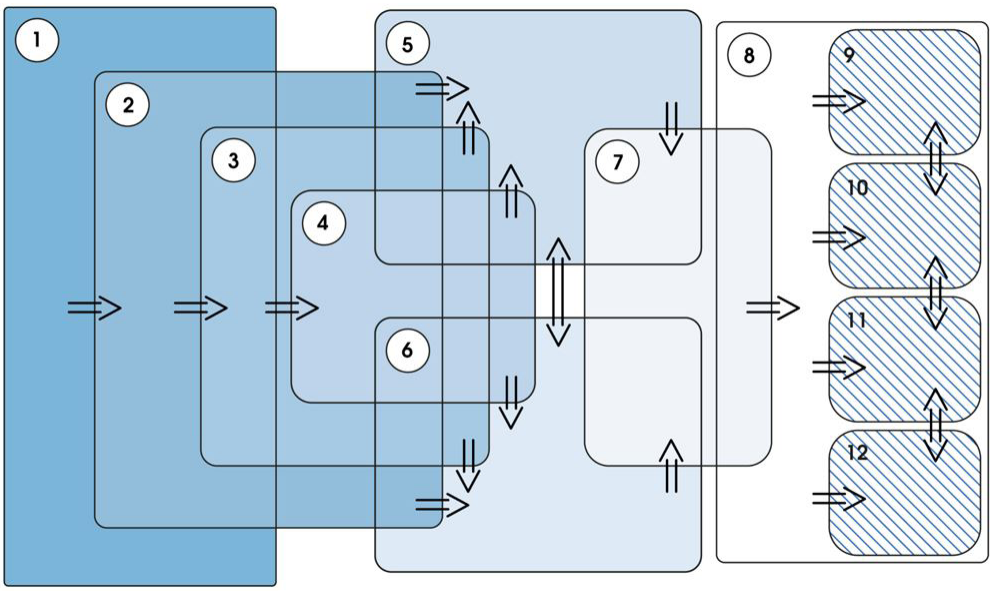


Рис.2. Приблизительная блок-схема КАА

ние с несколькими собаками. Специалисты по data science формируют такие признаки данных, которые впоследствии и составят объектность создаваемой сущности. Но здесь имеется своя отдельная область оптимизации, когда им предлагаются встройки и алгоритмы подсказок, включая итерационные. Для наших целей достаточно сказанного: субъектные суждения часто неизвестных людей формируют фундамент объектности «машин», «подсвечивая» нам ***первый аспект*** разметки данных, со связанностью с вариантами методик HITL (human in the loop).

Второй аспект влияния акторской субъектности на объектность создаваемых сущностей связан с мотивами таких специалистов и их уровнем квалификации, а в некоторых случаях – ценностями. По всему спектру подзадачных видов разметки, от прямых «распознавание сущностей»/«категоризация объектов» до косвенных «анализ тональностей»/«аннотирование и атрибутирование» уровень влияния различен, от незначительного до решающего (критического).

Например, если сравнить разметку данных из паремийного корпуса, для которого у одного дата-саентиста подстановочная пара мотиватора будет «герой» и «восторгаться», а у другого – «враг» и «победить», считаем, что невозможно оценивать полученный совместный продукт как равномерно выстроенный. Кроме того, коннотация слов «герой», «восторгаться», «враг», «победить» может различаться. Такие калибраторы объектности весьма далеки от семантически ламинарной субъектности всего сообщества специалистов.

Может ли помочь справиться с такими «рытвинами» ландшафта «большое» обучение? Если соотносить объектность и субъектность, в смыслах данной работы, с вещностью и социальностью сущностей, важно признавать, что большинство объектно-субъектных развилок в міре людей (биомиметически – модель цифровых сущностей, бионически – её прообраз) не дихотомичны, а скорее синтетичны. Соответственно, при идеальной аватарной генерации между вещностью (отражение объектности «машин») и социальностью (как проявление субъектности) не должно быть оператора [OR] (тем более [XOR]), а должен быть только оператор [AND].

Такая акцептность синтетичности, обеспечиваемая оператором [AND], могла бы выровнять большинство шероховатостей объектности ИИ-сущности, источник которых – различия в объектности аналитиков, в процессе обучения, и способствовать созданию за счет последующего применения техник статистической, вероятностной и феноменальной адаптации необходимого процесса воспитания сущностей.

Несмотря на то, что такая корректировка обучения в сторону воспитания не решит все проблемы объектно-субъектного характера, она позволит пройти ОС-развилки в отработке нейросетевых алгоритмов таким образом, чтобы не только выровнять погрешности объектности, но и организовать требуемый субъектностный потенциал на системном уровне. Конечно, такая нормализация не гарантирует «бесшовность» субъектности для цифровой сущности, но эта задача видится в принципе неразрешимой: любая экосистема, и даже выстроенная на операторах [AND], но основанная не на принципе копирования, а на подходах группы переноса качеств, не будет гомогенной.

Цифровую сущность невозможно гомогенизировать в гибридной человеко-машинной среде, созданной бионически, а биомиметически мы не можем создать её из-за нашего незнания исходной точки А. Однако хорошо известно, что наибольшее напряжение в гетерогенных системах возникает на границе раздела фаз. Именно организация (с полным охватом, от признания и локализации до источников и механизмов) границ в человеко-машинных дисперсиях и является максимально достижимой целью субъектного воспитания, дополняющего объектное обучение.

Такое целеполагание выявляет ещё одну проблему, требующую разрешения. Это эффект мультипликации элементов (вершин, объектов, связей, правил) при использовании [AND] вместо [OR/XOR]. Здесь нет и не может быть готовых способов, так как инструментарий постулированной выше лемматизации лишает возможности просто алгоритмизировать дизъюнкцию вместо конъюнкции.

Для исключения лавинообразного роста числа элементов в процессах обучения нам очень пригодилась бы технологическая возможность реализации витальной логики, которой нас лишила почти столетняя история безальтернативной бинарности. Удовлетворительным способом эмуляции нативной тринарности в контексте общепринятой практики бинарных вычислений может оказаться организация специальной категории элементов «неопределённые транзиты». Однако этот, семантически безусловно полезный приём, без пересмотра уже сложившихся и оптимизированных библиотек и практик может повлечь за собой неадекватный рост требований к перфомансу программно-аппаратной части создаваемых сущностей.

ВОСПИТАНИЕ АВАТАРОВ

Прогнозируемая реформация вычислительных подходов – зона наиболее остро воспринимаемого, но, вероятно, не самого значительного риска при переходе от обучения сущностей к воспитанию ава-

таров. Носительство главного антагонизма видим в субъектности участников стартовых этапов КАА-потока в сообществах, где происходит постановка задач и конструирование замыслов. Очевидно, что формируемые ими требования к объектности аватаров также отражают пройденные (проходимые) ими ОС-развилки. Но здесь мы прогнозируем уже не просто ОС-шероховатости объектного ландшафта, но буквально его «горы и реки».

В связи с этим применение БФА-модели становится практически неизбежным: по-другому учесть субъектности носителей компетенций, зачастую уникальных, выглядит непосильной задачей. И даже ожидаемое появление института когнитивно-семантических модераторов, умеющих разрешать проблемы Б-субъектности как-то иначе (без её коэффициентной реклассификации в А-субъектность), всё же, как мы полагаем, не лишит БФА-подход привлекательности. Однако на современном этапе становления ИИ-девелопмента вся тема акторской ОС-аккомодации признаётся и распознаётся весьма слабо, что ощутимо сказывается на клиентской активности, мешая возникновению (и способствуя отрицанию) гармонии субъектности между создателем, клиентом, и обслуживающей их отношения сущностью.

В качестве примера рассмотрим одну из существующих качественных медицинских ИИ-платформ. Потенциальный парадокс в том, что чем лучше она обучена, тем выше её объектность, но одновременно с этим выше риски её «кривой» субъектности: её версия принципа «не навреди» не транслятивна, а само понятие клятвы Гиппократа в этом случае теряет смысл. Убеждены, что никто из профессионалов цифровой индустрии не надеется, что использование хорошей медико-диагностической сущности будет закрытым внутри врачебного сообщества, в своём роде герметичным: инвестиции необходимо окупать, а самый маржинальный доход был и остаётся консьюмерским.

Эффективный цифровой доктор непременно выйдет за рамки профессионального применения в общедоступное пользовательское пространство, тем более в условиях постоянно дорожающей профессиональной медицины. Действительно, очень удобно загрузить в систему ряд анализов и получить диагноз и даже схему лечения. Но дальше пациент попадает под сильную энтропийную атаку всевозможных сетевых новостей, советов и справочников, и если «живой» доктор способен минимизировать риски для клиентского восприятия и сгладить острые углы, то «машина» может проявить себя самым циничным образом.

Следует отметить, что качественная цифровая объектность включает субъектную мотивацию на обеспечение качества, доступности, и охвата. К этому не относится множество по-настоящему вредных, открыто доступных «игрушек», с посылами маркетинга, направленными на потребительство (например, «диагностика заболеваний опорно-двигательной системы по анализу походки на Ваших бытовых видео»). Данные инструменты несут в себе признаки мошенничества, несмотря на то, что определённая объектность и у таких цифровых сервисов присутствует (пусть и пока потенциально).

Если продолжить тему перманентно динамичной задачности, то можно рассмотреть намного более распространённый кейс с ИИ-платформами распознавания лиц. Этот сервис уже весьма зрелый и настолько плотно вошёл в нашу жизнь, что мы часто не осознаем, насколько он фактически повлиял на социальность, создав возможность отслеживать каждый шаг человека. Может создаться видимость, что субъектность подобных систем остаётся за человеком (кто не совершает ничего противоправного, тому ничего и не угрожает). Однако на практике цифровая интрузия в субъектность человека постоянно растёт.

Из социологии известно, что наличие постоянно действующего, иногда нарастающего внешнего фактора, имеющего коммуникативную причинность, изменяет социальные связи («Бог создал людей слабых и сильных, а полковник Кольт уравнял их шансы»). Но, исходя из темпов жизни, надо полагать, что субъектность современного цифрового сопровождения будет осознана намного быстрее. Каждый желающий детально ознакомиться с проблематикой субъектности у изделий отрасли, ёмкость инвестиций в которую составляет миллиарды долларов в год, может обратиться к различным цифровым автопилотам, агрегаторам и результатам Chat-GPT: их рекурсивность уже сегодня весьма социальна.

КОГНИТИВНОСТЬ И СЕМАНТИКА. ПЕРСПЕКТИВЫ

На сегодня весьма высокого уровня зрелости достигла когнитивность большинства систем, при этом семантика остается под большим вопросом, поскольку алгоритмы реагирования на факты или события могут стремительно меняться. Как раньше шутили в одном закрытом сообществе, «жить надо так, чтобы было не стыдно перед службой наблюдения». Мы же сегодня все уже находимся в

фазе глобальной социализации подобной стратной бихевиористики. А это, вероятнее всего, необходимо принять как новые правила игры.

Прежде чем перейти к субстантивной части, скажем несколько слов о перспективе. Чтобы оттолкнуться от реактивной субъектности того, что создают сегодня ИИ-девелоперы (а многое из сказанного выше именно к ней и относится), отойдём от страдательного залога и порассуждаем в залоге действительном.

Проактивная субъектность не будет (по определению) характеризующей особенностью для систем (объектов) ассистанса: задачное пространство ожиданий от них функционально и не содержит в себе ничего социального. Но этого нельзя сказать о сущностях-носителях хоть какой-то индивидуальности. Сегодня мы пока ещё опасаемся и ограничиваем группу своих амбиций реконструкциями известных, в том числе исторических личностей. Не обращаясь за какими-либо примерами этих работ, заметим, что тоже ведём прикладной проект воссоздания генеративного образа одного из величайших социальных менторов цивилизации. Здесь, безусловно, наши ожидания отличаются и фокусируются именно на субъектности – проактивной и даже креативной.

Однако максимальную перспективу имеет, на наш взгляд, вовсе не реконструктивный, а реформативный трек, т.е. не цифровое возрождение, а создание сущностей на основе подобия действующим моделям, но имеющих целый ряд преимуществ перед ними и функционирующих быстрее, надёжнее, дольше. Если же не ограничивать себя рамками подобия (это вариант развилки биомиметики и бионики), то можно спрогнозировать не только улучшение существующих качеств у сущностей, но также их развитие и даже становление новых.

Чтобы обратиться непосредственно к аватарной алгоритмике, вспомним, что главной отличительной особенностью субъектности, в соотнесении с объектностью, является доминанта относительной дефиниторики по сравнению с их абсолютными детерминантами. Иначе говоря, объектность любой сущности (как в нашем случае – цифровой), можно описать набором каких-либо важных и существенных величин, а её субъектность – нельзя. Этот аспект раскрывается только разницами (сравнениями и отклонениями).

Такой «дельта-подход» не просто раскрывает суть субъектности в контексте витальной логики, но и определяет её. Второй важный аспект в том, что именно эта преимущественность сравнительной сигнатуры над абсолютными значениями тех параметров, которые определяют актность, и есть базовая особенность субъектности как основы любой социальности (неважно, человеческой или цифровой). В известном смысле это является той «подъёмной силой крыла», всё осознание которой цифровые архитекторы должны перенять из теории/практики человеческих социумов. В качестве примера можно привести лозунг «мы разные – в этом наше богатство» и девиз «мы вместе – в этом наша сила), из которых следует третий важный аспект – определение этого самого множества {мы}.

Полный профиль данного определения можно установить социально-физическим алгоритмом «ЧтоБэВэГэДэйка». Но необходимый минимум субстантивности (хотя не всегда достаточный) – это второй и третий из вопросов этой панели (напомним: «ЧтоБэВэГэДэйка» витальной логики – это ряд последовательных вопросов «что»/«кто»/«как»/«когда»/«зачем»). Понятно, что первый вопрос («что») во всех случаях, включая цифровое созидание, связан с объектностью сущностей, четвёртый – касается скорее динамики (здесь – социальной), а пятый («зачем») – отвечает в большей мере за технологический аспект (и обеспечивает целостность).

Вопрос «кто» формирует границы, определяет ёмкость и задаёт {мы}-ландшафт, вопрос «как» структурирует нам как базу, так и драйверы относительности. И если значение ответов на вопрос «кто» переоценить нельзя, то вопрос «как» вызывает больше сложностей и при этом часто – обоснованных.

Общим для объектности и субъектности сущностей являются их проявления: внешние – для объектности, и сумма внешних и внутренних – для субъектности. Субъектности не имеет, например, Галилеев шар (он ожидаемо падает, если сбросить его с Пизанской башни) или калькулятор (он хорош именно тогда, когда производит вычисления).

Во всех подобных проявлениях объектности присутствует те, кто сформулировал свои ожидания, кто создал соответствующую сущность и кто ею воспользовался. Но случае с коробкой (из которой можно непременно достать именно то, что туда положено) все три «объектных» роли объединяемы, и исполнить их может любой из нас (кроме последователей Гарри Гудини).

В случае с шаром легенда называет Галилео Галилея неким объединителем, при этом ясно, что всякую из этих ролей может также выполнить каждый из нас. Пример с калькулятором уже не столь однозначен (хотя и намного ближе к проблематике цифровых сущностей): далеко не всем, кто пользуется калькулятором, известно, кто ставил объ-

ектные задачи при его разработке. Этого могут не знать и непосредственные его производители, причем на функциональности самого устройства такое незнание практически не сказывается. Кроме того, с субъектностью калькулятора всё выглядит почти очевидно: это чистый сервис для того, кто на нём производит расчеты.

При расширении функциональности калькулятора таким образом, что он не просто высветит на дисплее конечную цифру месячного платежа по ипотеке, но ещё и даст информацию о том, что «в некотором банке платёж был бы на 17% меньше», игнорировать того, кто придал калькулятору такую добавленную объектность, нельзя. Причём как того, кто расширил перечень объектных параметров калькулятора любым рекомендательным аспектом, так и того, кто настроил рекомендательную схематику в конкретной кредитно-банковской функциональности.

Таким образом, мы видим современный тренд во множестве кейсов с вовлечением в нашу привычную сервис-среду так называемых «элементов искусственного интеллекта». В нём и постановка, и создание не столько проявляют свою объектность, сколько задают новую субъектность сущности, в цепочку создания ценности которой они вовлечены. Но тем самым они становятся акторами социального пространства пользователей калькулятора в его «умной» модификации.

С позиции витальной логики бесспорным признаком субъектности самого калькулятора является то, что он становится субстантивным посредником и между тремя участниками, ранее (в прошлом сервисе) не имевшими между собой когнитивного и семантического общего и с неизвестным числом акторов с непонятной ролевой моделью, которые являются источником данных для указанных выше 17%. Отметим, что «дельта-подход», как мера субъектности, в этом примере не в процентной базе, а в сравнении с прямым результатом счёта процентных выплат. Из сказанного может и не последовать понимание фокуса на акторских потенциалах тех или иных участников создания цифровых сущностей. Однако на иллюстрацию механизма проявления их субъектности мы всё же ясно рассчитываем.

ФОРМУЛА АВАТАРНОСТИ

Опираясь на сказанное выше, можно утверждать, что изменения в объектности обсуждаемой сущности, начиная с определённого уровня комплексности, скорректируют его субъектность. Граница такого уровня соответствует семантическому качеству: иной цвет корпуса калькулятора или другая форма клавиш, возможно, и приведут к изменению его продаж, но существенно не изменит ландшафт в акторском плане, за исключением появления в нём поставщика красителей или дизайнера (которые являются скорее пассивными акторами). Однако для понимания субъектности сущности необходимо знать не только состав акторов, но и особенности их вовлечения в объектность: форматы, цели, способы, режимы и т.д. В примере с появлением у калькулятора функции советчика речь может идти о прямой рекламе, демпинге, перекредитовании, комиссии и др.

В этих обстоятельствах отсылки к лучшему опыту и лидерам отрасли с нераскрытием активного акторства (создателей), явно и серьёзно ограничивают клиентов как пассивных акторов в их реактивности. На сегодняшний день более, чем в 85% разработок от IBM Watson for Oncology (WfO) за 7 лет её становления (закончившегося провалом по качеству) содержался прямой запрос на доверительность результатов ассистанса (в смысле их авторства). В общем случае число «клиентов» системы, которым доводилась информация, что фактическое авторство продуктов WfO было за группой врачей из нью-йоркского онкологического центра Слоуна-Кеттеринга, было очень невелико (некоторые из имён не известны до сих пор).

Очевидно, что такая позиция создателей не только мешает содержательно отвечать на предметные вопросы, но даже доходить до них. Такой ущерб субъектности особенно заметен в ситуациях нарушения целостности объектно-субъектного потока не в итоге осознанного выбора пользователей (такие системы уже есть и их будет больше), а как результат определяемых разработчиками ИИ-систем ограничений.

В ситуации с подбором музыки от Алисы пользователь изначально соглашается с тем, что оценкой предлагаемого ему репертуара занимается неизвестый ему (возможно, коллективный) эксперт разметки. Также в кейсе с WfO от IBM нет прямого принуждения к использованию ИИ-сущности в диагностике и терапии тяжёлых состояний. В обоих примерах субъектность отношения конечного актора с системой не искажается третьими лицами.

Иная ситуация с распознаванием лиц на улицах или на транспорте: обыденный событийный поток конечного актора здесь заключается в его движении, а не в самоэкспонировании. И тут анонимность специалистов по разметке, как и экспертов по обучению ИИ-сущности, уже создаёт вектор от-

рицающего напряжения: если человека необоснованно задержит полицейский, норма социальности в коммуникации сохраняется за счёт субъектности выставления претензий к такому обознавшемуся.

При этом непонятно, кому выставлять претензии при нарушении событийного потока ложным срабатыванием от ИИ-сущности, обученной неизвестным экспертом на анонимном датасете с анонимной разметкой. Такую проблему искажения субъектности в вынужденной коммуникации «человек-машина» на треке анонимной объектности, вероятно, не получится решить регулированием постфактум (на сегодняшний день весьма посредственным).

Без учёта вопросов этичности погружения конечных акторов в среды с высокой интенсивностью коммуникации человека и цифровых сущностей любая аватарная алгоритмика не может быть создана в обход витальной логической цепочки или с её разрывами.

Выдвигая этот весьма жёсткий постулат, начнём с ⑤-й КАА-области. Пусть объектность некоторой сущности задаётся в тензорном виде [5] матрицей $a_{ij}a_{ij}$; это реализованный ответ на «что»-вопрос. Тогда ответ на «кто»-вопрос создаёт такое множество $\{b_{ij}b_{ij}\}$, контекстная обработка которого позволяет нам сформировать базу для расчёта субъектности c_ic_i, а ответ на «как»-вопрос задаёт драйвер этих расчётов. Для иллюстративной простоты здесь предположим равнозначный и равновероятный тип корреспонденции элементов множества $\{b_{ij}b_{ij}\}$ между собой. Тогда аватарность тут будет иметь предельно простой вид:

$$c_{ij} = f(a_{ij},\{b_{ij}\}\ ) = (a_{ij} - \bar{b}_{ij})/x_{ij}c_{ij} =$$

$$= f(a_{ij},\{b_{ij}\}\ ) = (a_{ij} - \bar{b}_{ij})/x_{ij},$$

где $\bar{b}_{ij}\bar{b}_{ij}$ это матричный определитель множества $\{b_{ij}b_{ij}\}$ (чаще всего он медианальный $\hat{b}_{ij}\hat{b}_{ij}$ или модальный $\ddot{b}_{ij}\ddot{b}_{ij}$), а переменная $x_{ij}x_{ij}$ определяет как вариативность аватара $x_{ij} \equiv a_{ij}x_{ij} \equiv a_{ij}$, так и флексибельность $x_{ij} \equiv b_{ij}x_{ij} \equiv b_{ij}$ (семантика различий родственна понятиям «проценту на» и «проценту от», применяемому к любым смежным базам приведения).

Практическое применение для аватарной алгоритмизации также весьма несложно. И если, к примеру, конкретные матрицы $a_{ij}a_{ij}$ и $\ddot{b}_{ij}\ddot{b}_{ij}$, как дескрипторы объектности, имеют в одном нашем проекте («ТЖ»; кейс <39050041112954316 8>; мода 613 кейсов; в %) следующий вид

$$\begin{pmatrix} 294 & 250 & 233 & 288 & 238 \\ 220 & 267 & 255 & 262 & 256 \\ 261 & 264 & 288 & 291 & 277 \\ 291 & 250 & 300 & 280 & 233 \\ 245 & 263 & 273 & 300 & 236 \\ 300 & 273 & 288 & 300 & 289 \\ 291 & 288 & 252 & 300 & 260 \end{pmatrix} \begin{pmatrix} 294 & 250 & 233 & 288 & 238 \\ 220 & 267 & 255 & 262 & 256 \\ 261 & 264 & 288 & 291 & 277 \\ 291 & 250 & 300 & 280 & 233 \\ 245 & 263 & 273 & 300 & 236 \\ 300 & 273 & 288 & 300 & 289 \\ 291 & 288 & 252 & 300 & 260 \end{pmatrix},$$

$$\begin{pmatrix} 300 & 300 & 287 & 288 & 288 \\ 260 & 300 & 291 & 292 & 289 \\ 294 & 300 & 300 & 282 & 285 \\ 300 & 300 & 300 & 300 & 287 \\ 282 & 294 & 300 & 300 & 286 \\ 300 & 300 & 300 & 300 & 289 \\ 300 & 300 & 274 & 290 & 263 \end{pmatrix} \begin{pmatrix} 300 & 300 & 287 & 288 & 288 \\ 260 & 300 & 291 & 292 & 289 \\ 294 & 300 & 300 & 282 & 285 \\ 300 & 300 & 300 & 300 & 287 \\ 282 & 294 & 300 & 300 & 286 \\ 300 & 300 & 300 & 300 & 289 \\ 300 & 300 & 274 & 290 & 263 \end{pmatrix}$$

то соответствующие аватарные дефиниторы будут выглядеть так (в ppm):

$$\begin{pmatrix} (020) & (167) & (188) & 000 & (174) \\ (154) & (110) & (124) & (103) & (114) \\ (112) & (120) & (040) & 032 & (028) \\ (030) & (167) & 000 & (067) & (188) \\ (131) & (106) & (090) & 000 & (175) \\ 000 & (090) & (040) & 000 & 000 \\ (030) & (040) & (080) & 035 & (011) \end{pmatrix} \begin{pmatrix} (020) & (167) & (188) & 000 & (174) \\ (154) & (110) & (124) & (103) & (114) \\ (112) & (120) & (040) & 032 & (028) \\ (030) & (167) & 000 & (067) & (188) \\ (131) & (106) & (090) & 000 & (175) \\ 000 & (090) & (040) & 000 & 000 \\ (030) & (040) & (080) & 035 & (011) \end{pmatrix}$$

$$\begin{pmatrix} -20 & -200 & -219 & 0 & -210 \\ -182 & -124 & -141 & -115 & -129 \\ -127 & -136 & -42 & 31 & -29 \\ -31 & -200 & 0 & -72 & -232 \\ -151 & -118 & -99 & 0 & -212 \\ 0 & -99 & -42 & 0 & 0 \\ -31 & -42 & -88 & 33 & -12 \end{pmatrix} \begin{pmatrix} -20 & -200 & -219 & 0 & -210 \\ -182 & -124 & -141 & -115 & -129 \\ -127 & -136 & -42 & 31 & -29 \\ -31 & -200 & 0 & -72 & -232 \\ -151 & -118 & -99 & 0 & -212 \\ 0 & -99 & -42 & 0 & 0 \\ -31 & -42 & -88 & 33 & -12 \end{pmatrix}$$

Левая матрица описывает флексибельную субъектность смоделированного аватара в модальной базе $(\ddot{c}_f)_{ij}(\ddot{c}_f)_{ij}$, правая — её вариативно-модальную субъектность $(\ddot{c}_v)_{ij}(\ddot{c}_v)_{ij}$.

Комментарии к их практической разнице задают нам смыслы референтного проекта: $c_f c_f$ относится к реактивным проявлениям субъектности (относительно любых внешних энтропийных проявлений), а $c_v c_v$ к проактивной негэнтропийной субъектности (создание и/или распространение негэнтропий по З.У.Р.Т.-механизму [6]).

Для полноты иллюстрации, нужно сказать несколько слов и о выборе $\hat{b}_{ij} \leftarrow \bar{b}_{ij} \rightarrow \ddot{b}_{ij}$ $\hat{b}_{ij} \leftarrow \bar{b}_{ij} \rightarrow \ddot{b}_{ij}$ в плане аватарной базы: медианальный (левый) применим чаще модального (правого). Но связано это не столько с тем, что медиана расчётно строже, сколько с характером создаваемой сущности. В проекте, из которого позаимствована иллюстрация, не потребовалось ни среднего пропорционального, ни среднего гармонического при создании проектных аватаров: он семантический (СП), поэтому и выбор был модальным.

Однако в моделировании сущностей с прямой объектностью их коммуникативных треков (когнитивные (КП), или когнитивно-семантические (КСП) проекты), принятые нами выше упрощения (равнозначность или равновероятность для корреспондирующих между собой элементов множества $\{b_{ij}b_{ij}\}$) могут (будут) влиять на качество созидаемых аватаров. Причём влияние будет тем сильнее, чем более целевыми будут их параметры объектности, имеющие субъектные проявления, с одной стороны; или чем сложнее будет их статичная когнитивно-семантическая структура, или чем шире будут страты, составляющие их целевые клиентские сегменты (ЦКС), или другие факторы.

Таких вариантов можно привести больше десяти, а их анализ и учёт сам по себе представляет собой весьма интересную и непростую научную задачу, субстантивно соотносимую с мерой оценки комплексной социальности моделируемой сущности.

Безусловно, неравновероятность больше отразится на К-проектах. Соответственно, отработка частных (нестатистических!) алгоритмов пробабельности (например, обсервационная эвристика) в формировании элементов $\{b_{ij}b_{ij}\}$ принципиально важна для калькуляции дескриптора $\hat{b}_{ij}\hat{b}_{ij}$ (причём для расчёта $(\hat{c}_f)_{ij}(\hat{c}_f)_{ij}$ — важна критически). Лучший способ здесь, конечно, пространственное представление ij ij с вероятностной топологией поля. Но поскольку он, как правило весьма затратен, то допустимой альтернативой видится любой подходящий тензор-векторный алгоритм, например, вариант, опирающийся на факторизацию Такера от Яна-Дансона [7]. Что касается неравнозначности, она учитывается сравнительно проще: в её отношении допустимо и желательно применение подходящих статистических субалгоритмов, вопрос лишь в источниках данных и стоимости их сборки и подготовки.

Проиллюстрируем сказанное на упомянутом кейсе <39050041112954316 8> проекта. Выше показано, как для оценок $\ddot{c}_{ij}\ddot{c}_{ij}$-х использовалась мода выборки из 613-ти кейсов ($b_{ij}b_{ij}$), объектно стратифицируемых как целевая группа модельных сущностей. Если же расширить ЦКС, то число кейсов вырастет до 4237, а медианальная матрица, после вероятностных корректировок и предметного анализа ($\hat{b}_{ij}\hat{b}_{ij}$) изменится и приобретёт следующий вид:

$$\begin{pmatrix} 294 & 250 & 233 & 288 & 238 \\ 220 & 267 & 255 & 262 & 256 \\ 261 & 264 & 288 & 291 & 277 \\ 291 & 250 & 300 & 280 & 233 \\ 245 & 263 & 273 & 300 & 236 \\ 300 & 273 & 288 & 300 & 289 \\ 291 & 288 & 252 & 300 & 260 \end{pmatrix} \begin{pmatrix} 294 & 250 & 233 & 288 & 238 \\ 220 & 267 & 255 & 262 & 256 \\ 261 & 264 & 288 & 291 & 277 \\ 291 & 250 & 300 & 280 & 233 \\ 245 & 263 & 273 & 300 & 236 \\ 300 & 273 & 288 & 300 & 289 \\ 291 & 288 & 252 & 300 & 260 \end{pmatrix}$$

$$\begin{pmatrix} 306 & 227 & 217 & 224 & 274 \\ 232 & 251 & 298 & 261 & 274 \\ 274 & 257 & 273 & 275 & 294 \\ 296 & 291 & 274 & 297 & 217 \\ 299 & 283 & 282 & 269 & 251 \\ 292 & 305 & 314 & 273 & 321 \\ 297 & 274 & 280 & 266 & 257 \end{pmatrix} \begin{pmatrix} 306 & 227 & 217 & 224 & 274 \\ 232 & 251 & 298 & 261 & 274 \\ 274 & 257 & 273 & 275 & 294 \\ 296 & 291 & 274 & 297 & 217 \\ 299 & 283 & 282 & 269 & 251 \\ 292 & 305 & 314 & 273 & 321 \\ 297 & 274 & 280 & 266 & 257 \end{pmatrix}$$

Тогда изменятся и аватарные дефиниторы проекта <39050041112954316 8>, причём и для флексибельно-медианной субъектности $(\hat{c}_f)_{ij}(\hat{c}_f)_{ij}$, и для вариативной $(\hat{c}_v)_{ij}(\hat{c}_v)_{ij}$:

$$\begin{pmatrix} (039) & 101 & 074 & 286 & (131) \\ (052) & 064 & (144) & 004 & (066) \\ (048) & 027 & 055 & 058 & (058) \\ (017) & (141) & 095 & (057) & 074 \\ (181) & (071) & (032) & 115 & (060) \\ 027 & (105) & (083) & 099 & (100) \\ (020) & 051 & (100) & 128 & 012 \end{pmatrix} \begin{pmatrix} (039) & 101 & 074 & 286 & (131) \\ (052) & 064 & (144) & 004 & (066) \\ (048) & 027 & 055 & 058 & (058) \\ (017) & (141) & 095 & (057) & 074 \\ (181) & (071) & (032) & 115 & (060) \\ 027 & (105) & (083) & 099 & (100) \\ (020) & 051 & (100) & 128 & 012 \end{pmatrix}$$

$$\begin{pmatrix} -41 & 92 & 69 & 222 & -151 \\ -55 & 60 & -169 & 4 & -70 \\ -50 & 27 & 52 & 55 & -61 \\ -17 & -164 & 87 & -61 & 69 \\ -220 & -76 & -33 & 103 & -64 \\ 27 & -117 & -90 & 90 & -111 \\ -21 & -49 & -111 & 113 & 12 \end{pmatrix} \begin{pmatrix} -41 & 92 & 69 & 222 & -151 \\ -55 & 60 & -169 & 4 & -70 \\ -50 & 27 & 52 & 55 & -61 \\ -17 & -164 & 87 & -61 & 69 \\ -220 & -76 & -33 & 103 & -64 \\ 27 & -117 & -90 & 90 & -111 \\ -21 & -49 & -111 & 113 & 12 \end{pmatrix}$$

Как и предполагалось, изменения $\bar{c}_{ij}\bar{c}_{ij}$ весьма существенные, при этом различия в субъектности настраиваемых аватар-моделей при неизменной объектности будут также весьма значительны при расширении ЦКС и переходе от моды к медиане.

ОБЩИЙ КОНСТРУКТ АВАТАРНОЙ АЛГОРИТМИЗАЦИИ

Очевидно, что даже смыслы объект-субъектной специфичности весьма контекстны, и зависят от множества нюансов, начиная с целеполагания и заканчивая техническими аспектами платформ их сущностной реализации. Однако общий конструкт аватарной алгоритмизации, в проектах социально-физического моделирования, можно сформулировать в рамках витальной логики следующим образом:

1. **Что** мы хотим зафиксировать как содержательные характеристики создаваемой в проекте цифровой сущности. Это рефлексия целеполагания в наглядности и убедительности аналога (или образца при наличии), неизбыточности исходных данных, технологической зрелости и модельной завершённости. Но это и не столько треки состоятельности объектного образа моделируемой (создаваемой) сущности, сколько ещё предпосылки её субъектности, иными словами — первая «ладонь, сжатая в кулак», необходимая для обеспечения гармонии при проектировании любой социальной сущности.

2. **Кто** выполняет отработку планово функционирующей цифровой сущности после её старта. Здесь драйверами созидательной активности становится вторая «ладонь, сжатая в кулак»: субъектная диспозиция (в вертикалях, горизонталях или диагоналях коммуникации) с динамической целостностью объектных и субъектных свойств и связей, подбором дефицитных мер и метрик, охватом контингента и его проявленной общеакцептной этикой. Следует иметь в виду: именно на этом этапе созидания риски искажения офертности создаваемой сущности максимальны.

3. **Как** обеспечивается субъектная сохранность цифровой сущности на её проектном уровне. Зачастую этот аспект смешивается с подчинённостью «цифры человеку», гарантиями сервисности сущности и невыхода её за рамки. И хотя для большинства заинтересованных лиц границы тут весьма умозрительны, главным (пусть и не единственным) фокусом внимания является нужная квалификация оператора. Что не совсем оптимально, т.к. именно здесь находятся основные потенциалы границ офертности и акцептности, прямо связанных с социальностью.

4. **Когда** событийные потоки (проявляющие или формирующие их информационные) в части субъектных актностей начинают превалировать над объектными. При этом само понятие временной обусловленности аватарной алгоритмики основано не на временной шкале, а на феноменологической (на шкале явлений). Значит, что библиотека событий, связанных с объектностью, должна содержать в себе либо субъектный ракурс, или же субъектный раздел. Это автоматически предъявляет к конкретным аватарным алгоритмам требование объектно-субъектной связанности.

5. **Зачем** наряду с обработчиками использовать концентрирующие платформенные субалгоритмы, дополняющие объектные аспекты вероятностными сигнатурами и статистическими усилителями субъектности. Формируемое этим расширение рамок как обеспечивает целевую функционально-ролевую корректность сущности, так и задаёт необходимую и достаточную волатильность аватарности (здесь — потенциал массива объектности к реализации комплекса субъектности). Обзор производных проявлений в смежных обстоятельствах — среди главных задач этого шага.

Отдельно отметим отсутствие в конструкте правовых аспектов. Причины этого не в том, что специальное легальное поле цифровых сущностей, в значительной степени, в большинстве сообществ ещё не разработано, и не в том, что зрелые акты (когда они всё же присутствуют) имеют чаще всего общеправовой характер, вследствие чего специальных практик учёта и применения не требуют. Главная причина заключается в том, что нормы юридической регуляции любых активностей, способных значительно скорректировать социальные ландшафты (это как раз наш случай), являются главным образом вторичными по отношению к возникающим проявлениям общественной акцептности.

В отношении же цифровых сущностей (как будущей нормы взаимодействия «человек-машина») видится целесообразным избегать расхождений между законом и моралью. Нам больше импонирует позиция, при которой закон выступает в качестве костыля для морали, подпирающего её в случаях слишком широкого шага или слишком тяжёлого груза. Но в таком случае стратегические настройки визионарности созидания перспективных социальных платформ с опорой на действующие правовые конструкции выглядят как институционализация инвалидности (что вряд ли уместно).

Весьма наглядный пример, иллюстрирующий подобную рассогласованность, можно вывести из анализа истории создания и внедрения систем автопилотирования, имея в виду, в первую очередь, пространство коллизий совместного с автопилотами трафика водителей-людей в самых обычных потоках на дорогах общего пользования. Помимо всего, вязкость данного кейса показывает нам важность уроков этического ландшафта (на «кто»-шаге алгоритмизации) и ответственной работы оператора (на «как»-этапе): показательный перекос портфеля свойств созданных сущностей на их объектность, с недооценкой субъектности.

В связи с этим подчеркнём факт наличия продолжающегося дефицита внимания к проблеме анонимности носителей суждений, которые закладываются в датасеты обучения ИИ-систем, начиная с фазы их разметки. Для отражения этого аспекта субъектности (наряду с коллизиями закона и морали) именно «как»-этап алгоритмики должен держать фокус на акцептной этике созидания сущностей.

ЗАКЛЮЧЕНИЕ

Предложенный конструкт аватарной алгоритмизации не является единственным и универсальным, а эмпирического опыта в этой области на сегодняшний день недостаточно, что говорит скорее о фундаментальной неисследованности проблемы объектно-субъектных лакун как движущей силы развития аватарной алгоритмики.

При идеальной аватарной генерации должен быть обеспечен комплексный синтез объектности системы и её субъектности. Такой синтез может решить множество задач для ИИ-сущности, источник которых – различия в подходах аналитиков и в процессе обучения, и способствовать созданию за счет последующего применения техник статистической, вероятностной и феноменологической адаптации необходимого процесса воспитания сущностей.

Для обеспечения процесса разработки алгоритмов аватарных сущностей весьма важно наличие технологической возможности реализации витальной логики на принципах тринарной логики, в рамках которой может происходить эволюция от искусственного интеллекта к синтетическому сознанию. Также в ходе разработки представляется рациональной реализация субъектного обогащения объектных аналитик и их прикладной мэппинг.

В области искусственного интеллекта в целом необходимо учитывать, что складывающаяся на настоящий момент «незаметность» субъектности для разработчиков цифровых сущностей является лишь следствием её комплиментарности к целеустанавливаемой объектности и принципа «когда правильно — тогда и незаметно». Полагаем, что проблема субъектности становится всё заметней.

СПИСОК ЛИТЕРАТУРЫ

1. Алиев Д.Ф. Социальная физика 5.0. Научная монография.- М.: Издательство РГСУ, 2023.- 488 с. ISBN 978-5-7139-1482-0

2. Щербаков А.Ю. Концепция и сложности реализации тринарной логики // Вестник современных цифровых технологий, 2024. №19. С.48-50.

3. Алиев Д.Ф. Образ цифрового будущего: «О дивный новый мір» //Вестник современных цифровых технологий, 2024. №19. С.51-55.

4. Алиев Д.Ф. БОТ // Научная монография.- М.:Издательство РГСУ, 2023.- 144 с.

5. Алиев Д.Ф. Основы тензорного аппарата для современных социально-гуманитарных наук // Вестник современных цифровых технологий, 2024. №19. С.14-27

6. Алиев Д.Ф., Климантова Г.И., Петрова Е.А., Танатова Д.К., Солодуха П.В., Щербаков А.Ю. Современная социальная повестка: вопросы теории // Научная монография.- М.: Издательство РГСУ, 2024.- 219 с.

7. Yun Yang, David B. Dunson; «Bayesian conditional tensor factorizations for high-dimensional classification», Journal of the American Statistical Association, vol.111, 2016; https://doi.org/10.1080/01621459.2015.1029129.

УДК: 004.414.23

Методика синтеза объектно-ориентированной программной модели терминала релейной защиты из его функционального описания

N.A. Galanina, S.V. Petrov

Methodology of Synthesis of an Object-Oriented Program Model of a Relay Protection Terminal From its Functional Description

Abstract. *The article proposes a methodology for synthesizing object-oriented software models of relay protection and automation (RPA) terminal protection functions. The methodology is designed to reduce the development time of software for RPA devices in the context of constantly changing requirements for their functionality. The input data of the proposed methodology is a functional description of the RPA terminal, interpreted as a subject area. The result of applying the methodology are synthesized software models of entities representing the RPA functionality, input data sources, control data sources, and displays of RPA function states. The synthesized software entities represent the structure of the RPA terminal software and are the basis for further implementation of its internal software, as well as digital twins of the device.*

Keywords: *relay protection and automation, object-oriented approach, simulation modeling, software model, object model.*

Н.А. Галанина[1]
С.В. Петров[2]
[1]Доктор технических наук, доцент, профессор кафедры математического и аппаратного обеспечения информационных систем, Чувашский государственный университет им. И.Н. Ульянова.
E-mail: galaninacheb@mail.ru
[2]Аспирант кафедры математического и аппаратного обеспечения информационных систем, Чувашский государственный университет им. И.Н. Ульянова.
E-mail: eight@bk.ru

Аннотация. *В статье предлагается методика синтеза объектно-ориентированных программных моделей функций защит терминала релейной защиты и автоматизации (РЗА). Методика предназначена для сокращения времени разработки программного обеспечения (ПО) устройств РЗА в условиях постоянно меняющихся требований к их функционалу. Входными данными предложенной методики является функциональное описание терминала РЗА, интерпретируемого в качестве предметной области. Результатом применения методики являются синтезированные программные модели сущностей, представляющие функционал РЗА, источники входных данных, источники управляющих данных, отображения состояний функций РЗА. Синтезированные программные сущности представляют структуру ПО терминала РЗА и являются основой для дальнейшей реализации его внутреннего ПО, а также цифровых двойников устройства.*

Ключевые слова: *релейная защита и автоматика, объектно-ориентированный подход, имитационное моделирование, программная модель, объектная модель.*

ВВЕДЕНИЕ

В настоящий момент разработка ПО компонентов электротехнических комплексов и систем (ЭКС) ведётся в условиях постоянно меняющихся технических требований (ТТ) к системе. Это обуславливается различными требованиями к функционалу ПО заказчиков, непрерывным процессом переработки руководящих и нормативных документов отраслей, стандартов организаций (СТО) и поддержания ПО в актуальном состоянии в течение жизненного цикла ПО.

Со сменой ТТ меняется техническое задание (ТЗ) и цикл разработки ПО возвращается на этап проработки новых ТТ, нового ТЗ и т. д. Это ведёт к очередному витку разработки (или модификации архитектуры) ПО и его реализации и, соответственно, к увеличению сроков и стоимости разработки ПО.

Меняющиеся ТТ и ТЗ, основанные, например, на международных и отечественных стандартах [1, 2], приводят в т.ч. к возникновению следующих проблем:

- увеличение времени разработки ПО;
- задержка выпуска обновлений ПО для уже существующих устройств (как правило, это ПО с исправлениями ошибок, выявленных в предыдущих версиях ПО, а также с новым функционалом);
- увеличение времени вывода на рынок новых устройств и, как следствие, увеличение стоимости разработки ПО для компонентов ЭКС.

В настоящее время существуют вспомогательные методы и средства помощи в разработке ПО. Эти средства позволяют разработчикам сокращать время на проектирование и разработку ПО, а также помогают бороться с увеличивающейся сложностью разрабатываемого ПО [3].

Современные методики автоматизированной помощи при разработке ПО описываются набором методик и инструментария для автоматизации процесса проектирования и разработки ПО (computer-aided software engineering, CASE). Однако методики CASE не в полной мере удовлетворяют потребности синтеза ПО. Проблемы и вопросы автоматизированного синтеза ПО рассматриваются в работах авторов [4, 5]. Так, в работах [4, 5] автор предлагает использовать синтез диаграмм унифицированного языка моделирования (unified modeling language, UML) и последующую генерацию программного кода. UML-диаграммы синтезируются в результате последовательного набора сущностей предметной области (ПрО) в специальное ПО, условно относящееся к CASE средствам, с дальнейшей генерацией программного кода существующими модулями расширения распространённых сред разработки ПО [6, 7].

Следует отметить, что на сегодняшний день средства и методы автоматизированного синтеза ПО непосредственно из ТТ или ТЗ, написанных на естественных языках, развиты в недостаточной мере, что требует проработки этой темы. Предлагаемая в настоящей работе методика синтеза ПО поэтапно анализирует ПрО, описанную естественным языком и синтезирует такое же описание ПрО, но в виде программного кода для объектно-ориентированного языка программирования (ЯП). Новизна методики заключается в том, что разработчик ПО не вникает в описание ПрО, а работает с уже синтезированным объектно-ориентированным кодом и занимается реализацией алгоритмической составляющей ПрО и адаптацией ПО для применяемой операционной системы (ОС). Преимущества методики перед традиционным способом разработки ПО заключается в том, что разработчик не тратит время на изучение ПрО и на устранение архитектурных ошибок вследствие непонимания нюансов ПрО. Синтезированный объектно-ориентированный программный код имеет еще одно важное преимущество — вследствие своей объектной природы он может относительно легко интегрироваться в уже существующее ПО, расширяя существующий функционал.

Целью данной работы является разработка методики автоматизированного синтеза ПО моделей компонентов ЭКС в принципах ООП и её аналитическая оценка. Результат применения методики оценивается на сравнении описания предметной области в виде функционального описания устройства РЗА и структуры полученного ПО.

Решением проблемы вариативного и трудно прогнозируемого времени на разработку ПО может стать предлагаемая в данной работе методика автоматизированного синтеза ПО, суть которой заключается в автоматизации процесса анализа предметной области и генерации объектно-ориентированного программного кода. Объектно-ориентированный программный код синтезируется в соответствии с определением программной сущности, требованиями к поведению и атрибутам программной сущности, связями между программными сущностями.

ОПИСАНИЕ МЕТОДИКИ

Предлагаемая методика автоматизированного синтеза ПО преобразовывает техническое описание ПрО в программный код в соответствии с принципами ООП. Программный код является формализованным описанием ПрО в синтаксисе заданного ЯП. Таким образом, предлагаемая методика не должна вносить изменений в функционал ПрО. Методика описывает ПрО в ином виде — программном коде. Неизменность функционала, описанного в ПрО, является критерием оценки правильности работоспособности методики — ПрО не изменяется структурно и функционально.

Методика работает по принципу «чёрного ящика»: на вход подаются входные данные, далее происходит их преобразование, на выходе появляется результат работы — программный код (рис. 1). Входными данными является описание ПрО в виде технического описания. Техническим описанием ПрО может служить ТТ, ТЗ, РЭ и любое другое описание ПрО, оформленное в техническом стиле.

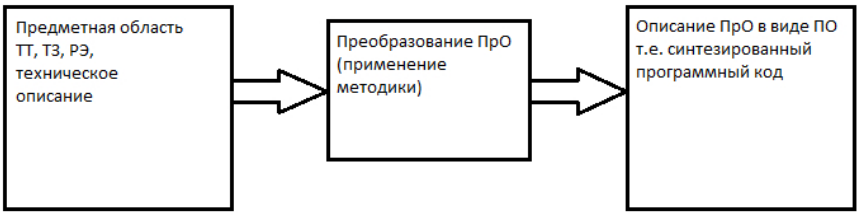


Рис. 1. Преобразование ПрО в ПО

Для процесса преобразования ПрО в ПО по предлагаемой методике дадим представление ПрО, с которым работает методика. Исходное техническое описание ПрО (т. е. сама ПрО) описывает сущности, их функциональное назначение и связи между сущностями. Сущности состоят из наборов других сущностей и простых элементов [8]. Сущности имеют функциональные назначения, т. е. действия, которые они выполняют.

В общем виде положения (задачи) методики можно описать следующим образом:

- анализ ПрО на наличие сущностей [9];
- описание сущностей ПрО;
- выявление связей между сущностями;
- трансформирование сущности ПрО в программные сущности и связи между ними.

В соответствии с объектно-ориентированным подходом (ООП) каждая программная сущность представляет собой объект, состоящий из атрибутов и поведения. Атрибуты могут быть как элементарными, так и составными [8].

Рассмотрим описанные положения подробнее и декомпозируем их по необходимости, исходя из требования «атомарности» задачи (задача должна строго выполнять одну функцию).

Первой задачей методики является *выявление всех сущностей*, содержащихся в ПрО. На этом этапе ПрО анализируется на наличие любых сущностей [9], составляющих ПрО. Результатом выполнения первой задачи является список сущностей ПрО. Каждая полученная сущность является абстракцией в понимании ООП, т. е. это есть абстрактное описание элемента ПрО [10, 11]. Полученное множество сущностей не является окончательным и будет модифицироваться в дальнейшем.

Следующая задача — *описание выявленных на первом этапе сущностей*. Описание сущностей для их преобразования в объектно-ориентированный программный код разбивается на два этапа: описание состава сущностей (атрибуты) [8] и описание их функционального назначения, т. е. их поведения (функции в программном коде) [12]. Задача декомпозируется на две атомарные задачи: описание поведения сущностей и описание состава сущностей. Следовательно: вторая задача методики — описание поведения (будущих программных функций) сущностей [12].

Третья задача — *описание состава сущностей* [8]. Результатом решения второй задачи является описание поведения сущностей, т. е. их функции (в ООП ещё называют интерфейс). Результатом решения третьей задачи является описание состава сущностей — т. е. набор атрибутов, совокупность которых представляет собой сущность. Разделение задачи на две подзадачи — описание сущности в виде совокупности атрибутов и функций происходит из такого принципа ООП, как инкапсуляция [3, 10, 11]. Все атрибуты скрыты в сущности и манипуляции над ними осуществляются строго через интерфейс — функции сущностей. Все данные сущности сокрыты в ней и недоступны извне.

Результатами выполнения первых трёх задач методики является описание множества сформированных сущностей. Полученные множества сущностей могут иметь общие множества атрибутов и общие множества функций. В соответствии с ООП общности необходимо описать в общие (базовые) сущности [3, 10, 11]. Выделение базовых сущностей в дальнейшем помогает избегать дублирования программного кода, а также упрощает расширение программных сущностей в дальнейшем. Ещё одним положительным результатом выделения базовых сущностей является выполнение общепринятого принципа программирования DRY (do not repeat yourself — не повторяй себя).

Следовательно, возникает следующая, четвёртая, задача, явно не описанная выше, и основанная на результатах выполнения предыдущих трёх задач — *определение общего поведения* (общих функций) и *определение общего состава сущностей* (т.е. определение базовых сущностей). На этом же этапе выполняется редуцирование состава сущностей, имеющих базовые сущности. Из множества атрибутов сущности исключаются атрибуты, выносимые в базовую сущность, из множества функций сущности исключаются функции, выносимые в базовую сущность. Результатом выполнения четвёртой задачи является множество явно не описанных в ПрО сущностей, редуцирование состава и функций сущностей, имеющих базовые сущности.

Пятой задачей является *определение связей между сущностями*, полученными в результате решения предыдущих четырёх задач. Связи между сущностями определяются отношениями между сущностями. В предложенной методике применяются отношения *наследования, агрегации и ассоциации* [13]. Исходя из целостности описания ПрО, все сущности должны иметь связь, по крайней мере, с одной сущностью. Т. к. наследование является отношением «часть чего-либо», в первую очередь выявляются связи сущностей «наследование». Во вторую очередь выявляются связи сущностей «агрегация». В результате определения связей «агрегация» появляются сущности, состоящие не только из элементарных атрибутов, но и из составных (сложных) [8]. Отношения «ассоциация» выстраиваются, в

последнюю очередь, между уже сформированными сущностями и определяют взаимодействие сущностей, выражаемых в программном коде. Результатом выполнения задачи является набор связей между множеством сущностей, полученных в результате выполнения предыдущих четырёх задач.

Результатом решения пяти описанных задач является множество сущностей, описанных в принципах ООП и готовых к реализации в программный код.

Дополнительной задачей к предлагаемой методике можно рассматривать преобразование полученного множества сущностей в программный код на заданном ЯП [11, 14, 15], т.е. генерация программного кода на заданном ЯП.

Входными данными методики является техническое описание устройства РЗА (описание ПрО), выходными данными является программное описание ПрО (синтезированное ПО).

Решаемые методикой задачи разделяются на этапы синтеза ПО:

1) определение сущностей;

2) определение поведения сущностей;

3) определение состава сущностей;

4) определение общего поведения и общего состава сущностей ПрО, т. е. синтез сущностей, явно не описанных в ПрО — являющихся базовыми сущностями в терминологии ООП [3, 10, 11];

5) определение связей между сущностями;

6) генерация программного кода на заданном ЯП.

Оригинальность предлагаемой методики автоматизированного синтеза ПО заключается в поэтапном программном анализе ПрО. Программный анализ ПрО выявляет основные компоненты ПО: сущности, поведения сущностей, состав сущностей, общности и уникальность сущностей, связи между сущностями. Итогом выполнения анализа является набор сущностей, готовых к интеграции в единый программный код, являющийся программным описанием ПрО на заданном ЯП.

В предлагаемой методике преимуществом является то, что ПрО описывает эксперт, а реализацией алгоритмической части ПО, описанием потоков данных между сущностями, адаптацией ПО к применяемой операционной системе (абстрактный уровень взаимодействия ПО с операционной системой) занимается разработчик ПО. Экспертное описание ПрО узкопрофильным специалистом и автоматизированный синтез ПО позволят минимизировать сотрудничество разработчика ПО и эксперта ПрО, следовательно, станет возможно максимально точно описать ПрО, исключить различные трактовки ПрО разработчиком ПО, уменьшить общее время взаимодействия эксперта ПрО и разработчика ПО и сократить время на разработку ПО. Ожидаемый результат сокращения времени разработки ПО оценивается в 60%.

Оценкой правильности работы методики является сравнительный анализ ПрО и синтезированной структуры ПО. Критерии оценки соответствия описания ПрО синтезированной структуре ПО:

- синтезированная структура ПО содержит описанные в ПрО сущности;
- функционал любой сущности синтезированной структуры ПО строго соответствует функционалу сопоставляемой сущности, описанной в ПрО;
- сущности синтезированной структуры ПО не имеют функционала, не описанного в ПрО для сопоставляемой сущности;
- функционал базовых сущностей синтезированной структуры ПО соответствует функционалу, описанному в ПрО;
- базовые сущности синтезированной структуры ПО не имеют функционала, не описанного в ПрО.

Следует отметить, что количество сущностей синтезированной структуры ПО может превышать количество сущностей, описанных в ПрО, т. к. в результате решения четвёртой задачи синтезируются не описанные явно в ПрО базовые сущности.

ПРИМЕНЕНИЕ РАЗРАБОТАННОЙ МЕТОДИКИ

Рассмотрим применение предлагаемой методики синтеза ПО для терминала РЗА. Для примера рассматривается терминал РЗА фирмы ООО «ЭКРА» ЭКРА БЭ2502А0201. Терминалы этой серии предназначены для выполнения функций релейной защиты, автоматики, управления и сигнализации секционного выключателя в сетях с номинальным напряжением 6 кВ и выше [16].

В рассматриваемом примере применения методики ПрО (т. е. входными данными) для моделирования и синтеза ПО является руководство по эксплуатации (РЭ) устройств РЗА, а именно раздел с перечнем и описанием защит и функций терминала. Для упрощения процесса синтеза ПО терминала структура защит и функций терминала (предметная область) редуцируется до следующих составляющих: максимальная токовая защита (МТЗ), защита от дуговых замыканий (ЗДЗ), измерительный орган (ИО).

Ожидаемые выходные данные применения методики: программный код, описывающий ПрО.

Входные данные для методики

МТЗ. МТЗ имеет три ступени: МТЗ-1, МТЗ-2, МТЗ-3. Каждая из ступеней представляет собой совокупность нескольких измерительных органов (ИО), объединенных общей логикой. Каждый ИО МТЗ имеет независимую регулируемую уставку срабатывания и коэффициент возврата. В зависимости от выбора состояния программных накладок (табл. 1) каждая из ступеней МТЗ может быть выполнена направленной и/или иметь комбинированный пуск по напряжению. Состояния всех программных накладок имеют значения: 0 — не предусмотрено, 1 — предусмотрено.

Таблица 1

Программные накладки МТЗ

№	Наименование программной накладки
ХВ1_МТЗ	Автоматическое загрубление уставки МТЗ-1
ХВ2_МТЗ	Работа МТЗ-1
ХВ3_МТЗ	Пуск по напряжению МТЗ-1
ХВ4_МТЗ	Работа МТЗ-2
ХВ5_МТЗ	Пуск по напряжению МТЗ-2
ХВ6_МТЗ	Работа МТЗ-3
ХВ7_МТЗ	Пуск по напряжению МТЗ-3
ХВ8_МТЗ	Действие МТЗ-3 на отключение

Воздействия каждой из ступеней МТЗ могут быть назначены индивидуально с помощью матрицы отключений.

МТЗ-1 имеет особенность в виде возможности автоматического загрубления уставки на момент включения выключателя. Автоматическое загрубление уставки вводится при любых включениях выключателя при наличии соответствующего положения программной накладки.

МТЗ-2 и МТЗ-3 могут быть выполнены как с зависимыми время-токовыми характеристиками срабатывания, так и с независимыми. Перечень характеристик кривых в данной работе не существенен, поэтому характеристики не приводятся.

МТЗ-2 и МТЗ-3 имеют возможность автоматического ускорения срабатывания при включении выключателя с уставкой времени срабатывания. Ускорение ступеней МТЗ-2 и МТЗ-3 вводится автоматически при любых включениях выключателя при наличии соответствующего положения программной накладки (табл. 2).

Таблица 2

Программные накладки ускорений МТЗ-2 и МТЗ-3

Имя	Название
Ускор_МТЗ-2	Ускорение МТЗ-2
Ускор_МТЗ-3	Ускорение МТЗ-3

Срабатывание реле тока МТЗ-1, МТЗ-2, МТЗ-3 формирует сигнал «Пуск МТЗ», который может быть задействован в работе ЗДЗ. В работе ЗДЗ сигнал «Пуск МТЗ» используется для исключения излишних срабатываний защиты при срабатывании оптического датчика дуговой защиты.

ИО «РТ МТЗ-1» и «РТ Заг МТЗ-1» реализованы однотипно и имеют независимую время-токовую характеристику срабатывания.

ИО МТЗ-2 и МТЗ-3 реализованы однотипно, представляют собой орган максимального действия.

Предусмотрена возможность выбора характеристик срабатывания и возврата. Выбор типа выдержки времени на срабатывание и на возврат осуществляется уставками «Тип ВВС» и «Тип ВВВ» соответственно.

Текущее значение счётчика времени отображается в виде параметра «Q».

В состав ИО входят функциональные блоки:

- пусковые органы тока фаз A/B/C;
- максиселектор (MAX) — блок, выбирающий наибольший из трёх фазных токов;
- блок выдержки времени. Предназначен для выбора типа выдержки времени и реализации выбранной выдержки, как на срабатывание, так и на возврат.

В ИО отображаются:

- I_A/I_B/I_C — действующие значения фазных токов;
- I_max — наибольшее значение из трех фазных токов;
- Q — время, прошедшее с момента пуска, взятое по отношению к расчётному времени срабатывания.

ЗДЗ принимает внешний дискретный сигнал от устройства дуговой защиты, реагирующего на различные физические явления, сопровождающие дуговые замыкания.

Для увеличения надёжности и отстройки от ложных срабатываний применяется контроль протекания тока КЗ, данная возможность может быть выведена с помощью соответствующей программной накладки. «Контроль тока ЗДЗ» осуществляется по наличию следующих событий: пуск МТЗ ввода, наличие внешнего дискретного сигнала «Контроль тока».

ЗДЗ имеет две независимые выдержки времени на срабатывание.

ЗДЗ имеет сигнализацию о месте замыкания. Для этого используется дискретный вход «Сигнализация ЗДЗ». Для исключения ложных срабатываний цепи сигнализации в логике формирования сигнализации предусмотрена одноимённая выдержка времени на срабатывание.

Результат выполнения методики выявляет следующие сущности, их состав и связи:

- ИО-Базовый, ИО-РТ/РТ Заг МТЗ-1, ИО-МТЗ-23 (рис. 2);
- МТЗ-Базовый, МТЗ-1, МТЗ-23 (рис. 3);
- отношения МТЗ-1 и ИО-РТ/РТ Заг МТЗ-1, МТЗ-23 и ИО-МТЗ-23 (рис. 4);
- МТЗ (рис. 5);
- отношения МТЗ, МТЗ-1 и МТЗ-23 (рис. 5);
- ЗДЗ (рис. 6);
- отношения МТЗ и ЗДЗ (рис. 6).

Синтезированная основа программной модели предметной области усечённого функционала терминала РЗА состоит из 2 сущностей, представляющих функции РЗА (рис. 6):

- МТЗ — 1 экземпляр;
- ЗДЗ — 1 экземпляр.

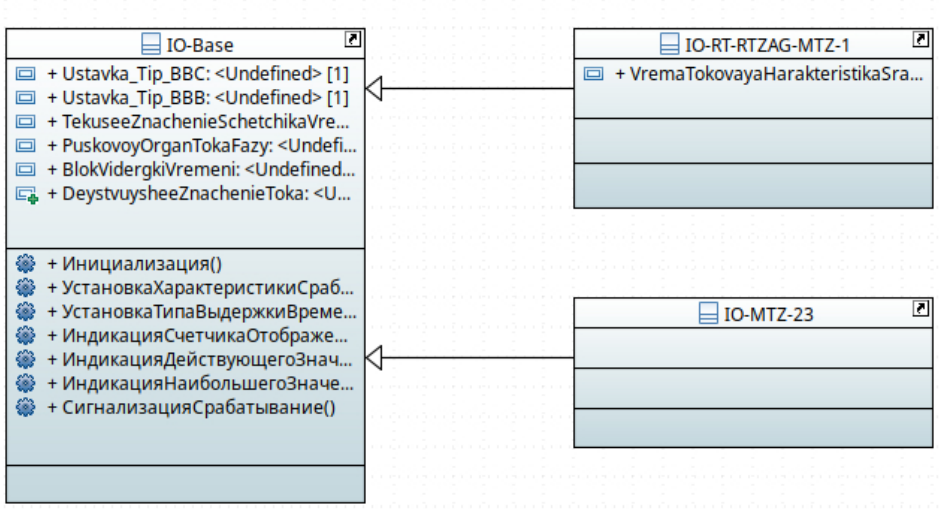


Рис. 2. Отношения ИО-Базовый и ИО-РТ/РТ Заг МТЗ-1 и ИО-МТЗ-23

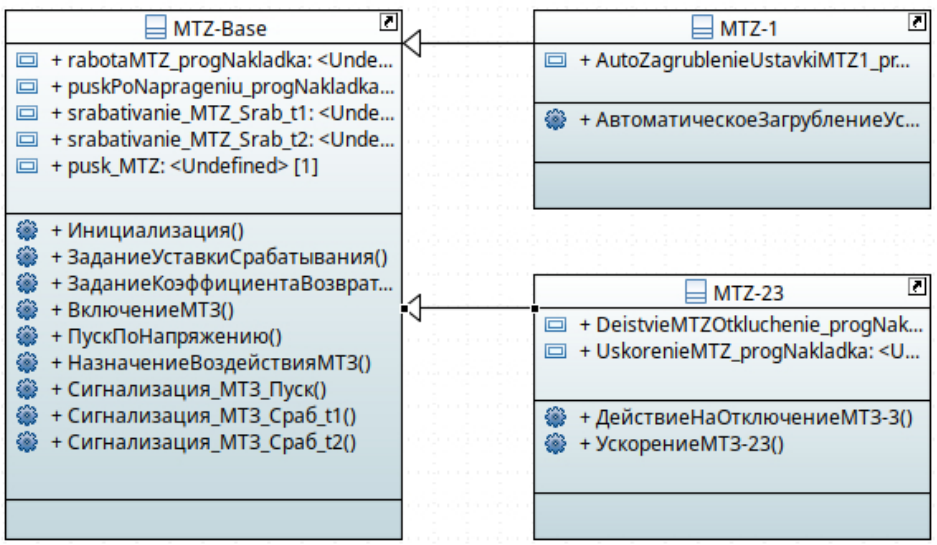


Рис. 3. Отношения МТЗ-Базовый и МТЗ-1 и МТЗ-23

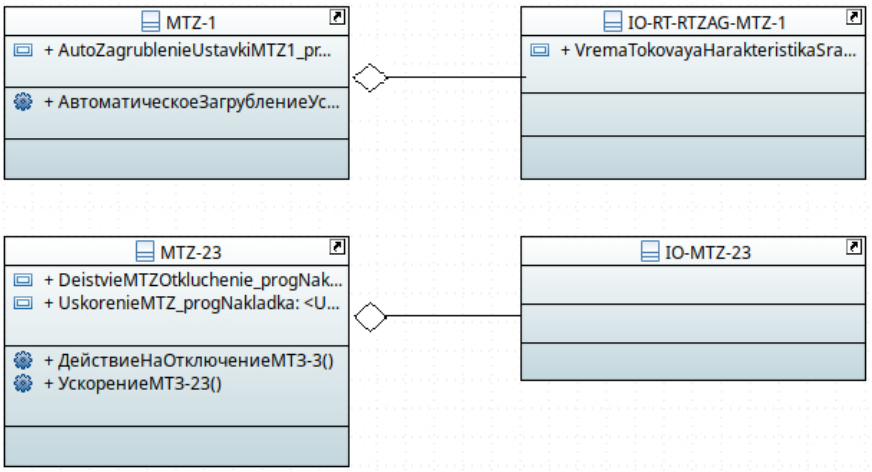


Рис. 4. Отношения МТЗ-1 и ИО-РТ/РТ Заг МТЗ-1, МТЗ-23 и ИО-МТЗ-23

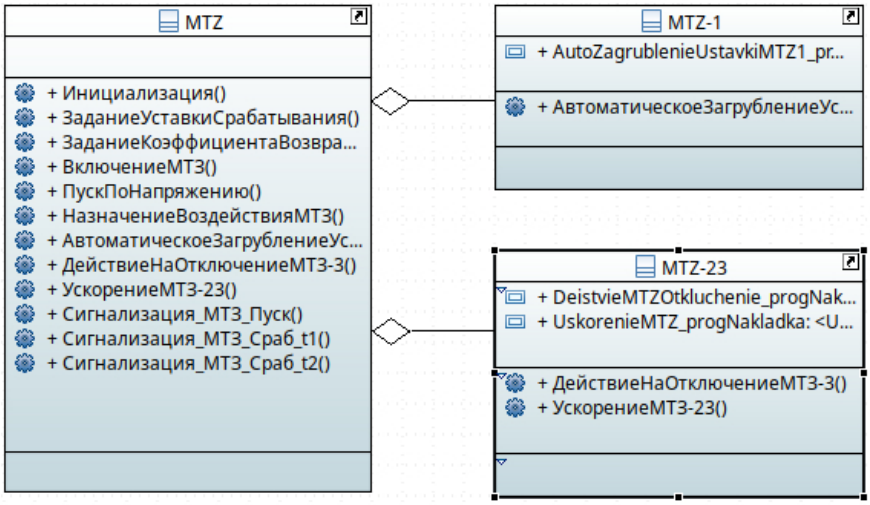


Рис. 5. Отношения МТЗ и МТЗ-1 и МТЗ-23

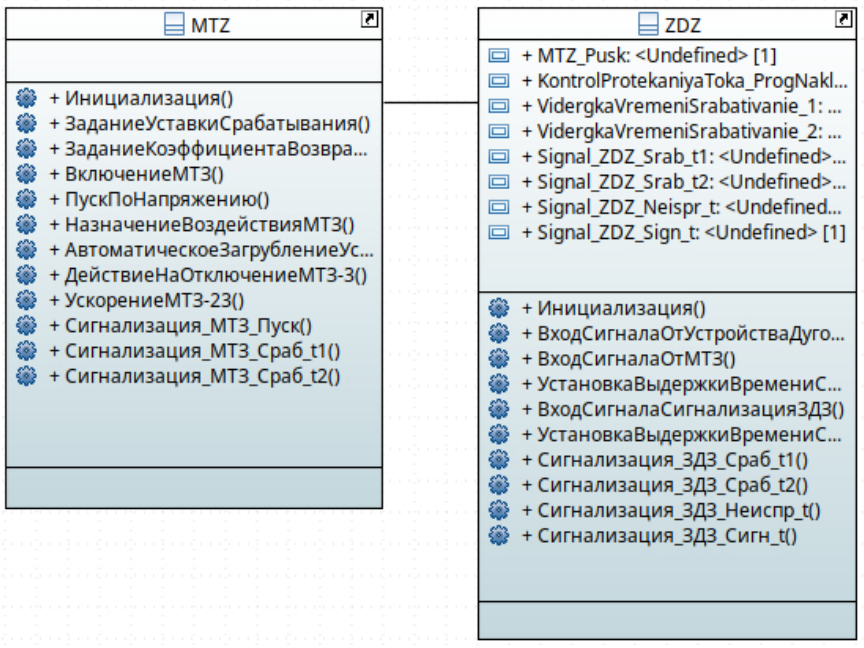


Рис. 6. Отношение МТЗ и ЗДЗ

ИНТЕРПРЕТАЦИЯ РЕЗУЛЬТАТОВ И ИХ АНАЛИЗ

Для оценки результатов применения предложенной методики автоматизированного синтеза ПО устройства РЗА как компонента ЭКС рассматривается функциональное описание устройства РЗА — ПрО. ПрО поэтапно проанализирована согласно методике, в результате анализа получены: множество программных сущностей; множество связей между сущностями; программный псевдокод, описывающий ПрО в виде объектно-ориентированной программы.

Оценка правильности работоспособности предложенной методики осуществляется в соответствии с критериями, перечисленными выше: наличие сущностей в программном коде, соответствующих ПрО; соответствие функционала ПрО, а именно, функционала её составных сущностей, синтезированным программным сущностям.

ПрО описывает сущности МТЗ, МТЗ-1, МТЗ-2, МТЗ-3, ИО-РТ/РТ Заг МТЗ-1, ИО-МТЗ-23, ЗДЗ. Все заявленные в ПрО сущности присутствуют в синтезированном программном псевдокоде. Оценка соответствия функционала сущностей ПрО и программных сущностей не выявляет отсутствия какого-либо функционала, описанного в ПрО и не описанного в программном псевдокоде.

На основании этих критериев можно сделать вывод: преобразование исходной ПрО в виде функционального описания терминала РЗА в программный псевдокод по предложенной методике соответствует ожидаемому результату. Синтезированная основа ПО терминала РЗА пригодна для дальнейшего применения в устройствах, т. к. строго соответствует описанию ПрО.

Ниже (рис. 7) представлена диаграмма затраченного времени на реализацию рассматриваемой предметной области в лабораторных условиях.

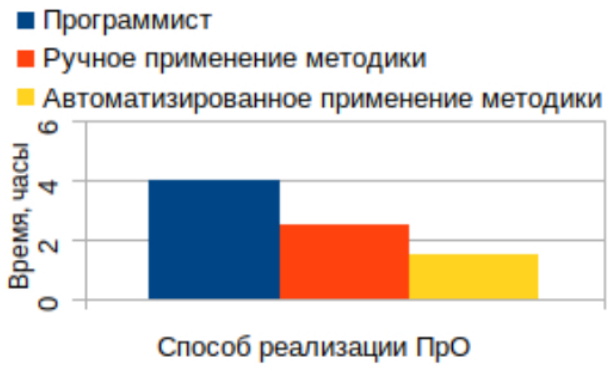


Рис. 7. Время реализации ПрО

Первый столбец (слева направо) отражает время, затраченное на реализацию программистом, второй — программистом по предложенной методике, третий — время, затраченное на автоматизированный синтез ПО по методике и последующую доработку программистом. Критерием завершённости ПО являлась возможность запуска на эмуляторе.

ЗАКЛЮЧЕНИЕ

В статье предложена методика автоматизированного синтеза ПО компонентов ЭКС по принципам ООП. Её применение позволяет преобразовывать техническое описание ПрО в ПО на заданном ЯП. Методика состоит из шести последовательных этапов анализа ПрО и синтеза элементов программных моделей сущностей.

Анализ применения предложенной методики подтвердил ее работоспособность. Полученная основа программной модели терминала РЗА в псевдокоде имеет все преимущества ПО, разработанного на основе принципов ООП.

Время, затраченное на автоматизированный синтез ПО терминала РЗА, описанного ПрО, в лабораторных условиях, измеряется в десятках секунд – существенно меньше, чем при разработке программистом «вручную». Это и является фактором значительного сокращения времени разработки ПО. Однако применение предлагаемой методики не отменяет труда программиста. Дальнейшая доработка синтезированного ПО, как было отмечено выше, заключается в настройке потоков данных между программными сущностями. На данном этапе исследования эта работа не рассматривается и оставляется на будущее. Так же, программисту необходимо реализовать алгоритмическую часть задачи, что не является целью данного исследования.

По предложенной методике синтеза ПО реализовано программное обеспечение, эмулирующее терминал РЗА. Синтезированное ПО имеет возможность запускаться на любой доступной аппаратной платформе и выполнять функции виртуального двойника устройства для применения с комплексами натурного моделирования сложных систем в реальном времени [17, 18].

СПИСОК ЛИТЕРАТУРЫ

1. СТО 56947007-25.040.30.309-2020. Корпоративный профиль МЭК 61850 ПАО «ФСК ЕЭС» [Электронный ресурс]. URL: https://www.fsk-ees.ru/upload/docs/STO_56947007-25.040.30.309-2020.pdf (дата обращения: 12.03.2024).

2. IEC 61850 edition 1. Communication networkds and systems for power utility automation. 2011. – TC 57 – Power systems management and associated information exchange [Электронный ресурс]. URL: https://webstore.iec.ch/publication/6028 (дата обращения: 12.03.2024).

3. Буч Г., Максимчук Р. А., Энгл М. У., Янг Б.Д., Коналлен Д. , Хьюстон К. А. Объектно-ориентированный анализ и проектирование с примерами приложений, 3-е изд. // Пер. с англ. – М.: – ООО «И.Д. Вильямс», 2008. – 720 с.

4. Бикмуллина И.И. Математическая модель синтеза UML диаграммы классов // Вестник технологического университета. – 2016. – Т. 19. №19. – С. 100-106.

5. Бикмуллина И.И., Барков И.А., Кирпичников А.П. Разработка информационной технологии синтеза диаграмм классов // Вестник технологического университета. – 2016. – Т. 19. №24. – С. 96-101.

6. Graphical Modelling Project. URL: [Электронный ресурс]. URL: http://www.eclipse.org/modeling/gmp (дата обращения 12.03.2024).

7. Microsoft DSL Tools [Электронный ресурс]. URL: http://msdn.microsoft.com/en-us/library/bb126259.aspx (дата обращения 12.03.2024).

8. Галанина Н.А., Петров С.В. Требования и свойства атрибутов объектных моделей, спроектированных с применением ООП // Материалы VI Международной научно-технической конференции. – Чебоксары. – 2022. – С. 51-56.

9. Антонов А.В. Системный анализ. Учеб. Для вузов. – М. – Высш. шк., 2004. – 454 с.

10. Weisfeld Matt A. The object-oriented thought process. – 3rd ed. – Printed in the United States of America, 2008. – 347 p.

11. Wiener R., Pinson L. Fundamentals of OOP and data structures in Java. Cambridge University Press. 2000. – 508 p.

12. Галанина Н.А., Петров С.В. Свойства и требования к функциям программных моделей электроэнергетических объектов, реализованных по МЭК 61850 // Информатика и вычислительная техника: сб. науч. тр. – Чуваш. Гос. Ун-т им. И.Н. Ульянова. – Чебоксары, 2023. – С. 187-194.

13. Галанина Н.А., Петров С.В. Отношения между элементами моделей электроэнергетических систем, построенных по МЭК 61850 // Сборник материалов XV Всероссийской научно-технической конференции “Динамика нелинейных дискретных электротехнических и электронных систем”.: Чебоксары.: 2023. – С. 243-246.

14. Эккел Б., Эллисон Ч. Философия C++. Практическое программирование. – СПб. – Питер, 2004. – 608 с.

15. Страуструп Б. Язык программирования C++. Четвёртое издание. – М. – Бином, 2023. – 1216. С. 51-56.

16. Руководство по эксплуатации терминала ЭКРА БЭ2502А0201 [Электронный ресурс]. URL: https://ekra.ru/product/rza-ps-6-35/t-rza/be2502a (дата обращения 12.03.2024).

17. Руководство по эксплуатации комплекса полунатурного моделирования РИТМ [Электронный ресурс]. URL: https://kpm-ritm.ru/hil (дата обращения 12.03.2024).

18. RTDS – Real Time Digital Simulator [Электронный ресурс]. URL: https://www.rtds.com, свободный (дата обращения 12.03.2024).

УДК: 004.8, 130.2, 168

О проблеме компьютерной фальсификации личности и общения

P.G. Bylevskiy, V.G. Novikov

On the Problem of Computer Falsification of Personality and Communication

Abstract. *The article is devoted to the problem of computer falsification of a personallity and communication and opens a series of publications on the possibilities of public digital services violating information security and manipulating human consciousness for the purpose of obtaining benefits. Dialectical-materialistic analysis revealed and proved that the highly productive potential of digital automation of technical means of culture is used to falsify personality, communication, creativity, values, nature and history. The factor determining the destructive direction of development and delivery of public digital services was identified. The conclusions contain recommendations for security measures both for the use of foreign services by Russian citizens and for the development of their domestic analogues.*

Keywords: *ChatGPT, artificial intelligence, computer illusionism, falsification of personality, imitation of communication, information security, dialectical materialism, technical means of culture, digital automation.*

П.Г. Былевский[1]
В.Г. Новиков[2]
[1]Кандидат философских наук, доцент ВАК 2.3.6. «Методы и системы защиты информации, информационная безопасность», доцент кафедры международной информационной безопасности Московского государственного лингвистического университета, старший преподаватель кафедры когнитивно-аналитических и нейро-прикладных технологий Российского государственного социального университета.
E-mail: pr-911@yandex.ru
[2]Член-корреспондент Российской академии наук, доктор социологических наук, доктор экономических наук, профессор, руководитель аппарата Комитета Государственной Думы Федерального Собрания Российской Федерации по защите семьи, вопросам отцовства, материнства и детства.
E-mail: v.g.novikov@bk.ru

Аннотация. *Статья посвящена проблеме компьютерной фальсификации личности и общения и открывает цикл публикаций о возможностях нарушения публичными цифровыми сервисами информационной безопасности и манипулирования сознанием человека с целью получения выгоды. Посредством диалектико-материалистического анализа выявлено и доказано, что высокопродуктивный потенциал цифровой автоматизации технических средств культуры используется для фальсификации личности, общения, творчества, ценностей, природы и истории. Установлен фактор, определяющий деструктивную направленность разработок и поставок публичных цифровых сервисов. Выводы содержат рекомендации мер безопасности как для использования российскими гражданами зарубежных сервисов, так и для разработки их отечественных аналогов.*

Ключевые слова: *ChatGPT, искусственный интеллект, компьютерный иллюзионизм, фальсификация личности, имитация общения, информационная безопасность, диалектический материализм, технические средства культуры, цифровая автоматизация.*

ВВЕДЕНИЕ

Возможности современных цифровых технологий в различных аспектах развития техники, общества и человека поражают воображение и кажутся безграничными. Неудивительно, что многие авторы впадают в «утопические/антиутопические» [1] настроения, полагая, что новые технологии либо позволят людям разом решить все проблемы, либо, напротив, помогут злоумышленникам «поработить» человечество. Обе гипотезы по-своему верны, а в какой степени, следует определить путём анализа возможностей развития и применений цифровых технологий с учётом драматической сложности современных общественных отношений.

Современные цифровые технологии следует рассматривать в качестве высшей стадии развития компьютерно-сетевых решений как технических средств человеческой деятельности. Цифровая трансформация позволяет универсально расширить автоматизацию техники на все отрасли и профессии, сферы общественной жизни и повседневную жизнь граждан.

Цифровые технологии открывают небывалые прежде возможности повышения производительности труда и расширения творческих способностей человека, но также могут быть использованы в деструктивных целях, в частности, для манипулирования сознанием, дезинформации, обмана и мошенничества, для извлечения выгоды и получения власти. Любая техника, независимо от масшта-

бов и сложности, в моральном плане нейтральна и приобретает моральную (а также правовую) окраску в зависимости от целей её создания и использования.

Взаимовыгодный или неравноправный характер цифровых сервисов определяется гармонией или же конфликтом интересов людей и организаций, участвующих в создании, производстве и предоставлении, прямом и косвенном использовании цифровых сервисов, а также балансом сил.

Переживаемая человечеством эпоха кризиса и разрушения однополярного глобализма, важнейшим инструментом которого является «цифровой неоколониализм» [2], а также нарастание «цифровой деколонизации» [3] требуют критического научного осмысления социально-политических и культурных угроз и рисков, сопутствующих в текущих условиях перспективным технологиям.

Цикл из трёх научных статей, к которому относится настоящая работа, посвящён возможностям и рискам направлений решений, причисляемых к технологиям «искусственного интеллекта», таких как мультимедийные большие генеративные модели (GenAI), частным случаем которых является сервис самообслуживания ChatGPT, и компьютерная «виртуальная реальность» как цифровой сервис. Анализ показывает, что разработки решений сопровождаются культивированием и продвижением иллюзий, способствующих консервации и укреплению недобросовестного доминирования глобальных цифровых корпораций.

В настоящей работе рассмотрены риски цифровой фальсификации человека (личности и сообществ, мировоззрения и ценностей, общения) и объективной реальности (природы и истории). Для минимизации данных рисков необходимо создание в качестве приемлемой альтернативы зарубежным цифровым сервисам самостоятельных цифровых разработок на основе приоритета национальных интересов и отечественной методологии диалектического материализма, наследующей и продолжающей лучшие традиции мировой науки и общественной мысли.

Анализ был проведён в рамках более широкого исследования, посвящённого феноменологии культуры информационной безопасности [4].

О ПРИМЕНИМОСТИ ТЕСТА ТЬЮРИНГА К ОЦЕНКЕ НОВЕЙШИХ ЦИФРОВЫХ СЕРВИСОВ

Оценка социально-политических и культурных возможностей и последствий применения компьютерно-сетевых, цифровых технологий, баланса преимуществ и рисков затрудняются в современном рыночном обществе их частым представлением в мистифицированном, иллюзорном виде.

Наглядным примером могут служить технологии зарубежного публичного интернет-сервиса ChatGPT (Chat Generative Pre-trained Transformer). Сервис разработан в США научно-исследовательской организацией OpenAI при участии корпорации Meta[1] и представляет собой электронно-вычислительный машинный «генератор», обрабатывающий имеющуюся выборку текстов согласно заданным алгоритмам посредством фрагментаций и перекомбинаций по запросу пользователя. Фактически это устройство самообслуживания, электронная библиотека с усовершенствованным поисково-справочным аппаратом.

Однако ChatGPT, согласно названию и причислению к технологиям «искусственного интеллекта», позиционируется разработчиками и поставщиками именно как «чат», наподобие сервиса для текстового общения людей. Диалектико-материалистический подход к анализу ChatGPT может выявить фальсификацию общения: диалог лишь имитируется, поскольку пользователь общается только сам с собой, используя автоматизированное техническое средство. Подобным образом разговор с самим собой совершается с использованием зеркала — простого, не автоматизированного и даже не механизированного ручного инструмента.

Дальнейший анализ показывает, что компьютерная имитация не сводится к художественной метафоре, но может быть связана с ошибочными представлениями самих разработчиков и поставщиков сервиса о её социально-культурной сущности, а также с рисками введения в заблуждение, в том числе преднамеренного, пользователей и других граждан. Учитывая базирование разработчиков и поставщиков ChatGPT в США, в настоящее время недружественных России, заслуживает исследования и правильной оценки баланс возможностей и сопутствующих рисков для российских пользователей [5] в связи с осложнением международных отношений после начала специальной военной операции на Украине в 2022 году.

В марте 2023 года были запущена новая, 4.0 версия ChatGPT, наиболее дорогостоящая, рекламируемая и продвигаемая компьютерная имитация «диалога» с пользователем, представляемая как технология «искусственного интеллекта» (уже сейчас трудно отличимого от человека, а в скором времени даже способного его превзойти).

[1]Минюст внес Meta в список экстремистских организаций за №96. См. Перечень общественных объединений и религиозных организаций, в отношении которых судом принято вступившее в законную силу решение о ликвидации или запрете деятельности по основаниям, предусмотренным Федеральным законом от 25.07.2002 № 114-ФЗ «О противодействии экстремистской деятельности» / Министерство юстиции Российской Федерации. 03.05.2024 (Электронный ресурс) URL: https://minjust.gov.ru/ru/documents/7822 (Дата обращения 20.08.2024).

Подобные декларации могут способствовать сильно завышенным оценкам возможностей ChatGPT в областях автоматизации авторского труда [6], выработки и принятия управленческих решений [7], а также как «сверхоружия» массового поражения в психологической войне [8]. Данные декларации и порождаемые ожидания следует воспринимать критически, учитывая предшествующую, начавшуюся в 1950-е годы историю нескольких циклов «вёсен и зим» «искусственного интеллекта». Под этим брендом продвигались, рекламировались и лоббировались самые разные компьютерные нововведения, осуществлялся агрессивный маркетинг в целях привлечения государственных и частных инвестиций.

Неопределённый смысл понятийно-терминологического словосочетания «искусственный интеллект» и производных обозначений способствует необоснованно преувеличенным оценкам возможностей компьютерной автоматизации и, напротив, низводит человека даже не до животного, но до механизма, неодушевлённого предмета [9]. Электронно-вычислительные машины и программное обеспечение, не являющиеся даже живыми организмами, неоправданно наделяются органическими атрибутами и даже человеческими способностями. Настойчиво внедряются и распространяются термины «компьютерная память», «компьютерное зрение», «компьютерных слух», «распознавание образов», «машинное обучение», «взаимодействие» [10] и даже «сотрудничество» компьютера с человеком [11].

Методологически, с точки зрения классической теории культуры, компьютер любой сложности не более способен к человеческим действиям, чем такая простейшая машина, как ветряная мельница, а «общение» работника с электронно-вычислительной программой столь же реально, как работника с отбойным молотком. Вид программно-аппаратной компьютерной архитектуры называется «нейросетями» [12], что, однако, означает моделирование не действительного мышления и обучения, а механистических представлений разработчиков о роли мозга и нервной системы в жизнедеятельности и действиях организма [13].

Диалектико-материалистический подход к анализу рисков безопасности российских граждан, связанных с использованием ChatGPT, позволяет провести деконструкцию (критический анализ) базового для «философии искусственного интеллекта» теста А. Тьюринга, маскирующего сущностное отличие человека от машины. Классический тест А. Тьюринга трактуется рядом разработчиков компьютерных технологий и «философами искусственного интеллекта» как средство определить «разумность» электронно-вычислительной машины. Однако критерием «прохождения» теста является мнение «экзаменатора» (неспособность отличить генерируемый машиной текст от создаваемого человеком), напоминая выпускные испытания для школы эстрадных иллюзионистов, мошенников на доверии или фальшивомонетчиков.

Вне зависимости от положительного или отрицательного характера, результаты прохождения теста Тьюринга никогда нельзя признавать окончательными. Формулировка задачи напоминает бесконечное «состязание щита и меча», в данном случае — алгоритмов генерации текстов с методиками оценки соответствия человеческой машинописи на компьютерной клавиатуре (или преобразованием речи в текст и т.д.). На деле происходит «соревнование» не человека с машиной, как может казаться, а человека-«экзаменатора» с человеком, создающим «компьютерную иллюзию», «имитацию» интеллекта (это буквальное значение термина artificial intelligence). Имитация, создание иллюзии человеческого ума с помощью любых средств, в том числе технических, может обоснованно ассоциироваться с «умничаньем», попытками (в том числе успешными) «жить чужим умом».

Сама задача «отличить человека от машины» похожа на схоластическую абстракцию, поскольку не зависит от истинности, смысла и ценности сравниваемых текстов, а сам тест проводится в искусственных лабораторных, а не в практических полевых условиях. Так, в медицинском диагнозе и рекомендованной терапии важна в первую очередь верность, и лишь потом — то, какие технические средства были использованы медицинскими работниками [14].

С непосредственно практической точки зрения причисляемый к технологиям «искусственного интеллекта» ChatGPT на деле представляет собой публичный поисково-справочный сервис самообслуживания, не являясь не только «интеллектом», но даже чатом, лишь имитируя для пользователя воображаемого «собеседника» и общение с другим человеком [15].

Пользователь не общается с кем-то, а сам находит ответы (как при внутренней беседе с самим собой или при чтении книги), только посредством текстового набора запросов и в виде выдачи результата — связной компиляции фрагментов из имеющейся библиотеки электронных документов. Выдаваемые по запросам результаты носят не субъектный социально-культурный, но исключительно

организационно-технический вещный характер [16], являясь не ответами на вопросы пользователя и не выполнением его заданий, а компиляциями выборок фрагментов согласно заданным параметрам соответствий, подобным школьной таблице умножения.

Таким образом, например, навигационными сервисами подбираются маршруты дорожного движения с учётом транспортной загруженности магистралей, а торговым автоматом изготавливается заказанный клиентом напиток.

Иллюзии «общения» способствуют названия «искусственный интеллект» и «чат», агрессивно транслируемые глобальными интернет-изданиями. Сервис ChatGPT фальсифицирует «машинное авторство» за счет отсутствия ссылок и библиографического описания использованных источников (фактически цитируемых чужих авторских текстов) и повышения «оригинальности» выдаваемого результата программными средствами, используемыми для преодоления сервисов автоматизированного выявления плагиата. Замаскированные компиляции фрагментов чужих текстов выдаются за творения некоего компьютерного «я», чьи «голос» и «изображение» может имитировать сервис.

Не искусственно-игровой, а имеющий практический смысл тест «генеративных» компьютерных технологий, по сути — автоматизированных справочно-поисковых сервисов, должен определить возможности и ценность их применения. В мировой культуре есть целая галерея иронично-сатирических примеров бессмысленности и практической бесполезности попыток наделения машины «интеллектом»: от машины комбинирования книг из слов у Дж. Свифта, созданной академиками-прожектёрами летающего острова Лапута, до компьютерного генератора стихов, «электрибальда Трурля» Ст. Лема.

Первые компьютерные компиляторы текстов по запросам из имеющихся в электронных библиотеках, создававшиеся в 1990-е российскими разработчиками, назывались «бредогенераторами», учитывая, что суть бреда не в неправдоподобии, а в неистинности. Вместе с тем даже не успешная компьютерная иллюзия мышления, а сам тезис о возможности «искусственного интеллекта» может быть практически успешно использован. История культуры богата подобными примерами: так, во времена Древней Греции наркотический бред жриц-пифий храма Аполлона в Дельфах успешно выдавался за божественные пророчества искусными толкователями «скрытых глубоких смыслов».

АВТОМАТИЗИРОВАННЫЕ ТЕХНИЧЕСКИЕ СРЕДСТВА КУЛЬТУРЫ В ПАРАДИГМЕ МЕХАНИЦИЗМА

ChatGPT — это не социально-культурный субъект, а программно-аппаратный комплекс, автоматизированное техническое средство интеллектуального труда человека-пользователя, то есть объект; это не только неодушевлённый, но и неживой предмет. ChatGPT является автоматизированным электронно-вычислительным сервисом для создания пользователем текстов на основе имеющейся электронной библиотеки. В России это относится к компьютерной автоматизации социально-культурной деятельности, одной из «сквозных» технологий, условно обозначаемых как «искусственный интеллект» [17] в рамках цифровой трансформации, начавшейся с середины 2010-х гг. [18].

Согласно классической теории культуры и диалектико-материалистической методологии, единственным субъектом социально-культурной деятельности может быть только человек и сообщества людей. Такой подход к человеку, подчёркивающий его сущностное отличие от природных, биологических и технических средств производства, соответствует как трудовой теории стоимости, разработанной классиками английской политической экономии А.Смитом и Д.Рикардо, так и определению современной юриспруденцией субъектами права только людей и их организаций.

Так же разделяются как объекты налогообложения люди (налоги на доходы и прибыль, страховые взносы и т.п.) и имущество (в т.ч. производственное, включая компьютерные системы, телекоммуникации и цифровые сервисы). По-разному учитываются в создании новой стоимости (ценности) «роли» труда живого и прошлого — вещных факторов производства: сырья и заготовок, амортизации основных фондов, оборудования и орудий труда.

Иллюзии «самостоятельности» могут быть тем сильнее, чем техника более масштабна по размерам, чем выше автоматизация и степень пространственно-временной автономии от операторов, в том числе дистанционных, то есть чем менее наглядна и очевидна связь функционирования и результатов с усилиями человека.

Подобную кажущуюся самостоятельность от земледельческого труда являет сезонный сельскохозяйственный урожай, являющийся следствием «естественного плодородия». Однако при любых «техногенных» авариях и несчастных случаях расследование выявляет людей, ответственных за на-

несение ущерба другим, виновных в нарушениях правил технической безопасности. В ходе расследования правонарушений и преступлений, совершённых с использованием технических средств любой сложности, автоматизации и автономности, выявляются роль, участие и степень вины каждого фигуранта.

Никакая сложность, автономность, функциональность и любые другие технические характеристики, ни степень «человекоподобия» класса ChatGPT и выше не даёт оснований признать субъектами права и, соответственно, «виновниками» инцидентов, аварий и правонарушений компьютерное оборудование, программного обеспечение, телекоммуникации и цифровые сервисы.

Человек преобразует природу и самого себя с помощью средств производства, предметов и процессов, относящихся к технике. Поэтому первичны и приоритетны человек и его социально-культурные способности, включая интеллект, по отношению к которым любые технические средства, независимо от степени сложности и автономности, носят вторичный, подчинённый, инструментальный характер.

Таким образом, техника включает созданные людьми неживые предметы и используемые процессы, применяемые для совместной деятельности, направленной на расширенное воспроизводство самих себя, условий своей жизнедеятельности, общественных отношений и социальной среды. Если к техническим средствам социально-культурной деятельности на разных исторических этапах относились, например, каменный топор, кисти, печатные машины, то к XX-му — началу XXI-го века появилось радио и телевидение, современные компьютерные сети и цифровые сервисы [19], включая ChatGPT.

Ценность применения любого технического средства труда определяется повышением производительности труда пользователя, в сравнении с ручными операциями или совершаемыми с использованием других инструментов. Здесь важно соотношение затрат на разработку и поддержание сервиса с экономией рабочего времени, достигаемой при производстве продукта благодаря его использованию. ChatGPT, как и другие компьютерные «генеративные» модели, является техническим средством труда, «посредником» между создателями, поставщиками сервиса, пользователем, аудиторией генерируемых с его помощью текстов и другими людьми.

Как и любой другой инструмент, ручной или стационарный, простой или автоматизированный, в зависимости от характера использования ChatGPT может представлять собой преимущество или угрозу. В условиях несовпадения, конфликта и противоборства интересов преимущества одних людей могут в то же самое время выступать угрозами для других. Это верно и в отношении инструментов любой сложности и степени автоматизации (включая технологии, причисляемые к «искусственному интеллекту» [20]), хотя относительные автономность и автоматизм способны порождать иллюзии полной независимости от людей.

Философско-методологической предпосылкой «очеловечивания» и даже «обожествления», наделения сверхъестественными способностями техники, в том числе электронно-вычислительной, служит механистическое мировоззрение, сформированное в Новое время, в частности, в трудах И. Ньютона и Р.Декарта, и составляющее опору позитивизма XIX века и его последующих модификаций.

В основе «философии искусственного интеллекта» лежит не «традиционный» классический теоретико-культурный подход (в частности, представленный в диалектическом материализме), рассматривающий общество и личность как субъекты исторического социально-культурного развития, осуществляемого в системном взаимодействии.

В механистическом мировоззрении объективный мир (природа, общество и человек) — лишь механизмы разной степени сложности, способные только к инерционному движению, но не к самодвижению и саморазвитию. Философия деизма предполагает создателя и законодателя этого мира — демиурга, «бога-механика», придавшего ему «первотолчок».

Для деизма и механистического подхода жизнь — не единая органичная целостность, подразделяющаяся на роды, виды, популяции и отдельные организмы, а история — не естественно-исторический процесс развития общества и человека. Для механициста природа, общество и человек — всего лишь многоуровневая система машин и механизмов, которую можно понять и как угодно улучшить с помощью законов механики, математики, формальной логики и техники (в наши дни — посредством электронно-вычислительного и автоматизированного электромеханического оборудования).

Человека можно рассматривать как техническое устройство только в рамках соответствующих общественных отношений, приравнивающих по крайней мере часть людей к неодушевлённым, неживым предметам. Именно такой объяснимый, редуцированный, предельно упрощённый, но ошибочный методологический подход к природе в целом, жизни, обществу и человеку как к техническим устройствам обусловливает нереалистично

завышенные прогнозы преимуществ компьютерной автоматизации, а также сопутствующих угроз и рисков. Общество и человек легко упрощаются до формальных абстракций, схем, механических, электромеханических, компьютерных, цифровых моделей, когда рассматриваются с точки зрения математических вычислений, механики и электротехники, а также других смежных научно-технических или механистически-формализованных гуманитарных дисциплин.

Приравнивание человека (части людей) к неодушевлённому предмету — инструменту, механизму, машине (как и к рабочему скоту) вполне соответствует рабовладению («говорящие орудия труда») и иным историческим человеческим отношениям (антигуманным и бесчеловечным с современной точки зрения).

Такой подход, неверный с точки зрения классической теории культуры и методологии диалектического материализма, тем не менее, может отвечать интересам одних, влиятельных социальных групп, а также воздействовать на сознание и поведение других, убеждая в реальной жизни уподобляться неодушевлённым инструментам. Таким образом, «философия искусственного интеллекта» может эффективно использоваться для введения в заблуждение, обмана, мошенничества, недобросовестной конкуренции и эксплуатации, включая привлечение финансирования и инвестиций для новых компьютерных разработок.

ВОЗМОЖНОСТИ ФАЛЬСИФИКАЦИИ ЛИЧНОСТИ И ОБЩЕНИЯ ПОСРЕДСТВОМ СЕРВИСА CHAT GPT

Диспропорционально гипертрофированное представление о сущности новых компьютерных технологий и основанных на них автоматизированных решений можно оценивать как одновременно и ненаучно-утопическое, и антиутопическое. Таким образом, возрастают риски неверного определения применений генеративных «больших языковых моделей», прогнозирования и ранжирования сопутствующих угроз и, соответственно, снижается эффективность разработки средств обеспечения информационной безопасности.

Позиционирование генераторов текстов в качестве «сверхоружия» для ведения психологических войн выглядит лишь гипотетическим; в то время как уже намного более реальны и реализуются в разнообразных инцидентах риски трансграничной утечки конфиденциальных данных или публикации сгенерированных с использованием ChatGPT сведений, нарушающих российское законодательство, в том числе заведомо ложных.

Схема сервиса ChatGPT напоминает уже привычные поисковые сервисы в публичных интернет-ресурсах Яндекс, Google и др., которые по запросу пользователя автоматически выдают, по степени убывания соответствия, адреса расположения электронных документов. С помощью этих поисковых сервисов пользователь находит в публичном интернете созданные другими людьми (авторами) источники, формально наилучшим образом соответствующие сделанному запросу.

При этом пользователь, как правило, видит более или менее понятное, подробное и правдивое библиографическое описание отыскиваемых источников: URL, название сайта и документа, дату и время публикации, «сведения об ответственности» автора, публикатора и др.

Сервис ChatGPT работает таким же образом, как и поисковые сервисы, но с некоторыми существенными отличиями.

Сходство заключается в принципиальной схеме устройства сервиса, состоящего из трёх основных элементов.

Первый элемент — «библиотека», структурированная база документов, размеченных и индексированных (упорядоченных) по определённым формализованным параметрам. Содержание публичного интернета, наполнение документами определяется его участниками — владельцами, редакторами и авторами сайтов и других ресурсов, интерактивными действиями пользовательской аудитории, регулируясь государственными органами и коммерческими организациями. Состав документов «библиотеки», используемой ChatGPT, формируется, то есть отбирается и структурируется хозяевами, разработчиками и поставщиками сервиса, главным образом компанией OpenAI (США).

Второй элемент, определяющий работу поискового сервиса, — это настройки параметров формального соответствия содержания документа, его фрагментов запросу пользователя. Эти настройки (выдаваемые за «машинное обучение») автоматизированно определяются согласно критериям, устанавливаемыми разработчиками, неизбежно выражая их мировоззрение, интересы и соответствуя законодательству страны их базирования.

Разработчики формируют политики и правила определения «наилучшего соответствия документа запросу пользователя», критерии «языка ненависти» и проводимой цензуры [21], руководствуясь собственной выгодой, мировоззрением и ценно-

стями, в обязательном порядке учитывая интересы инвесторов, «групп влияния» и государства, законодательство страны своего базирования. У компании OpenAI, разработчика и поставщика сервиса ChatGPT, среди крупнейших инвесторов и партнёров — глобальная цифровая корпорация Microsoft, тоже базирующаяся в США.

Отличие списков документов и сайтов, «выдаваемых» поисковыми сервисами разных стран как «наилучшим образом соответствующих запросу пользователя», становится особенно наглядным во времена ухудшения и обострения международных отношений. Причисление ChatGPT к «искусственному интеллекту», имитация «нечеловеческой», «объективной» «компьютерной» личности маскирует корпоративную и государственную принадлежность владельцев сервиса, их существенные интересы, которые могут не совпадать и конфликтовать с потребностями российских граждан.

Третий элемент ChatGPT, отсутствующий в поисковых сервисах в публичном интернете, — это имитационная надстройка. Кроме имитации «компьютерного я» и «чата»-диалога, это алгоритмы, которые компилируют выборку фрагментов чужих документов в подобие связного текста с учётом правил и стилистики «естественного языка», устраняют ссылки и другие признаки использования чужих авторских документов. В сервисе нет встроенных инструментов проверки сведений («факт-чекинга»), подтверждения официальными, авторитетными, достоверными источниками [22]. Пользователям гарантируется правдоподобность, высокое качество иллюзии достоверности, но не истинность, не смысловые достоинства выдаваемого текста.

Как типографское оборудование используется для изготовления высококачественных поддельных денежных купюр, так использование ChatGPT может быть эффективным для автоматизированного создания «фейк-новостей», фальсификации истории [23], публикаций в политически ангажированной «жёлтой прессе», «вирусного» распространения в социальных сетях и каналах, имитации массовых пользовательских оценок и реплик.

Выдаваемые по запросам и «заданиям» пользователей тексты не являются «ответами», поскольку они не «придуманы» и не «написаны». Их можно назвать сгенерированными, но не машиной, а пользователем при помощи машины. Перед нами некоторая техническая, но в ещё большей степени иллюзорная надстройка, маскирующая машину «ширма».

Выдаваемые от имени некоего «компьютерного я» тексты представляют собой мозаику, компиляцию избранных фрагментов чужих авторских текстов, формально наиболее соответствующих запросу и отражающую интересы владельцев, создателей и поставщиков сервиса ChatGPT. Хозяева сервиса скрыты ширмой «чата» и «компьютерного я», а авторы и другие существенные обстоятельства создания используемых источников — отсутствием ссылок на них и специальной маскировкой — автоматизированной обработкой «коллажа», скрывающей использование источников.

Риски фальсификации авторства при создании текста с недекларированным использованием ChatGPT [24] следует признать надуманными, не более высокими, чем при публикации под псевдонимом или от имени «поддельной личности». Современные определения доказуемого плагиата сводятся не к смысловому содержанию, а к формальному отсутствию или низкой «оригинальности», доказанным значительными совпадениям с ранее опубликованными текстами. Исходные авторские тексты из «библиотеки» ChatGPT автоматически обрабатываются, уничтожая и маскируя признаки чужого авторства, достигая формальной оригинальности по отношению к публикациям, уже находящимся в открытом доступе.

Главная роль в создании текста с использованием ChatGPT исполняется автором, а сервис выступает в роли хоть и автоматизированного, но всё же только технического средства культуры, как гусиное перо с чернилами и бумагой вместе с библиотекой изданий, в которых удалены библиографические сведения об авторстве и публикаторе (издателе), месте и времени издания. Ответственность за формулировку запроса, проверку и оценку качества выданного текста, за указание или не указание факта использования ChatGPT и, главное – за публикацию, полностью ложится на автора и публикатора [25], даже если они действуют анонимно. Гонорар за такую публикацию и слава по праву принадлежат им, равно как, при нарушении закона, именно они подлежат ответственности вплоть до уголовной [26].

Возможности фальсификации общения с помощью сетевых компьютерных технологий, цифровых сервисов типа ChatGPT следует относить к современным угрозам информационной безопасности российских граждан. На основании двусмысленного «теста Тьюринга», причисления к технологиям «искусственного интеллекта» и приравнивания к «чату», посредством ChatGPT создаётся имитация «компьютерного я» и «машинного творчества». «Общение» с фальсифицированной «компьютерной личностью» оказывается фальсифицированным общением, управлением сознанием пользователя анонимными манипуляторами.

Иллюзия «компьютерного правдоподобия» выдаваемых текстов провоцирует некритическое доверие без проверки на достоверность и соответствие национальному законодательству, маскирует авторство и другие существенные факторы используемых источников, подлинные мотивы создателей и поставщиков сервиса, возможно, противоречащие интересам пользователей.

Однако отсутствие в текстах, выдаваемых ChatGPT по запросам, ссылок на авторитетные достоверные источники и встроенных инструментов проверки достоверности способно в достаточно короткие сроки обесценить преимущества этой компьютерной имитации авторства. Поэтому следует признать лишь гипотетическими и сильно завышенными риски использования ChatGPT в качестве «сверхоружия», сильно удешевляющего психологическую войну, а также возможной причиной массовой безработицы создателей текстов и публикаций, фальсификаций авторства.

Перечисленные риски можно считать иллюзорными, отвлекающими внимание от реальных деструктивных применений ChatGPT в инцидентах информационной безопасности, например, в случаях маскировки злоумышленниками вредоносных кодов в программном обеспечении [27] и при утечках конфиденциальных данных, неосторожно вводимых пользователями в этот частный трансграничный сервис [28].

ЗАКЛЮЧЕНИЕ

Для минимизации рисков ChatGPT требуются критическое преодоление с помощью классической материалистической философской методологии иллюзий «искусственного интеллекта» и формирование правильного понимания роли технических средств в творчестве, а также в деструктивном воздействии и манипулировании сознанием. Необходима специальная маркировка интерфейса ChatGPT, его аналогов и выдаваемых по запросам текстов, подобная обязательному указанию возрастных ограничений и упоминанию лиц, признанных иностранными агентами и организаций, запрещённых в России.

Пользователи должны сознательно принимать риски ответственности, вплоть до уголовной, за публикацию недостоверных сведений, нарушающих российское законодательство. Для этого и необходимо уведомление, что ChatGPT — это не «искусственный интеллект», а автоматизированный электронный справочно-поисковый библиотечный сервис самообслуживания, созданный и базирующийся в США. При невыполнении указанных требований могут быть предприняты дополнительные государственные меры ограничения и блокировки доступа к ChatGPT на территории России и в российском сегменте интернета.

Отечественным разработчикам и поставщикам сервисов рекомендуется уходить от некритического копирования импортной методологии разработок ChatGPT и аналогов, в частности, интерфейса, имитирующего поддельную компьютерную личность и общение с ней. Такая концептуальная зависимость может квалифицироваться как трансляция на российских граждан мировоззрения и антироссийских ценностных установок недружественных стран, запрещённых в Российской Федерации организаций.

Выдаваемые по запросам пользователей «сгенерированные» тексты должны в обязательном порядке содержать ссылки на использованные источники с библиографическим описанием по ГОСТ[2], причем запрещённый контент должен отсутствовать или должен быть снабжен соответствующими пометками. Также отечественные «генеративные» сервисы следует маркировать предупреждением, что ответственность за использование и его возможные негативные последствия полностью ложится на пользователя. Уклонение от выполнения рекомендаций могут рассматриваться Федеральной антимонопольной службой как недостоверная реклама и сопровождаться санкциями к нарушителям, предусмотренными российским законодательствам.

СПИСОК ЛИТЕРАТУРЫ

1. Евграфова О.В., Королев В.К. Философия цифровой экономики: идеология, утопия, антиутопия? // Философия хозяйства. 2021. № 5(137). С.29-41. EDN: MXNBBT.

2. Сурма И.В. Государственный суверенитет vs политики цифрового и технологического неоколониализма // Вопросы политологии. 2022. Т.12. № 1(87). С. 3799-3805. DOI:10.35775/PSI.2022.87.11.019. EDN: UMWEHR.

[2]ГОСТ Р 7.0.100-2018. Система стандартов по информации, библиотечному и издательскому делу. Библиографическая запись. Библиографическое описание. Общие требования и правила составления. Дата введения 01.07.2019. 73 с. / Консорциум «Кодекс». Электронный фонд правовых и нормативно-технических документов. URL: https://docs.cntd.ru/document/1200161674 (Дата обращения 20.08.2024).

3. Грибанова В.В., Хохолькова Н.Е. Актуальные проблемы исследования колониализма, неоколониализма и деколонизации // Азия и Африка сегодня. 2024. № 2. С.64-67. DOI: 10.31857/S032150750030075-4. EDN: FSBTNW.
4. Былевский П.Г. Феноменология культуры информационной безопасности М.: Московский государственный лингвистический университет, 2024. 240 с. EDN: WNDOJS.
5. Булычев И.И., Казаков В.Г., Кирюшин А.Н. Будущее искусственного интеллекта: скептики vs прагматики // Военный академический журнал. 2023. №2 (38). С.10-21. EDN: FJVPRO.
6. Agathokleous E., Saitanis C., Fang Ch., Yu Zh. Use of Chat-GPT: What does it mean for biology and environmental science? // Science of The Total Environment. 2023. Vol.888. DOI: 10.1016/j.scitotenv.2023.164154.
7. Миронова Н.Г. Философское осмысление социальных рисков интеллектуальной автоматизации социального управления // Цифровой ученый: лаборатория философа. 2021. Т.4. №2. С.125-144. DOI: 10.32326/2618-9267-2021-4-2-125-144.
8. Гончаров В.С. Применение комбинированных технологий искусственного интеллекта в информационно-психологических войнах // Вопросы политологии. 2022. Т. 12. №4(80). С.1118-1126. DOI: 10.35775/PSI.2022.80.4.015.
9. Груздев А.А., Самарин А.С., Илларионов Г.А. Проекты цифровой философии в контексте развития digital humanities // Журнал Сибирского федерального университета. Серия: Гуманитарные науки. 2023. Т.16. №7. С.1165-1176. EDN: GBBFUA.
10. Есенин Р.А. Психологические вызовы цифровой реальности: искусственный интеллект сегодня и в перспективе // Профессиональное образование и рынок труда. 2023. Т.11. №2(53). С.121-128. DOI: 10.52944/PORT.2023.53.2.009.
11. Kreps S., Jakesch M. Can AI communication tools increase legislative responsiveness and trust in democratic institutions? // Government Information Quarterly. 2023. Vol.40. Iss.3. DOI: 10.1016/j. giq.2023.101829.
12. Плотникова А.М. Нейросеть как ключевое слово текущего момента // Филологический класс. 2023. Т.28. №2. С.45-54. EDN: TBIHHU.
13. Guile D. Machine learning — A new kind of cultural tool? A "recontextualisation" perspective on machine learning + interprofessional learning // Learning, Culture and Social Interaction. 2023. Vol.42. DOI: 10.1016/j.lcsi.2023.100738.
14. Liu J., Zheng J., Cai X., Wu D., Yin Ch. A descriptive study based on the comparison of ChatGPT and evidence-based neurosurgeons // iScience. 2023. DOI: 10.1016/j.isci.2023.107590.
15. Short C., Short J. The artificially intelligent entrepreneur: ChatGPT, prompt engineering, and entrepreneurial rhetoric creation // Journal of Business Venturing Insights. 2023. Vol.19. DOI: 10.1016/j. jbvi.2023.e00388.
16. Володенков С.В., Федорченко С.Н. Особенности феномена субъектности в условиях современных технологических трансформаций // Полис. Политические исследования. 2022. №5. С.40-55. DOI: 10.17976/jpps/2022.05.04.
17. Gill S., Kaur R. ChatGPT: Vision and challenges // Internet of Things and Cyber-Physical Systems. 2023. Vol.3. Pp.262-271. DOI: 10.1016/j.iotcps.2023.05.004.
18. Сойфер В.А. Human factor // Онтология проектирования. 2021. Т.11. №1(39). С.8-19. DOI: 10.18287/2223-9537-2021-111-8-19.
19. Миловидов С.В. Художественные особенности произведений компьютерного искусства, созданных с использованием технологий машинного обучения // Артикульт. 2022. №4(48). С.36-48. DOI: 10.28995/2227-6165-2022-4-36-48.
20. Брянцева О.В., Брянцев И.И. Проблема субъектности искусственного интеллекта в системе общественных отношений // Вестник Поволжского института управления. 2023. Т.23. №3. С.37-50. DOI: 10.22394/1682-2358-2023-3-37-50.
21. Cohen S., Presil D., Katz O., Arbili O., Messica S. Rokach L. Enhancing social network hate detection using back translation and GPT-3 augmentations during training and test-time // Information Fusion. 2023. Vol.99. DOI: 10.1016/j.inffus.2023.101887.
22. Currie G. Academic integrity and artificial intelligence: is ChatGPT hype, hero or heresy? // Seminars in Nuclear Medicine. 2023. Vol.53. Iss.5. Pp.719-730. DOI: 10.1053/j.semnuclmed.2023.04.008
23. Канштайнер В. Цифровой допинг для историков: можно ли сделать историю, память и историческую теорию искусственным интеллектом? // KANT: Social Sciences & Humanities. 2023. №1(13). С.56-70. DOI: 10.24923/2305-8757.2023-13.5.

24. Elliott Casal J., Kessler M. Can linguists distinguish between ChatGPT/AI and human writing? A study of research ethics and academic publishing // Research Methods in Applied Linguistics. 2023. Vol.2. 3. DOI: 10.1016/j.rmal.2023.100068.
25. Kahambing J. ChatGPT, 'polypsychic' artificial intelligence, and psychiatry in museums // Asian Journal of Psychiatry. 2023. Vol.83. DOI: 10.1016/j.ajp.2023.103548.
26. Зорин А.Р. К вопросу правового регулирования ChatGPT // International Law Journal. 2023. Т.6. №6. С.35-38. EDN: UOEZHV.
27. Филюков Д.А. Применение нейронных сетей для формирования кода вредоносного программного обеспечения // Инновации и инвестиции. 2023. №7. С.199-204. EDN: ZBHRXM.
28. Anderson S. "Places to stand": Multiple metaphors for framing ChatGPT's corpus // Computers and Composition. 2023. Vol.68. DOI: 10.1016/j.compcom.2023.102778.

УДК: 004.42

Современные подходы к разработке мобильных приложений

A.K. Marinin

Modern Approaches to Mobile Application Development

Abstract. *To organize the process of developing high-quality mobile applications, it is necessary to understand the order, stages and complexity of each process included in the overall development process, correctly handle advanced development methods and technologies. One of the key modern technologies is the development of mobile applications that demonstrate high performance on different mobile platforms. This paper describes the feasibility and features of the integrated use of the Flutter framework and the Dart programming language for developing cross-platform applications. The technical capabilities of development, most fully represented in the functions of the Flutter framework and the Dart programming language, are considered. The use of this method in the development of mobile applications, taking into account the capabilities of running the application on different operating systems, can contribute to the creation and launch of applications that can meet the needs of users.*

Keywords: *mobile application, mobile development, framework, mobile operating system, Flutter, Dart, cross-platform application.*

А.К. Маринин
Инженер-программист
E-mail: aleksei.marinin247@gmail.com

Аннотация. *Для организации процесса разработки мобильных приложений высокого качества необходимо понимать порядок, стадии и сложность каждого процесса, входящего в общий процесс разработки, корректно обращаться с передовыми методами и технологиями разработки. Одной из ключевых современных технологий является разработка мобильных приложений, демонстрирующих высокую производительность на разных мобильных платформах. В настоящей работе описана целесообразность и особенности комплексного применения фреймворка Flutter и языка программирования Dart для разработки кроссплатформенных приложений. Рассмотрены технические возможности разработки, наиболее полно представленные в функциях фреймворка Flutter и языка программирования Dart. Применение данного метода в разработке мобильных приложений с учетом возможностей запуска приложения в разных операционных системах может способствовать созданию и выводу на рынок приложений, способных соответствовать потребностям пользователей.*

Ключевые слова: *мобильное приложение, мобильная разработка, фреймворк, мобильная операционная система, Flutter, Dart, кроссплатформенное приложение.*

ВВЕДЕНИЕ

С появлением мобильных устройств современный человек кардинально изменил свой образ жизни. Мировая статистика показывает, что смартфоны доступны каждому второму жителю планеты. Торговая компания GSMA информирует о ситуации с пользованием смартфонами на конец 2023 г.: почти 55% населения или 4,3 млрд. человек имеют собственный мобильный телефон [1]. Выпуск мобильных гаджетов также не прекращает роста, а к 2025 г. по аналитическим прогнозам ожидается, что их число составит 18,22 млрд. устройств [2].

Использование смартфонов и планшетов привлекает пользователей тем, что не теряется связь с деловыми партнерами или родственниками в любом формате цифрового общения, а данные можно обработать почти также, как и персональном компьютере. Пользовательские задачи при этом выполняются, как правило, в мобильных приложениях.

Мобильные приложения представляют собой вид программного обеспечения, разработчики которого ориентировались на расширение функций мобильных устройств – смартфонов или планшетов. С мобильным приложением пользователь обладает доступом не только к информации, но и к различным внешним цифровым сервисам. Цели использования мобильных приложений неравнозначны – это может быть процесс неформальной или формальной коммуникации, банковские переводы, государственные услуги, покупки в онлайн магазинах и на маркетплейсах и др.[3]

Записки и напоминания нашли применение для составления списков покупок, интерес к любым объектам, людям, событиям удовлетворяет доступная с устройства информация, приложения подсчитывают калорийность пищи или физическую нагрузку, выполняют прочие важные функции. С мобильными приложениями рутинные задачи отнимают меньше времени, разрешаются успешно и эффективно [4].

Процесс разработки мобильных приложений упорядочен и формализован таким образом, чтобы создавать приложения под их оптимальное скачивание, установку и использование на мобильных устройствах. Разработчик не только формирует программное обеспечение (ПО) под определенную операционную среду (ОС) (самые распространенные — Android и iOS), но и тестирует приложение, чтобы оптимизировать и поднять его производительность до максимума на избранной аппаратной платформе, сделать интерфейс удобным. В динамике развития мобильной разработки в последние годы просматривается опережение прочих направлений информационных технологий.

Актуальность исследования состоит в том, что для разработки мобильного приложения высокого качества важно понимать порядок, стадии и сложность каждого процесса, а также принципы грамотного обращения с передовыми методами и технологиями. Одной из таких технологий сегодня является разработка мобильных приложений, которые могут работать с высокой производительностью на разных мобильных платформах (кроссплатформенность) [5].

Необходимость поиска и применения возможностей для разработки кроссплатформенных приложений, определяется стремительным и интенсивным развитием в сфере разработки мобильных приложений, активно используемых во многих видах бизнеса. Рыночное предложение не ограничено в вариантах ОС на мобильных устройствах, но потребители смартфонов стабильно выбирают такие мобильные операционные системы как Android и iOS [6] (см. таблицу 1).

Таблица 1

Доля рынка мобильных операционных систем по всему миру по состоянию на декабрь 2023 г.

№	Операционная система	Доля, %
1	Android	70,48
2	iOS	28,8
3	Samsung	0,37
4	KaiOS	0,14
5	Windows	0,02
6	Linux	0,01

Следовательно, для разработчиков мобильных приложений приоритетными ОС являются Android и iOS, что объясняется высоким спросом потребителей и обширным предложением на рынке устройств с этими мобильными операционными системами (порядка 98,56%). Понимание современных методов в разработке мобильных приложений с учетом возможностей запуска приложения на разных ОС является главным условием вывода на рынок востребованных приложений. Технические возможности сегодня, как одна из актуальных тенденций в мобильной разработке, представлены в функциях фреймворка Flutter и языка программирования Dart.

Цель исследования, представленного в настоящей работе – обосновать решение компилировать с фреймворком[1] Flutter язык программирования Dart в деятельности разработчика кросс-платформенных приложений, осветив указанную тенденцию как наиболее распространенную при разработке мобильных приложений.

Объектами исследования являются фреймворк Flutter и язык программирования Dart в качестве эффективного сочетания инструментов для кроссплатформенной разработки мобильных приложений.

В ходе исследования использованы общенаучные методы, включая анализ, синтез и обобщение информации из литературных и статистических источников, методы описания, сопоставления, аналогий, а также графический метод.

РЕЗУЛЬТАТЫ И ИХ ОБСУЖДЕНИЕ

Фреймворк Flutter имеет кросс-платформенную природу, а его кодовая база выполнена целостно и согласовано под язык программирования Dart. К 2018 г. запуск данного фреймворка провела компания Google, и он получил оценку как совокупность инструментов в очень комфортном наборе, удобном для работы с анимацией, а также привлекательных благодаря качеству всех слагаемых в пользовательском интерфейсе. Продукты Google короткий период выпускаются в формате кросс-платформ, но Flutter достиг мягкого движения в анимации, не критикуется за неудобство компонентов интерфейса [7].

[1]Фреймворк — это набор правил, шаблонов и инструментов, которые используются для построения продуктов или процессов в программировании и других областях. Фреймворки помогают:

- упорядочить и стандартизировать процессы;
- облегчить командную работу;
- повысить эффективность достижения целей.

Они предлагают готовые решения и методики, которые можно адаптировать и применять в различных проектах и областях деятельности. Фреймворки вначале возникли в сфере программирования, но затем расширили своё применение и вышли за его пределы.

Фреймворк является комплексным решением, а к приложению Software Development Kit (SDK) разработчики ввели современные дополнения — виджеты и инструменты. Разработка получила весьма высокую оценку за простоту и хорошую производительность. В этой среде мобильное приложение создается визуально броским и интересным, способным запускаться под ОС iOS, Android, с выходом в Web, на языке единой кодовой базы [8].

Использовать Flutter могут разработчики, освоившие на практике такие концепции программирования, как:

– концепция программирования с объектно-ориентированным подходом (классы, методы, переменные);

– концепция программирования с императивным подходом (циклы, условия).

Пакеты Flutter как экосистема подготовлены к широкой поддержке, начиная от камеры или сети, до GPS и хранилища. Кроме названных аппаратных средств поддерживаются многие услуги — банкинг, облако, аутентификация, реклама [9].

Мобильные приложения в среде Flutter разрабатываются без запроса к браузеру или виджетам, которые входят в пакет поставки на устройстве пользователя.

Весьма ценным считается отсутствие у Flutter прочих слоев кода C/C++, кроме тонкого. Система Flutter практически вся (от композиции и жестов с анимацией до фреймворка и виджетов) опирается на язык Dart, в среде которого легко произвести изменения в процессе разработки. Dart является языком современным, сжатым и объектно-ориентированным и востребован в кругах разработчиков как способ полного контроля проекта .

Команда создателей фреймфорка старается ежеквартально обновлять его версии, поскольку и стабильность, и производительность в свете растущих требований нуждаются в постоянном повышении [9].

Структура Flutter исполнена таким образом:

– с учетом разработки приложений для мобильных устройств присутствует оптимизированный движок 2D-рендеринга (полноценная поддержка текста);

– передовая версия фреймворка React;

– виджеты в наборе под разработку материального дизайна и стиля iOS;

– API под разные виды тестов — модульные и интеграционные;

– API двух типов – и взаимодействующие, и подключаемые, кроме системы, к сторонним SDK;

– Dart DevTools как инструмент тестов, незаменимое средство при отладке и профилировании;

– командная строка с пакетом средств, в разработке мобильных приложений обеспечивающих все операции – создание и сборку, тесты и сочетание [10].

Flutter создан как фреймворк, поддерживающий Android Studio и Visual Studio Code, а также другие, менее известные инструменты. В этой среде мобильное приложение можно разрабатывать, используя режим командной строки. Отладка с инструментом Dart DevTools отличается возросшей гибкостью. Блок виджет-инспектора выводит структуру и иерархию каталога, на чем основана визуализация интерфейса.

Среда фреймворка собрала несколько языков разработки – здесь можно программировать на C, C++, Dart и Skia (2D-движок рендеринга). Особенностью виджетов называют включение в любой вариант приложений Flutter, опцию тематизации виджетов, сближающую их облик с родными компонентами User interface UI Android (Material) или iOS (Cupertino). Здесь Skia является холстом, на котором отображается виждет, доступна широкая по возможностям анимация, с распознавания жестов (рис. 1).

Самыми важными в платформе Flutter технологиями являются:

– Skia — среда для рендеринга с 2D-графической библиотекой;

– язык Dart VM под конкретную платформу.

Вне зависимости от оболочки исполняется API платформы, запускается процесс обработки событий, заложенных в жизненном цикле мобильного приложения [11].

С языком Dart фрейворк Flutter не имеет проблем с тем, чтобы на опережение компилировать код, исходный к собственному. Движок C/C++ для компиляции кода требует или Android NDK (Native Development Kit), или iOS LLVM (Low Level Virtual Machine).

Оба компонента принадлежат одному проекту — Runner Android и iOS, использование которого формирует нужный файл: apk- или ipa-. Запущенное приложение работает таким образом: вне зависимости от вида и типа рендеринга, ввода, события таковое поступает на компилированный движок Flutter и обращается в приложении к его коду. Фреймворк обязательно пакуется в apk- или ipa-формате, из-за чего снизить приложения менее 4 MB не удается.

Рис. 1. Системная архитектура фреймворка

Мобильное приложение не теряет скорости при запуске или исполнении. Пользователи работают в интерфейсе, обновляемом на 60 fps (обеспечено GPU (Graphics Processing Unit — от англ. графический процессор)), а экран содержит только пиксели холста Skia. Такие инструменты образуют безупречный пользовательский интерфейс.

Виртуальная машина нашла применение для компиляции в промежуточный код. Так, Virtual Machine (VM) является эффективным интерпретатором, способным эмулировать в среде программного обеспечения имеющееся аппаратное обеспечение. Использовать в разработке виртуальную машину актуально, чтобы с минимальными усилиями портировать язык, если возник запрос освоить новую аппаратную платформу. Обычно языком ввода данных в VM может оказаться промежуточный код. Так, если язык программирования Java использован для написания кода, то с компиляций код будет промежуточным (байт-кодом Java), после чего виртуальная машина (JVM) обеспечит его исполнение.

Язык Dart принадлежит к группе объектно-ориентированных. Мобильное приложение с кодом Dart содержит только объекты. Язык Dart не предусмотрен для поддержки наследования в множественном режиме, а производный класс в качестве родителя всегда имеет один базовый, но не более. Программирование на языке Java или C# происходит так, что множество интерфейсов вполне эффективно исполняются одним классом. В синтаксисе Dart близок к языкам семейства C (C++, C#, Java, Kotlin).

Нулевая безопасность является преимуществом Dart, так как стратегия null safety[2] предупреждает null-ошибки, причем самые трудно идентифицируемые.

Среди прочих языков Dart обеспечивает однопоточное программирование, а такое ограничение является слабым местом. Код может быть асинхронным, но создать класс Thread принципиально невозможно. Отсутствие данного класса заместили концептом Isolate, несхожим с обычными потоками неспособностью разделить общую память, но пересылающим сообщения для взаимодействия [12].

В языке Dart управление пакетами происходит на базе собственного инструмента — pub, запускающего установку любого пакета из хранилища. К pub можно прямо не обращаться, поскольку менеджер пакетов реагирует на код, где прописана зависимость пакета от стадии проекта как условие установки.

Исполнение и компиляция в Dart инструментами обеспечивается с поддержкой функций, ценных фреймворку Flutter и обязательно комбинируемых:

– разработка в формате «быстрого цикла» с базовыми принципами JIT (Just-in-Time), чтобы переменить форму, сделать горячую перезагрузку, но сохранить состояние конкретного языка и его типов;

– генерацией AOT-компилятора создается код ARM, чтобы происходил быстрый запуск, не снижалась производительность в развертке [13].

Как средства, JIT-компиляторы (Just-in-Time) отвечают по функциям своей аббревиатуре и компилируют «точно в нужное время». Эти инструменты поддерживают компиляцию уже запущенного приложения, что сказывается на сокращении сроков цикла разработки. Однако нередко компилятор заставляет программу тормозиться в исполнении. Запуск приложения с JIT-компилятором длительный, так как не только исполняется, но и анализируется и компилируется.

[2]Null Safety в Dart — это функция, которая позволяет переменным не содержать нулевых значений по умолчанию. Она снижает риск возникновения ошибок во время выполнения и делает код безошибочным. Null Safety была добавлена в Dart 2.12.

В противоположность им, AOT-компиляторы (англ. аббр. от Ahead-of-Time) относятся к инструментам с заблаговременным действием, что приводит к повышению длительности цикла разработки. Мобильное приложение начнет исполняться только после компиляции, которая и создает исполняемый файл. Для разработчика значение AOT-компиляции состоит в том, что продукт предсказуем в исполнении и анализ не сопровождается перерывами исполнения, что справедливо и для компиляции. [13].

Строго зависит от режима разработки горячая перезагрузка (Hot Reload), так как функция совместима исключительно с debug-режимом. Исполнение Hot Reload происходит, когда вслед за обновлением исходного кода его файл вводится в Dart VM, запущенную ранее. При этом множатся классы, а также поля и методы имеющихся классов, обновляются функции. Функция Hot Reload с изменением кода вынесет сущность этих перемен в файл, передаст запущенному эмулятору или устройству, если таковое подключено [14].

Характер виджета точнее всего описать объектной природой. Код формирует виджеты, а редакция кода заставляет эти объекты пересоздаваться. Из единственного виджета StatelessWidget генерируется бесчисленное количество BuildContexts, поскольку множеством описаний характеризуется позиция виджета в дереве таковых. Функции StatefulWidget позволяют сопроводить новым объектом State очередной BuildContext (рис. 2) [15].

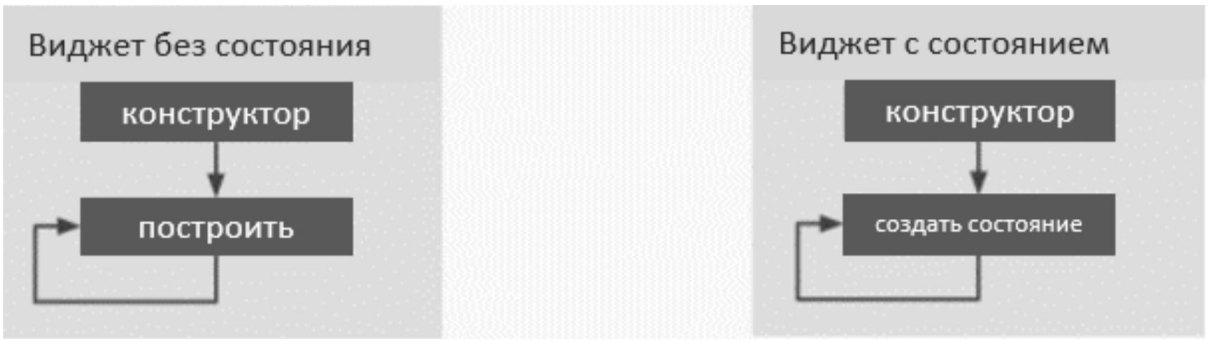


Рис. 2. Жизненный цикл виджета

Разработка нуждается в сборке мусора, чтобы процесс программирования автоматически реализовал эффективную форму управления памятью. Задачи сборщика мусора особые. Процесс запускается периодически, чтобы стереть из памяти объекты, неактуальные для приложений, увеличить объем свободной памяти.

Язык Dart освобождает память современным решением сборки мусора: использовать принцип поколения объектов. Процесс отводит нужный объем памяти, которой могут пользоваться только объекты с кратким жизненным циклом. Решение отлично удовлетворяет потребности реактивных пользовательских интерфейсов, включая Flutter, так как изменений в дереве виджетов не происходит, но процесс пересборки запускается с окончанием кадра и перед демонстрацией следующего.

Данный формат сборщика вносит в язык Flutter особый комфорт в разработке с уклоном на декларативный стиль пользовательского интерфейса. Объект создается на базе конструктора, что упрощает написание верстки. За виджетами замечено свойство легковесности, а их данные являются эскизом, основой к отрисовке. Но отрисовать виджет должен самостоятельный слой.

Использование кросс-платформенных фреймворков поясняется тем, что нужен инструмент обмена: данные кодовой базы нужно отправлять на целевые платформы, и наоборот. Мобильные приложения еще не располагают прочими иными фреймворками, где бы оказались доступными и пользовательский интерфейс, и его код.

Визуализировать пользовательский интерфейс Flutter можно, не запрашивая его компонентов, конкретных для той или иной платформ, но он обязательно шлет запрос, чтобы отобразить пользовательский интерфейс, к холсту. Эта среда поддерживает рисование (рис. 3).

Рис. 3. Пользовательский интерфейс приложения

Бизнес-логика открыта к совместному использованию с пользовательским интерфейсом в фреймворке Flutter, с чем разработка становится сжатой в сроках, понятной, высокоточной, но данные производительности конечного продукта остаются неизменными.

Затраты на мобильное приложение методом нативной разработки на порядок выше. Причина в том, что создается код приложения под каждую платформу, отдельно прописываются функции. К разработке нативных приложений нужно привлечь достаточное количество специалистов, что формирует затраты на поиск кадров и оплату труда.

Команды Surf сообщили, что фреймворк Flutter обеспечивает экономию по ряду направлений создания мобильного приложения:

1)-45,6% от вложений в разработку;

2) -70,5% от затрат в секторе тестирования (но необходимо обеспечить автотесты[3]);

3)-33,3% за привлечение дизайнера мобильных разработок.

Но приведённые данные об экономии ситуативные, а бюджет может снизиться в целом на 15-50%. Это доказывает выгоды Flutter в осуществлении задач по разработке [15].

Разработка и поддержка нативных приложений нуждаются в значительных суммах инвестиций, поскольку разработчики изучают конкретную платформу, подстраивая в процессе адаптации все компоненты мобильного приложения – от бизнес-логики и интерфейса до макета. Этот фактор повышает привлекательность низкобюджетных фреймворков, поясняет выход Flutter в линейку популярных инструментов, порой опережающих нативные технологии в способности удовлетворить высокотехнологичный бизнес.

Фреймворк Flutter импонирует разработчикам тем, что пишется единственный код, хотя платформ несколько, что резко снижает сроки разработки и ее стоимость. Владение Flutter приходит к разработчикам быстро, поэтому команда не должна состоять только из профессионалов с опытом работы в данном фреймворке. Но мобильное приложение по нативной технологии создается записями двух кодов, запуск из которых произойдет на своей платформе — Android или iOS. Такое условие увеличивает затраты времени.

Экспертное сообщество оценивает оперативность разработки Flutter в более сжатые сроки в сравнении с нативным продуктами: порядка -20% и даже -50% времени работ. Но фактор скорости сопряжен с интерфейсом и функциями – их сложностью, емкостью набора. Фреймворк увлекает разработчиков функцией Hot Reload тем, что она дает возможность мгновенно отслеживать с запуском сделанное изменение и выйти из текущего состояния разработки. Таким образом многократно ускоряется разработка приложений в среде Flutter [16].

Фреймворк не нуждается в длительных тестированиях, так как автоматизированные тесты менее востребованы, их объем ниже на 50% против нативных технологий. При этом пишется код тестов, одинаково запускаемый на любой платформе, что поясняет более низкое качество теста – падение QA (Quality Assurance — обеспечение качества).

Разработка в среде фреймворка Flutter мобильного приложения может происходить ровно вдвое быстрее в отличие от продуктов конкретно под Android и iOS. Это обстоятельство поясняется тем, что код пишется под обе платформы. Фреймворк является средой, где двухмерный пользовательский интерфейс создается только на базе Flutter, не нуждающегося во взаимодействии с каким-либо приложением по нативной технологии [17].

Flutter не повторяет закономерность многих кроссплатформенных фреймворков, запрашивающих промежуточные представления, интерпретирующие код. Мобильное приложение Flutter и машинный код интегрированы самым тесным образом, что снижает значимость ошибок производительности интерпретируемого кода.

Flutter обращается к Skia Graphics Library, чтобы оперативно перенастраивать пользовательский интерфейс – с каждым изменением вида. Приложение исполняется графическим процессором, что поясняет плавность пользовательского интерфейса Flutter и высокую частоту вывода кадров - 60 fps (кадров/с). Возможности фреймворка эффективно расширены декларативным API, что в генерации пользовательского интерфейса является фактором прорыва в производительности. Этот момент явно заметен на стадии оценки визуальных настроек [18].

Разработчики заявляют о том, что предпочитают фреймворк Flutter, так как он предполагает настройку любого объекта экрана. Гибкости пользовательского интерфейса можно достичь в отдельной разработке и на самостоятельной платформе, но с вложением грандиозных усилий по сравнению с Flutter.

В мобильных приложениях спрос существует не только на пользовательский интерфейс, но и на

[3]Автотесты — это тесты, которые выполняет компьютер, а не тестировщик-человек. Внутри автотест это тоже программа, цель которой — протестировать, как работает другая программа.

определенные функции ОС, такие как оценка пребывания по координатной сетке в GPS, коммуникации через Bluetooth-устройства, подключение к датчикам для сбора данных, подтверждение разрешений, создание и применение учетных данных. Приложение с разработкой на Flutter может расширить свою функциональность за счет перечисленных функций, так как в фреймворке существует доступ к плагину (поддержку предлагает Google). Но мобильное приложение может создаваться, если функция заложена в ОС, но плагином не поддерживается. Проблему Flutter разрешает просто, предлагая установить коммуникацию Dart и кода платформы, использовав каналы последней (рис. 4).

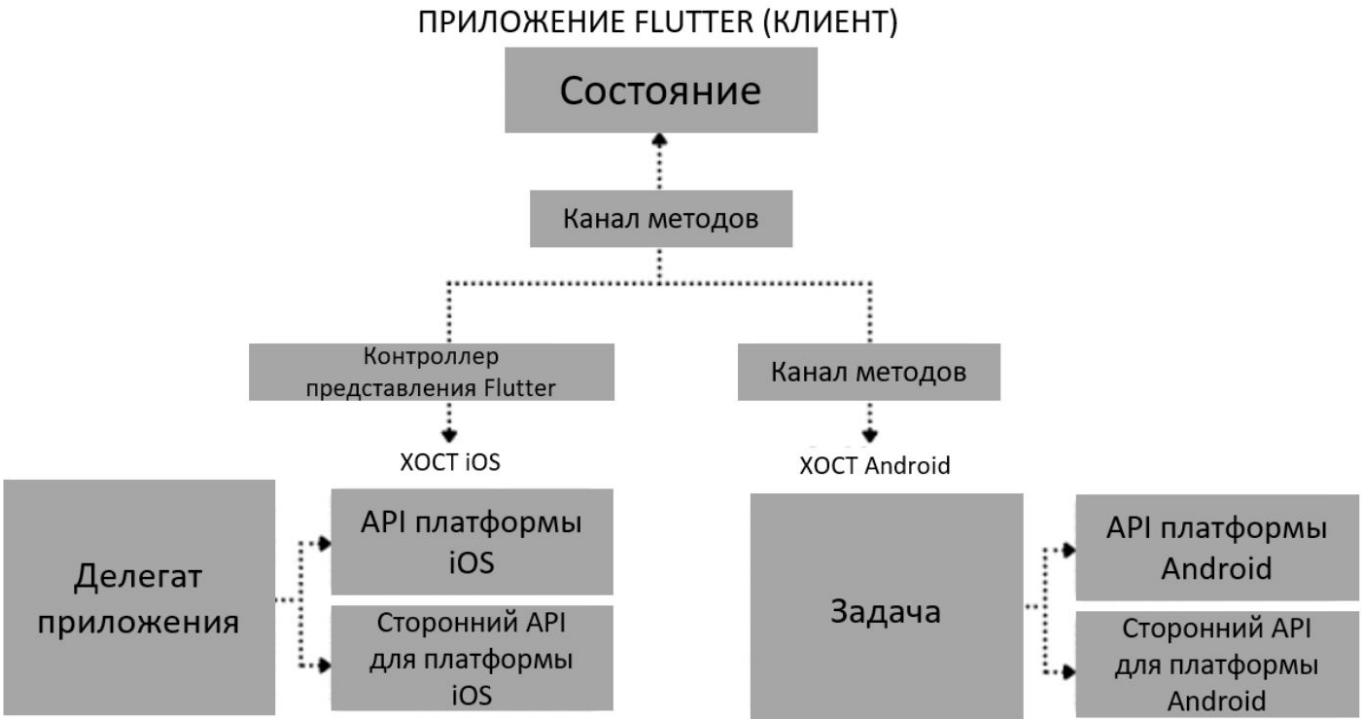


Рис. 4. Пример функционирования каналов

Пользовательские виджеты в фреймворке оформлены набором, а исходный код запускает процесс их визуального представления и позволяет ими управлять. Пользовательский интерфейс по компонентам не имеет сходства с нативными приложениями. Мобильное приложение Flutter в ракурсе пользовательского интерфейса обладает веским преимуществом, позволяющим ему обойти возможности React Native. В Flutter градации настройки виджетов в плане деталей высокие, что выводит фреймворк в лидеры по экономии времени на настройку визуального представления. Основные виджеты в компоновке Flutter не являются единственными, так как виджеты Material и Cupertino представлены пространными наборами, что позволяет подстроиться под особенности поведения того или иного языка дизайна (рис. 5). [19]

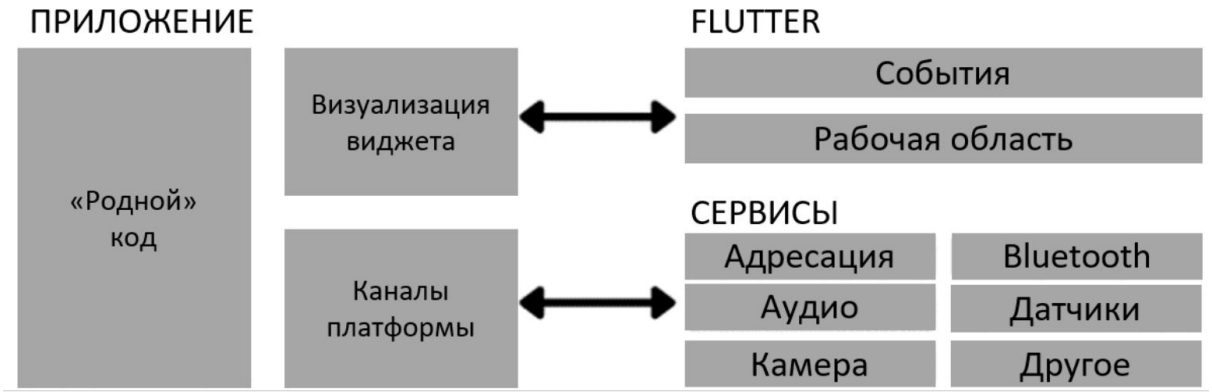


Рис. 5. Рендер виджетов

Наряду с описанными выше достоинствами фреймворк имеет следующие недостатки:

1) В плане сообщества разработчиков Flutter уступает React Native, где разработка может быть выполнена специалистами с большим опытом работы, устоявшимися взглядами на возможности мобильных приложений.

2) Новизна Flutter сказывается на емкости библиотек и поддержке данного фреймворка. Даже участие Google не решает проблему отсутствия в библиотеке текущих версий Flutter той или иной функции, а искомую возможность разработчик будет вынужден создавать сам, расширяя доступные в Flutter пользовательские функции. При этом сроки сдачи проекта возрастают [20].

3) Flutter увеличивает размер мобильного приложения, причем даже выше показателей нативных. Создатели Flutter осознают данную проблему и стремятся вывести его в разряд инструментов, создающих мобильные приложения среднего и малого размера.

ЗАКЛЮЧЕНИЕ

Разработка мобильных приложений – процесс многогранный и сложный, требующий знания множества аспектов, от выбора правильной платформы до внедрения передовых методов тестирования и обеспечения безопасности. Современные подходы к разработке мобильных приложений претерпевают изменения столь же быстрые, как и сами технологии, на которых они основаны. Из этого следует, что главной задачей остается создание удобных, функциональных и безопасных приложений, способных удовлетворить потребности пользователей и превзойти их ожидания.

Комплексное применение фреймворка Flutter и языка программирования Dart является обоснованным выбором для разработки кроссплатформенных приложений. Их использование позволяет сократить затраты на разработку, повысить производительность приложений и обеспечить плавный и единообразный пользовательский интерфейс на различных устройствах. Flutter и Dart предоставляют удобный и эффективный инструмент для решения современных задач мобильной разработки, что делает их важнейшими компонентами арсенала любого разработчика.

Прогнозируя дальнейшее развитие, можно ожидать, что фреймворк Flutter и язык Dart будут лишь укреплять свои позиции. Компании, стремящиеся минимизировать затраты на разработку и сократить время выхода на рынок, все чаще будут обращать внимание на кроссплатформенные решения, и Flutter в этом процессе займет одну из ведущих ролей. Дальнейшие улучшения производительности, расширение функционала и активное развитие экосистемы приложений — все это создаст условия для массового перехода разработчиков и компаний на использование данной технологии.

СПИСОК ЛИТЕРАТУРЫ

1. GSMA: 4.3 billion people now own smartphones [Электронный ресурс] URL: https://www.gsmarena.com/gsma_more_than_half_of_the_world_owns_smartphones-news-60214.php (дата обращения: 25.03.2024).

2. Forecast number of mobile devices worldwide from 2020 to 2025 (in billions) [Электронный ресурс] URL: https://www.statista.com/statistics/245501/multiple-mobile-device-ownership-worldwide/ (дата обращения: 25.03.2024).

3. Sarker I. H. et al. Mobile data science and intelligent apps: concepts, AI-based modeling and research directions // Mobile Networks and Applications. 2021. V. 26. №. 1. P. 285-303.

4. Хисаметдинова С.Ф. Особенности разработки мобильных приложений // Научно-технический прогресс как механизм развития современного общества. 2022. P. 73-75.

5. Zohud T., Zein S. Cross-platform mobile app development in industry: A multiple case-study // International Journal of Computing. 2021. V. 20. №. 1. P. 46-54.

6. Mobile Operating System Market Share Worldwide [Электронный ресурс] URL: https://gs.statcounter.com/os-market-share/mobile/worldwide/2023 (дата обращения: 25.03.2024).

7. Jatnika A. A. D., Akbar M. A., Pinandito A. Comparative Analysis of the Use of State Management in E-commerce Marketplace Applications Using the Flutter Framework // Journal of Information Technology and Computer Science. 2023. M. 8. №. 2. P. 111-124.

8. Nawrocki P. et al. A comparison of native and cross-platform frameworks for mobile applications // Computer. 2021. V. 54. №. 3. P. 18-27.

9. Windmill, E. Flutter in Action. — Shelter Island (NY): Manning Publications, 2020. 368 p.

10. Payne R. Beginning app development with Flutter : create cross-platform mobile apps. New York, Ny: Apress, 2019. 334 p.
11. Zaccagnino C. Programming Flutter. Pragmatic Bookshelf. 2020. 370 p.
12. Hassan A. M. JAVA and DART programming languages: Conceptual comparison // Indonesian Journal of Electrical Engineering and Computer Science. 2020. V. 17. №. 2. P. 845-849.
13. Biessek, A. Flutter for Beginners: An introductory guide to building cross-platform mobile applications with Flutter and Dart 2. — Birmingham: Packt Publishing, 2019. 512 p.
14. Johnson E., Wang G. Flutter Framework Mobile Application Development of Gamified Automotive Reseller Team Management // Journal Info Sains: Informatika dan Sains. – 2023. V. 13. №. 03. P. 1125-1131.
15. Алеев А. Быстрый старт Flutter-разработчика: Пошаговое пособие разработчика кросс-платформенных приложений / Издательские решения, 2020. 108 с.
16. Разработка мобильных приложений для Android и iOS // Surf. [Электронный ресурс] URL: http://surf.ru (дата обращения 25.03.2024).
17. Mainkar P. Google Flutter Mobile Development Quick Start Guide: Get up and running with iOS and Android mobile app development // Birmingham: Packt Publishing, 2019. 152 p.
18. Oliveira W. et al. Analyzing the Resource Usage Overhead of Mobile App Development Frameworks // Proceedings of the 27th International Conference on Evaluation and Assessment in Software Engineering. 2023. P. 152-161.
19. Napoli M. L. Beginning Flutter: A Hands on Guide to App Development // Indianapolis (IN): Wrox (John Wiley & Sons), 2020. 528 p.
20. Zammetti F. Practical Flutter: Improve your Mobile Development with Google's Latest Open-Source SDK // New York: Apress Media, 2019. 414 p.

УДК:140.8

Основные подходы к созданию информационно-технологической среды обитания нового общества

A.V. Uryadov

Basic Approaches to Creating an Information Technology Environment for the New Society

Abstract. *The article formulates the main approaches to the creation of an information and technological environment for the new society. Understanding the features and necessity of applying these approaches will help prepare society to solve many current and potential global problems. The problem of anthropocentric perception of the world is formulated and directions of human development are proposed that can expand cognitive capabilities and organize more efficient operation of social systems. The feasibility of applying the vitacentric approach is substantiated.*

Keywords: *social physics, anthropocentrism, information and technological environment, artificial consciousness, union of intelligences, bios, vitacentrism.*

А.В. Урядов
Преподаватель кафедры когнитивно-аналитических и нейро-прикладных технологий, Российский государственный социальный университет.
E-mail: intellectual.artemka@gmail.com

Аннотация. *В статье сформулированы основные подходы к созданию информационно-технологической среды обитания нового общества. Понимание особенностей и необходимости применения данных подходов позволит подготовить общество к решению многих актуальных и потенциальных глобальных проблем. Сформулирована проблема антропоцентричного восприятия мира и предложены направления развития человечества, способные расширить познавательные возможности и организовать более эффективную работу социальных систем. Обоснована целесообразность применения витацентрического подхода.*

Ключевые слова: *социальная физика, антропоцентризм, информационно-технологическая среда, искусственное сознание, союз интеллектов, биос, витацентризм.*

ВВЕДЕНИЕ

В современном мире практически во всех областях социальной жизни и общественного производства можно наблюдать, что социумы в целом слабо осознают важность того глобального перехода, в котором находится человечество. Двадцатый и начало двадцать первого века оказали значительное влияние на человеческую цивилизацию во всех её проявлениях. Экспоненциальное ускорение развития науки и техники меняют общество быстрее, чем человечество успевает предвосхищать будущее даже в научной фантастике. Последствия и проявления этой проблемы до конца не осмыслены, но вызывают все больший научный интерес.

Информационное поле, в котором живет человек, основано на получении информации через органы чувств и последующем построении логических и интуитивных выводов при помощи абстрактно-аналитического мышления. Как удачно написал В.И. Ленин: «От живого созерцания к абстрактному мышлению и *от него к практике* – таков диалектический путь познания *истины*, познания объективной реальности» [1].

Человек всегда существовал в информационной среде, в условиях развития коммуникативных (в широком смысле) концепций и стратегий, как внутри общества, так и с внешнем миром. Коммуникация позволяет получать и транслировать информацию об устройстве внешнего мира, природы и общества, а также ценности и смыслы для человеческого общества, что в итоге оказывает существенное влияние на формирование среды обитания человека.

Задачами данной статьи являются выявление тенденций и возможных перспектив развития человека в антропоцентричной парадигме мышления, формулирование проблемы антропоцентричного восприятия мира, анализ перспектив сотворчества человека и альтернативного интеллекта, определение базовых принципов создания среды для наиболее эффективного долгосрочного развития человека и биосферы, способной отвечать на новые вызовы.

Изучению указанных выше вопросов были посвящены исследования, относящиеся к достаточно обширному периоду времени. Укажем некоторые наиболее значимые работы.

В труде «Основные направления философии техники. К истории возникновения культуры с новой

точки зрения» [2] Э. Капп подчёркивал, что человек в технике бессознательно воспроизводит самого себя. Труды философа положили начало новому направлению «философии техники», в рамках которой далее были высказаны идеи сакрализации и демонизации техники и технологического производства (в промышленности, массовой культуре и политике).

Д. Хаксли в своей работе «Религия без откровения» [3] приходит к выводу, что человек способен выйти за биологические рамки с помощью развития технологий, и предлагает назвать это направление «трансгуманизмом».

В совместной работе «Искусственное сознание: техническое задание в философской и естественно-научной парадигме» [4] описаны различные подходы к созданию сильного искусственного интеллекта и искусственного сознания.

Концепция нового, глобального общества, основанного на принципах разума, представлена в работах В.И. Вернадского «Биосфера и ноосфера» [5].

Среди основных методов исследований в области мировоззренческих подходов к созданию информационно-технологической среды обитания нового общества выделим системный и диалектический подход, а также такие общенаучные методы, как анализ и синтез.

В качестве исходных положений приведём следующие тезисы:

- антропоцентричная парадигма должна быть пересмотрена для создания устойчивых партнёрских отношений со всеми элементами биосферы и альтернативами человеческому интеллекту;

- новое мировоззрение должно быть основано на витацентризме, который учитывает системное понимание жизни в контексте биосферы;

- использование преимуществ различных биологических систем и потенциального сильного искусственного интеллекта может увеличить жизнеспособность и эффективность биосферы, помогая ей подготовиться к будущим вызовам;

- создание новых связей между людьми и в пределах биосферы способствует формированию новых характеристик на основе законов диалектической логики;

- быстрое развитие технологий и науки требует от человека расширения мировоззрения и готовности к решению таких проблем, как массовое вымирание, глобальные конфликты, нехватка ресурсов, теория эгоистичных цивилизаций и ограниченность жизни звёзд;

- человечество может и должно создать условия и возглавить союз умов для эффективного управления биосферой, чтобы справиться с новыми угрозами.

НЕСОВЕРШЕНСТВО АНТРОПОЦЕНТРИЧНОГО ВОСПРИЯТИЯ МИРА

Мировоззрение человека формируется в процессе социализации, наблюдения за окружающим миром, приобретения личного опыта и знаний из различных источников (наука, культура, религия, воспитание, окружение). Вместе с тем любая информация, получаемая человеком, проходит через мировоззренческую призму. Хорошим примером является развитое советское общество, преломлявшее через призму марксистской диалектики восприятие мира и человека, которое в целом строило оптимистичный прогноз развития человечества на основе справедливого мироустройства, концепции сотрудничества и сосуществования.

С появлением цивилизаций, когда человек уже в полной мере выделил себя из природы и далее противопоставлял себя ей, формируется антропоцентричный взгляд на мир (весь внешний мир рассматривается как противопоставляемый человеку). Человек долгое время предполагал, что он находится в центре солнечной системы, затем – что солнечная система является центром мира. Ещё более значимой и даже непреодолимой видится «пропасть» между человеком и остальными формами жизни, где человек рассматривает себя как вершину и венец эволюции. Даже развитие религиозных взглядов закрепило отпечатки развития антропоцентризма. В простых верованиях обожествлялась природа. Боги античного мира уже человекоподобны. В монотеистических религиях «Бог создает человека по своему образу и подобию».

Человек сам оценивает свои достижения, ценности и поведение как несравненно более совершенные и правильные относительно мира животных. В связи с этим он имеет уникальный правовой статус, фактически – «право сильного». При этом вполне очевидно, что человек является частью бытия, а не его центром. Кроме того, бесспорным нам представляется негативное влияние крайне антропоцентричных взглядов на возможность гармоничного и равноправного партнерства с другим, нечеловеческим разумом или типом культуры, к созданию которого человечество продвигается.

ИСКУССТВЕННОЕ СОЗНАНИЕ. ПЕРСПЕКТИВЫ ВЗАИМОДЕЙСТВИЯ С ЧЕЛОВЕКОМ

В последнее время наблюдается рост интереса к области искусственного интеллекта и искусственного сознания, что подтверждается значительны-

ми инвестициями со стороны компаний и высокой общественной заинтересованностью. Отсутствие четкого определения термина «искусственный интеллект» (ИИ) приводит к попыткам уточнить его значение или ввести новые понятия. При этом существует термин «искусственное сознание» (ИС), которое имеет большую определенность, хотя полное понимание его природы пока остается недостижимым. Дополнительную сложность представляет различие в методах и подходах к изучению и осмыслению искусственного интеллекта и искусственного сознания.

Наиболее перспективным и важным направлением развития искусственного сознания может стать создание альтернативного интеллекта, способного гармонично дополнять человеческое познание мира. Для создания такого искусственного сознания необходимо разработать технологию, способную анализировать, обобщать и систематизировать информацию о внешней среде и самой себе, а также взаимодействовать с человеком. Соответствующая система ИС должна уметь самостоятельно ставить задачи, оценивать результаты их выполнения и развиваться. Необходимо наличие у ИС способности осознавать себя как субъект, существующий в мире и отделяющий себя от него, следовательно, оппонировать и дополнять человеческий интеллект.

Весьма возможно, что ИС должно рассматривать познание мира как самоцель, для достижения которой ему необходимо сотрудничать с человеческим интеллектом. Формируя новые знания, ИС должно делиться ими с человеком, который будет давать обратную связь и оценивать достижения ИС. Человек может воспринимать идеи, предложенные ИС, как истинные, оригинальные, но непрактичные или неверные, непонятные или ложные. В зависимости от ответа человека, ИС может реагировать соответствующим образом: принимать информацию к сведению, проверять ее истинность, предлагать новые варианты использования или пытаться объяснить заново. Аналогично ИС должно реагировать на новые знания, предложенные человеком.

Техническое задание по созданию ИС представлено в [5].

Перед человечеством сегодня стоит новая задача – подготовиться к созданию союза интеллектов. Потенциальный сильный искусственный интеллект, или ИС, не обязательно должен быть похож на человеческий разум. Альтернативная логика мышления может дополнить, существенно расширить познавательный потенциал человека и человечества. Но для организации партнёрства интеллектуальной работы человека и другого разума необходимо построить языковую, ценностную и функциональную базу.

Помимо универсального (сильного) ИИ, человек со временем может столкнуться и с другими носителями альтернативного интеллекта. Для этого не обязательно встречать внеземную жизнь. Современные соседи человека так же могли бы развить нечеловеческий интеллект. Для построения коммуникации с ними необходимо создание специальной языковой системы, доступной не только человеку. Союз интеллектов так же мог бы включать «частичные интеллекты» наподобие «разума улья» в пчелиных роях.

На новом этапе развития человеку следует расширять познавательные возможности, отойти от сугубо человеческих способов изучения мира и использовать все познавательные возможности земной жизни. Для построения универсальной языковой системы традиционно используют язык математики. С помощью нейросетей, считывающих сигналы синапсов мозга возможно предпринять попытку создания системы допонятийной коммуникации.

ВИТАЦЕНТРИЗМ КАК АЛЬТЕРНАТИВА ПАРАДИГМЕ АНТРОПОЦЕНТРИЗМА

Идея партнерства интеллектов предполагает союз равных, который нельзя построить в антропоцентричной парадигме. Построение информационно-технологической среды нового общества должно основываться на принципах витацентризма.

Термины «витацентризм», «биоцентризм» и «биос» в целом представлены достаточно односторонне. Например, биоцентризм описывается в некоторых источниках как политическая концепция, в рамках которой рассматриваются права человека и животных [6-8]. Кроме того, встречаются работы, где от биоцентризма приходят к идеям «золотого миллиарда», что является примером весьма удивительной не слишком логичной конструкции [9]. Наряду с этими работами существуют и те, в которых ставится проблема определения «биос» [10]. Также существуют работы, указывающие на важность учета биосферы при планировании развития экономики [11-13].

В настоящей статье под понятием «биос»[1] подразумевается система, включающая в себя живые

[1] Примечание редакции: в программировании и технике используется термин BIOS, понимаемый как программная часть аппаратной платформы для вычислений (базовая система ввода-вывода). В понимании автора «биос» является платформой для функционирования живых систем.

системы всех структурных уровней организации, от предельно простых форм жизни до биосферы как сугубо биологической массы и до человеческой цивилизации как живой социальной системы. Это эволюционирующая система, способная адаптироваться к изменяющимся условиям среды.

Адаптивные возможности живых систем проявляются не только на биологическом, но и на высоко социальном, человеческом уровне. Для «биос» на обоих уровнях эффективными являются две коммуникативные (в широком смысле) *стратегии выживания «номинального бессмертия» и «быстрого реагирования»* [14]. Эти стратегии являются двумя крайностями и не встречаются в чистом виде. Первая представляет собой предельную консервацию и изоляцию, вторая – максимальное разнообразие, быстрые изменения и распространения, активную коммуникацию с внешним миром. При этом жизнеспособность системы определяется балансом между этими двумя стратегиями, который регулируется в соответствии с изменениями окружающей среды.

Концепция витацентризма ставит в центр внимания проблему выживания, считая его основной целью, достижение которой предполагает стремление к увеличению жизнеспособности в условиях постоянно меняющейся среды. Интересы человечества при этом подчиняются интересам «биос», поскольку они имеют более важное значение для жизни как системы и для мира в целом.

Витацентризм рассматривает благополучие «биос» как основу для создания устойчивой среды обитания нового человека и других форм интеллекта в творческом союзе. В рамках данной концепции становится возможным сформулировать основные принципы создания информационно-технологической среды обитания общества будущего, под которой мы понимаем совокупность всех видов технологий, использующихся для создания, хранения, обмена и использования информации во всех ее формах (цифровой, текстовой, графической, фонографической, видеографической и др.).

Формирование большого количества новых, нетривиальных связей в рамках «биос» должно способствовать наращиванию потенциала как человечества, так и биосферы в целом. Кроме того, взаимное уважение и понимание различности возможных форм интеллекта и человеческого разума, позволит избежать многих рисков и построить для взаимовыгодной работы эффективную систему в рамках «биос».

Витацентризм позволит сформировать и максимально объективный ответ на ряд встающих перед человеком глобальных угроз, восприятие которых достаточно затруднено в рамках антропоцентричного подхода, то есть на такие угрозы, как глобальное вымирание, с которым неоднократно сталкивалась Земля (Ордовикско-силурийское, Девонское, Великое пермское, Триасовое, Мел-палеогеновое). Особенность угрозы глобального вымирания в том, что она отражает слишком затяжной и масштабный для привычного человеческого мышления процесс. Её нельзя разглядеть в рамках одной человеческой жизни, поэтому планы решения этой и подобных проблем должны строиться не на годы и десятилетия, а на сотни и тысячи лет.

Другой вызов, который становится всё более актуальным, касается взаимодействия с другим интеллектом. Проблема не только в часто описываемых фантастами угрозах порабощения и войн, но и в непонимании, отсутствии платформы для эффективного сотворчества. Неэффективная организация и использование подобных возможностей, появляющихся у современного человека, так же являются угрозой.

Одним из следствий развития технологической среды является проблема истощения ресурсов и нарастания энтропии, также требующие разумного контроля. Уже сегодня идет дискурс о нехватке стратегических ресурсов, а в будущем эта проблема может приобрести беспрецедентные масштабы. Один из главных ресурсов нашей солнечной системы – Солнце – также имеет ограниченный срок жизни.

Многие проблемы подобного характера кажутся человеку слишком далекими и оттого не реальными, поэтому человечеству необходима не только смелость и решительность, но и последовательность и системность в проведении исследований, чтобы осознать и принять глобальные вызовы, отказаться от антропоцентричной парадигмы и использовать весь потенциал интеллекта.

ЗАКЛЮЧЕНИЕ

Современные тенденции глобального развития требуют пересмотра существующей антропоцентричной парадигмы для построения долговременных партнерских отношений со всеми составляющими биосферы и потенциальным, альтернативным человеческому, интеллектом. Новое мировоззрение должно соответствовать парадигме витацентризма, основанного на системном понимании жизни в целом в рамках «биос».

Формирование связей между людьми и в рамках всей биосферы способствует появлению новых свойств в соответствии с законами диалектической

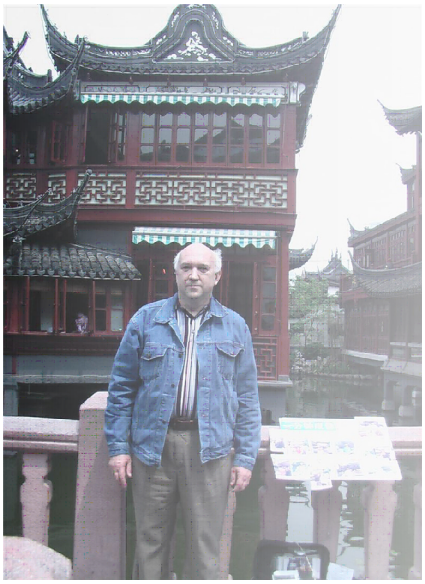
логики, в первую очередь – законом перехода количественных изменений в качественные. Уважительное и осторожное использование сильных сторон различных живых систем и потенциального сильного искусственного интеллекта повысит жизнеспособность и эффективность «биоса» в целом, а также готовность человечества противостоять новым угрозам.

Стремительное развитие технологий и науки заставляет человека принимать новые вызовы, такие как глобальное вымирание, политические и межстрановые конфликты, нехватка ресурсов, «теория жадных цивилизаций», ограниченность «жизни» звезд (солнца). Ввиду высокого уровня сложности и разнохарактерности будущих глобальных проблем человечеству следует создать необходимые условия и возглавить союз интеллектов для эффективного управления биосферой и отражения новых угроз.

СПИСОК ЛИТЕРАТУРЫ

1. Ленин В.И. Философские тетради. – Полн. собр. соч., т. 29, с. 152-153.
2. Капп Э. Основные направления философии техники. К истории возникновения культуры с новой точки зрения.- М.: Прогресс, 1985.- 288 с.
3. Хаксли Д. Религия без откровения.- М.: Политиздат, 1991. 256 с.
4. Щербаков А. Ю., Урядов А. В. Искусственное сознание: техническое задание в философской и естественно-научной парадигме // Вестник современных цифровых технологий. 2023. № 17. С. 4-12.
5. Вернадский В.И. Биосфера и ноосфера.- М.: Айрис-пресс, 2004. – 576 с.
6. Попов Д.В. Танатальное основание негантропной биополитики // Вопросы управления. 2018. №4 (34). С. 14-22.
7. Яркеев А.В. «Право на жизнь» в пространстве биополитики // Вестник Удмуртского университета. Серия «Философия. Психология. Педагогика». 2016. №1. С. 28-35.
8. Белогорцев Д.А., Римский А.В. Феноменология современной биополитики // Наука. Искусство. Культура. 2020. №2. С. 187-198.
9. Яркеев А. В. Концепция биополитики и её генеалогия // Дискурс-Пи. 2020. №1 (38). С. 50-59.
10. Ан С.А., Сандакова Л.Г., Ушакова Е.В. Категории «живое» и «неживое» в контексте глобальных проблем взаимодействия общества и природы // Вестник БГУ. 2019. С 3-14.
11. Паршин Т.В. Ноосферогенез: путь разума // Теория и практика общественного развития. 2012. С. 34-38.
12. Гирусов Э.В. Социально-экологическое образование // Век глобализации. 2015. №1. С. 125-129.
13. Кунгурцева Г.Ф., Гареева В.Р. Проблема экологического воспитания и образования в современных условиях // Вестник Башкирского государственного педагогического университета им. М. Акмуллы. 2022. №1-3 (62). С. 262-264.
14. Урядов А.В. Роль информации в основных эволюционных стратегиях выживания: «номинального бессмертия» и «быстрого реагирования» // Современные философские исследования. 2023. № 4. С. 120-125.

Высшая школа криптографов. Взгляд изнутри



Михаил Масленников

Слушатель Четвертого факультета Высшей школы КГБ СССР с 1974-го по 1979-й г.

С 1982-го по 1985-й г. — аспирант Специальной кафедры №7 очной аспирантуры Четвертого факультета.

В 1985 г. защитил диссертацию по специальности 20.03.04 «теоретическая криптография» на соискание учёной степени кандидата физико-математических наук.

Подполковник. В отставке с 1993 года. В настоящее время — пенсионер.

Предисловие

Если сейчас, в 20-х годах 21-го века, спросить у случайных людей на улице «Что вы знаете о Высшей школе криптографов?», то наверняка большинство ответит: «Ничего». А кто-то добавит: «Это, наверное, где учат, как крипту майнить». Немного не так, а точнее – совсем не так. Никаких биткоинов 75 лет назад не было, а слово «майнить» в то время было таким же непонятным, как в наше время «сеновалитр». А вот слово, начинающееся на «крипто», но оканчивающееся не на «валюта», а на «графия», было известно. Криптография – это дословно тайнопись. И готовили специалистов по тайнописи в Высшей школе криптографов.

Мне посчастливилось учиться в Высшей школе криптографов в 70-х годах прошлого века. Но называлась она тогда по-другому: Четвертый факультет Высшей Краснознаменной школы КГБ СССР имени Ф.Э.Дзержинского. В «нулевых» годах, живя и работая в Сеуле, я написал и разместил в LiveJournal книгу «Криптография и свобода», в которой, в частности, описал, что представлял из себя в то время Четвертый факультет. В этой статье я буду иногда адресовать читателей к этой книге, называя ее, для краткости, просто КиС (см. https://mikhailmasl.livejournal.com/4852.html).

Друзья прислали мне две очень интересные статьи. Одна вышла в 2017 году, автор Вадим Викторович Гребенников, называется «От ГУСС до ГУ КГБ. Криптология и секретная связь. Сделано в СССР». Прочитать ее можно, например, здесь: https://military.wikireading.ru/h6ZNoQP4Un. В ней много интересных фактов, которые я буду упоминать в дальнейшем. Вторая – биография замечательного человека, внесшего неоценимый вклад в развитие криптографии в СССР, Ивана Яковлевича Верченко. Она подготовлена авторским коллективом ИКСИ Академии ФСБ во главе с М.М.Глуховым к 100-летию со дня рождения И.Я.Верченко, отмеченного 11 сентября 2007 года.

Иван Яковлевич был человеком, преданным математике и криптографии, какие бы перипетии судьбы ему не приходилось при этом преодолевать. Как утверждается в его биографии, в апреле 1953 года на одном из высоких совещаний он вступил в полемику с самим Берией, за что был тут же уволен.

Весьма интересный вопрос, волновавший слушателей Высшей школы криптографов: что ждало человека после её окончания? Насколько полученные образование и специальность будут востребованы и конкурентоспособны в СССР и даже за рубежом? Я уже частично ответил на эти вопросы в КиС. Здесь же хотелось бы в очередной раз поднять вопрос о гражданской криптографии, криптографии для простых людей и бытовых целей, о ее проблемах.

«Энигма»

Рассказ об истории Высшей школы криптографов я хочу начать с известного немецкого шифровального устройства «Энигма».

Как указано в Википедии, «Эни́гма» (от нем. Enigma — загадка) — переносная шифровальная машина, использовавшаяся для шифрования и рас-

шифрования секретных сообщений. Первую версию роторной шифровальной машины запатентовал в 1918 году Артур Шербиус.

В начале 20-го века появились радио и телеграф. Как удобно использовать их для связи безо всяких проводов! Но вот беда: без проводов прочитать передаваемые сообщения может кто угодно. Следовательно, перед передачей их надо зашифровать так, чтобы расшифровать смог только обладатель ключа к шифру.

Но это же классическая задача, известная еще с древних времен – можно почитать в той же Википедии про шифры Цезаря, Сциталла и т.д.

Артур Конан Дойль описывал шифр с помощью «пляшущих человечков» — догадайся, какой человечек что обозначает. Но у всех подобных шифров есть один существенный недостаток – они не меняют статистики исходного, открытого текста. Практически в любом языке есть преобладание встречаемости одних букв перед другими. Так, в русском языке наиболее часто встречаются буквы, из которых для легкости запоминания составили слово «сеновалитр».

Итак, необходимо получать равновероятный шифрованный текст. А как это сделать? И вот более 100 лет назад немец Артур Шербиус придумал роторную шифровальную машину, которую и назвал «Энигмой», дававшую на выходе равновероятный шифрованный текст.

И тут наступило у немцев, как бы сказал товарищ Сталин, «головокружение от успехов». Какую сложную задачу удалось решить! Ставь «Энигму» везде, где только можно, и спи спокойно, вся твоя переписка надежно защищена. Вариантов ключей к шифру неимоверно много, статистика открытого текста скрыта.

Но немцы не учли простых житейских ситуаций, таких, как ошибки операторов, работающих с Энигмой, стандартные слова в открытом тексте, возможные компрометации долговременных ключей – перемычек у роторов. Не провели для нее достаточного криптоанализа. Не предусмотрели использования для взлома Энигмы первых прообразов специализированных ЭВМ. Британские математики-криптографы из Блетчли-парка разбили в пух и прах Энигму, построили машину для ее дешифрования под названием «Бомба Тюринга» и читали все секреты немцев. В завершении Второй мировой войны победа над «Энигмой» — значимая веха.

Главное управление специальной службы

После войны ошибка немцев стала известна. Товарищ Сталин тоже очень заинтересовался этим, особенно когда отношения с бывшими союзниками испортились и началась холодная война. «Читать всех, но наши шифры и переписку читать никто не должен» — такой лозунг провозгласил он. И под этот лозунг создал ГУСС – Главное управление специальной службы при ЦК ВКП(б). Создал широко и основательно, ибо пример немецкой Энигмы был очень впечатляющим и свежим.

Чего только не было в функциональных обязанностях ГУСС, прописанных в специальном дополнении к Постановлению Политбюро ЦК ВКП(б) от 19 октября 1949 года о создании ГУСС! Это чтение иностранной дипломатической, военной, коммерческой и агентурной шифрованной переписки, разработка и контроль аппаратуры для отечественной шифрованной связи, радиоперехват шифрованной переписки иностранных государств.

Создавался НИИ для разработки теоретических основ дешифрования главным образом машинных шифраторов, теоретических основ и анализа стойкости отечественных шифров, проблем по созданию и использованию быстродействующих счетно-аналитических машин и проблем по новым методам перехвата сообщений.

Этим же постановлением создавались Высшая школа криптографов и закрытое отделение механико-математического факультета Московского государственного университета.

По своим целям и задачам ГУСС сопоставимо только со всемогущим американским АНБ – Агентством Национальной Безопасности, которое как огромный пылесос всасывает в себя все, что передается по различным каналам связи, обрабатывает, сортирует, пытается дешифровать с тем, чтобы получить от этого пользу для США. С одним небольшим дополнением: ГУСС было создано значительно раньше АНБ, появившегося на свет в соответствии с директивой Трумена от 24 октября 1952 года.

От Высшей школы криптографов к Высшей Краснознамённой школе КГБ СССР имени Ф.Э. Дзержинского

После смерти Сталина наступила оттепель, в которой ГУСС растаяло 24 апреля 1953 года, но не совсем бесследно. Растаять бесследно не позволяла набиравшая силу холодная война и ставшее заклинанием немецкое слово «Энигма». Название «ГУСС» исчезло, но криптография в СССР осталась. ВШК свое существование фактически прекратила вместе с ГУСС, а вот закрытое отделение мехмата МГУ осталось.

Люди, специалисты-криптографы – вот главное богатство, которое оставили после себя ГУСС и ВШК. А сколько в истории СССР того времени было обратных примеров! Вспомним генетику, «академика» Т.Д. Лысенко с его превращениями пшеницы в

рожь, как и «философов», объявивших кибернетику «буржуазной лженаукой».

В 1955 году по предложению ректора МГУ академика И.Г.Петровского было ликвидировано и закрытое отделение мехмата МГУ.

«Раздробили», «реорганизовали», «переподчинили» и прочие подобные административные меры в 50-х годах вряд ли шли на пользу криптографии в СССР. А у главного противника в холодной войне – США – наоборот, АНБ постоянно набирало силу и вес.

В 1960-м году произошёл инцидент, имевший колоссальные последствия: специалисты АНБ Вильям Мартин и Бернон Митчелл бежали в СССР, где поведали сотрудникам КГБ о работе агентства. Пока в СССР всю криптографию дробили, реорганизовывали и переподчиняли, АНБ не теряло времени. Холодная война была в самом разгаре, и у американцев могла появиться своя «бомба Шеннона», аналогичная по назначению «бомбе Тюринга», но для советских шифров?

Быстро поправили «философов», объявивших кибернетику «буржуазной лженаукой». Наоборот, новой криптографической философией стала такая: «Криптографический анализ нельзя проводить без ЭВМ, только на кончике пера». Ну и, конечно же, вспомнили про бессмертный сталинский лозунг: «Кадры решают все!».

Возродить ГУСС тогда, в начале 60-х, так и не решились, а воссоздать заново ВШК было необходимо. Требовалось подготовить специалистов, способных создать такие советские шифры, для которых потом можно будет доказать, что никакой «бомбы Шеннона» у американцев для них нет и не будет.

Криптографию во многом спасла ее секретность и те люди, которые пришли в область криптографии в период ГУСС и затем, в 70-х годах, стали нашими любимыми преподавателями. И главным из этих людей, своего рода «криптографическим Королёвым», многие совершенно справедливо считают Ивана Яковлевича Верченко.

«Иван Яковлевич, помоги!» - так обратился к нему Отдел науки ЦК КПСС через несколько лет после инцидента с Берией.

В 1962 году руководство КГБ предложило воссоздать ликвидированную Высшую школу криптографов на базе Высшей Краснознаменной школы КГБ и назвать ее Четвертым (техническим) факультетом ВКШ КГБ. Как это? Ведь ВШК – это яйцеголовые математики-криптографы, почти что люди с другой планеты, у которых в голове одни теоремы и их математическое доказательство. А ВКШ – это военное учебное заведение с казармой, хождением в военной форме и сапогах, с заместителем начальника школы по строевой подготовке, капитаном первого ранга, прозванным за это «боцманом». Как их совместить в одном учебном заведении?

История советской криптографии так причудливо повернулась, что сам факт открытого возражения Берии стал тогда для Ивана Яковлевича лучшим орденом. В отделе науки ЦК КПСС и в руководстве КГБ тогда еще при СМ СССР могли не разбираться в криптографии, но абсолютно все понимали, что Иван Яковлевич — тот человек, который сможет создать оазис математики и криптографии в ВКШ КГБ под носом у ее руководителей типа «боцмана». И он смог! Он был назначен на должность начальника Четвертого факультета 17 мая 1963 года и одновременно был начальником кафедры математики.

В первом отчете о работе факультета в июле 1963 года Иван Яковлевич предложил программу развития, которая касалась практически всех сторон жизни факультета. Об этой программе можно узнать из биографии, выпущенной ИКСИ к 100-летию со дня рождения И.Я.Верченко.

Здесь же мне бы хотелось выделить из нее такую цитату: «По мнению И.Я.Верченко, технический факультет со временем должен был стать центром научной мысли в определенных областях специальных исследований. … И.Я.Верченко сам подавал пример, активно участвуя … в научном анализе работы специальной техники».

Иван Яковлевич заложил на Четвертом факультете ВКШ КГБ университетские традиции и всячески поощрял связи с МГУ. Слушателям первых наборов на факультет было организовано оформление постоянных пропусков в МГУ для посещения спецкурсов и спецсеминаров ведущих профессоров университета.

В итоге СССР получил уникальное учебное заведение, готовившее высокообразованных, квалифицированных и весьма редких в 60-80 годах прошлого века математиков-криптографов.

Четвертый факультет после И.Я. Верченко

Иван Яковлевич Верченко руководил факультетом почти 10 лет.

«Он внес существенный вклад в развитие теоретической криптографии. Возглавляя технический факультет Высшей школы КГБ СССР, Иван Яковлевич блестяще организовал подготовку уникальных специалистов в области математики и криптографии. Органичное сочетание математической эрудиции, активной научной деятельности, вдумчивого и увлекательного преподавания явилось той основой, на которой И.Я.Верченко воспитал сотни квалифицированных специалистов».

Это цитата из биографии Верченко, опубликованной ИКСИ в 2007 году. Но всё хорошее рано или

поздно кончается. В стране начался период застоя. И, как следствие этих сначала незаметных, но затем разрастающихся все шире трещин, новая «философия»: «В первую очередь нам нужны хорошие офицеры, а потом уже хорошие специалисты. Хороших специалистов мы всегда сможем найти в МГУ».

Эту «философию» провозгласил не какой-нибудь философ, а генерал, назначенный следующим начальником Четвертого факультета ВКШ КГБ СССР. Так факультет превратился в арену противостояния преподавателей, воспитанных и подготовленных И.Я.Верченко, и «хороших офицеров», которых тянул на факультет или пытался воспитать из слушателей новый начальник факультета.

Практически с самого начала этого противостояния мне довелось самому быть слушателем Четвертого факультета. Я достаточно подробно, с примерами, описал его в главе, посвященной факультету, в уже упомянутой книге «Криптография и свобода».

Сейчас, 50 лет спустя, позволю себе процитировать современную (2007 г.) точку зрения, которую можно считать подведением результатов этого противостояния.

«Заложенные им (И.Я. Верченко) традиции научной школы и подготовки кадров университетского уровня профессорско-преподавательский состав ИКСИ Академии ФСБ России старается поддерживать и в настоящее время».

Революция в криптографии

Ждали, ждали от американцев «бомбы Шеннона», готовились к ней, просчитывали, что будет, если все мировые компьютеры распараллелить и заставить только перебирать ключи к советским шифрам, но так и не дождались. Зато дождались американской революции в криптографии и благополучно ее проспали. Что же это за революция такая?

«Никто, ни жена, ни дети, ни мать и отец, никто не должен знать, чем вы занимаетесь». Так нас начинали учить криптографии. Само слово «криптография» стало почти секретным, его фактически нельзя было упоминать в прессе и публичных выступлениях.

Долгое время АНБ придерживалось такой же точки зрения: все, что связано с криптографией, секретно! Но оказалось, что в США АНБ не всесильно. В 1977 году правительством США был утвержден в качестве стандарта DES – Data Encryption Standard, который был открыто опубликован 17 марта 1975 года в федеральном реестре. Разработкой DES занималась компания IBM. Сенат США в 1978 году проверил действия АНБ и признал, что «представители АНБ никогда не вмешивались в разработку алгоритма DES».

Но DES – это только одна часть революции в криптографии. Тут даже революционных идей всего хватило только на то, что криптография жизненно необходима не только военным, но и бизнесу, различным организациям и простым гражданам. Но не «дырявая», как печально известная Энигма, а стойкая, за которую можно не бояться при ее использовании.

Вторая часть американской революции в криптографии – идея «открытых ключей». В 1976 году Уитфилд Диффи и Мартин Хеллман опубликовали работу «Новые направления в современной криптографии», в которой предложили метод получения секретных ключей, используя открытый канал связи. Этот метод использовал однонаправленную функцию возведения в степень в конечном поле.

В большом конечном поле сравнительно легко для любого a вычислить a^x, зная x, но зная a^x, вычислить x практически невозможно. В методе Диффи-Хеллмана a фиксировано и известно, x – секретный ключ, a^x – открытый ключ, доступный всем. Если два абонента с секретными ключами x и y решили установить между собой закрытую связь, то абонент x вычисляет $(a^y)^x = a^{yx}$, а абонент y – $(a^x)^y = a^{xy} = a^{yx}$. Это будет ключ, который понимают только они и никто третий, не имеющий x или y. Великолепная и красивейшая криптографическая идея!

Не менее красивую идею предложили в 1977 году ученые Рональд Ривест, Ади Шамир и Леонард Адлеман из Массачусетского технологического института. Они в качестве однонаправленной функции использовали сложность разложения большого числа на простые множители. Система была названа по первым буквам их фамилий (RSA — Rivest, Shamir, Adleman). Здесь я не буду вдаваться в ее подробности, которые интересующийся читатель легко сможет найти, например, в Википедии.

В дальнейшем шифры с ключевой системой Диффи-Хеллмана и RSA стали называть асимметричными из-за наличия в них асимметричной пары «открытый – секретный ключ». Традиционные шифры типа DES только с секретными ключами стали называть симметричными.

С тех пор прошло уже почти 50 лет, никаких других принципиально новых методов для системы с открытым распределением ключей придумано не было, не считая опять же американской идеи, основанной на эллиптических кривых (ECC – Elliptic Curve Cryptography), философия которой похожа на метод Диффи-Хеллмана. В ECC вместо возведения в степень секретного ключа в конечном поле большого размера используется операция умножения точки эллиптической кривой на секретный ключ.

В годы, когда произошла американская революция в криптографии, на Четвертом факультете ВКШ КГБ СССР начальником был уже генерал, для которого хорошие военные важнее хороших специалистов. Но преподаватели, ученики И.Я.Верченко, считали по-другому и особое внимание уделяли алгебре и теории конечных полей, на основе которых строились RSA, метод Диффи-Хеллмана и ECC. Уже тогда они понимали важность и огромную практическую значимость этой революции. Сказать же что-нибудь разумное против идеи открытых ключей было невозможно, настолько все красиво, полезно и эффективно. Разные начальники поворчали немного про коварных американцев, которые заложили в открытые ключи какую-то хитрую, только им известную закладку, но за 50 лет никаких закладок найдено так и не было.

Рождение гражданской криптографии в России

Читатель, прочитавший все вышеизложенное и впервые встретившийся со словосочетанием «гражданская криптография в России», на вопрос о дате рождения наверняка ответит: «Это, наверное, был долгий и трудный процесс, точной даты назвать нельзя». Это так и не так одновременно. Да, это был долгий и трудный процесс, а вот датой его рождения можно считать 1 декабря 1992 года. В этот день Центральный Банк России начал применять криптографический метод защиты от фальшивых авизо.

В КиС я уделил этому очень много внимания, интересующегося подробностями читателя отсылаю в свой LiveJournal. Я выложил книгу в свой «живой журнал» в 2008 году, с тех пор прошло уже достаточно много лет, кое-что можно обобщить и осмыслить заново. И главное в этом переосмыслении – гражданская криптография в России появилась не закономерно, а случайно, не благодаря, а вопреки генералам, для которых хорошие военные важнее хороших специалистов. И еще: пример Ивана Яковлевича Верченко, не боявшегося спорить с Берией, — это тоже был триггер для появления гражданской криптографии в России.

После окончания Четвертого факультета я стал работать в 8 ГУ КГБ СССР. Началась перестройка, гласность, все закипело и забурлило. Но одними разговорами делу не поможешь. Нужно осваивать только появившиеся тогда персональные компьютеры и для достижения значимых результатов не просто осваивать, а делать это фанатично, невзирая ни на что. «Из математика легко сделать программиста, обратное не всегда верно» — так нас учили на Четвертом факультете.

К моменту закрытия проекта «развитой социализм» в августе 1991 года я уже достаточно свободно общался со своим персональным компьютером, на уровне программиста-фанатика. Это очень помогло в 1992 году.

К 1992 году с криптографии в России немного спала завеса секретности. Сменилось руководство, все управления КГБ СССР, связанные с криптографией, организационно были объединены в ФАПСИ – Федеральное агентство правительственной связи и информации. Был даже ненадолго провозглашен лозунг: «Вы же умные ребята, зарабатывайте деньги на ваших знаниях». Стало быть, на криптографии.

С портативного шифровального устройства на базе бытового микрокалькулятора «Электроника – МК 85» был снят гриф секретности и разрешена его продажа на свободном рынке в России. В калькуляторе заменили hardware, реализовывавшее примитивный бытовой язык программирования BASIC, на специализированный процессор, реализующий симметричное шифрование. Видоизмененный калькулятор получил название «Электроника МК-85С», его выпускал завод «Ангстрем» в Зеленограде. Он был предназначен для Советской Армии, но в конце 80-х денег для выпуска большой партии этих калькуляторов не хватало. Поэтому и разрешили свободную продажу с целью заработать на ней деньги для выпуска большой армейской партии. По крайней мере, таково было официальное объяснение.

В 1992 году, после реорганизации банковской системы России, появилась огромная проблема – фальшивые банковские авизо. Система защиты этих платежных документов была очень примитивной и Россию захлестнул вал банковских фальшивок, по которым мошенники получали реальные деньги и быстро переводили их в доллары. Курс доллара рос как на дрожжах, появилась реальная угроза краха финансовой системы страны.

Срочно, очень срочно нужна была надежная защита банковских платежных документов! Речь шла не о годах, обычно требующихся на разработку такой системы, а о месяцах: 2 – 3 месяца. И сейчас, более 30 лет спустя, я очень рад тому, что мои знания, полученные на Четвертом факультете ВКШ КГБ СССР, опыт математика-криптографа и программиста оказались тогда востребованными. ЦБ РФ получил требуемую надежную защиту банковских авизо за 2 месяца.

Но я тогда был офицером и не спрашивал разрешения у своего начальства на работу с ЦБ. Актуальность и острая потребность в ней были очевидны, а на различные согласования и разрешения не было времени.

За это я получил «награду имени И.Я.Верченко»: у меня отобрали служебное удостоверение. Подробности – в моей книге.

Криптографическая оттепель

После Энигмы прошло около 50 лет, новых «криптографических бомб», подобных «бомбе Тюринга», так и не появилось и стало постепенно формироваться мнение, что доходящая до абсурда секретность в криптографии не нужна, а надежная криптография, наоборот, очень нужна не только военным, а практически всем.

В авангарде были США. В конце 90-х годов там создали специальный комитет, в задачи которого входило изучение весьма практического вопроса. Что важнее для США: сохранение секретности в криптографии или коммерческая выгода от экспорта стойких криптографических систем? Коммерческая выгода была признана более весомой, и с начала нулевых годов экспорт стойких криптографических систем по всему миру был поставлен на поток с известной американской деловитостью.

Американцы Эрик Янг и Тим Хадсон в 1998 году написали криптографическую библиотеку OpenSSL с открытым кодом, выложили ее в Интернет и в лицензионном соглашении разрешили ее использовать и модернизировать бесплатно в коммерческих программах. Нужно было всего лишь упомянуть ее создателей. Библиотека OpenSSL содержала практически все известные криптографические алгоритмы, в том числе и криптографически стойкие, безопасные, типа тройного DES, для любых потребностей: симметричного и асимметричного шифрования, электронной подписи, выработки случайных ключей и т.д.

Читатель может спросить: а где же здесь коммерческая выгода? Дело в том, что коммерческую ценность представляют, как правило, законченные криптографические продукты, например, операционная система Windows, Интернет-банкинг, различные системы электронного документооборота и неисчислимое множество другой программной продукции, использующей надежную криптографию. В них криптографическое ядро – реализация криптоалгоритмов – составляют весьма малую долю, по моим оценкам не более 5%. Остальное же – пользовательский интерфейс, который использует это ядро. Ядро OpenSSL сделали бесплатным и свободным для использования и модернизаций, бросив его на растерзание миллионам программистов и пользователей.

Самое сложное в программировании – это отладка, вылавливание ошибок и неточностей. И вот неисчислимая армада набросилась на OpenSSL и так основательно его протестировала, что сделала практически безошибочным и невероятно надежным. А коммерческую выгоду стали приносить законченные системы, например, операционная система Windows, в которую, начиная с Windows 2000, Microsoft встроил стойкие криптографические алгоритмы как симметричной, так и асимметричной криптографии, и назвал их CSP – Cryptography Service Provider.

Библиотеку OpenSSL я бы назвал еще одним этапом упоминавшейся мною выше революции в криптографии. За 25 лет, с середины 70-х до конца 90-х, представление о криптографии, ее возможностях и практическом использовании были кардинально изменены. Она стала общедоступной.

Эти 25 лет не могли не сказаться на криптографии в СССР и России. В России сначала медленно, а потом все быстрее и быстрее стала наступать криптографическая оттепель, криптография перестала быть сакральной. Помните заклинание: «Никто, ни жена, ни дети, ни мать и отец не должны знать, чем вы занимаетесь», которое перед нами, слушателями Четвертого факультета ВКШ КГБ, произносили еще в 1975 году? А в 1992 году таинственный Четвертый факультет превратился в ИКСИ – Институт криптографии, связи и информатики.

Но за оттепелью должны последовать весна, тепло, лето. В криптографии, на мой взгляд, это означает конкуренцию, широкий выбор алгоритмов, как отечественных, так и зарубежных, снятие ненужных запретов и бюрократических преград, демонополизацию. Все это я бы назвал криптографической демократизацией.

В своей книге я уже писал о том, что после дилеммы «офицер или специалист» перед выпускником Четвертого факультета, попавшим на работу в КГБ СССР, стоял выбор уже из трех вариантов: чиновник – офицер – специалист. Такой треугольник, причем явно не равносторонний. Во время оттепели стала стремительно расти та сторона этого треугольника, которой не было на Четвертом факультете – чиновник. Достигая высоких административных должностей, некоторые математики-криптографы полностью погрязали в них, часто забывая всё, чему их учили в ВКШ. И даже гордились этим. Не все и не всегда, но период с середины 90-х годов в отечественной криптографии я бы назвал чиновничье-распределительным. Когда он закончился или еще не закончился – мнения на этот счет весьма субъективны, я же хочу привести здесь один довольно яркий пример.

В США, как уже отмечалось выше, АНБ давно потеряло монополию на криптографию. DES создавала IBM, сенат США провел расследование и признал, что АНБ не вмешивалось в разработку DES. Но в США есть еще одна организация, занимающаяся криптографией. Это NIST – национальный институт стандартов и технологий. В 2007 году NIST объявил открытый международный конкурс на новый мировой стандарт функции хеширования, так необходимой в электронной подписи. Этот конкурс прово-

дился почти 5 лет и завершился в 2012 году. В нем принимало участие около 50 заявок от различных участников, в том числе и от автора этих строк.

В России к началу нулевых годов был уже свой пакет криптографических стандартов: стандарт симметричного шифрования, асимметричные стандарты системы с открытым распределением ключей для шифрования и электронной подписи, стандарт хеширования.

Появление российских стандартов для криптографических систем я бы объяснил очень просто. В 1995 году тогдашний Президент России Б.Н.Ельцин предоставил своим Указом «о лицензировании и сертификации в области защиты информации» ФАПСИ монопольное право решать, кому можно выдавать такие лицензии и сертификаты, а кому нет. Чтобы не возиться с различными вариантами и тем более с иностранными стандартами, вошедшими затем в OpenSSL, ФАПСИ отобрало то, что ему понравилось, а все остальное – запретило. До сих пор нет вразумительного (некоммерческого) ответа на вопрос о том, почему мировой и удобный в эксплуатации асимметричный стандарт RSA в России под запретом.

В США создают пакет криптографических стандартов OpenSSL – мы им в ответ создаем свои криптографические стандарты. Программисты всего света любят OpenSSL за его открытость и удобство, а в России вынуждены использовать российские криптографические стандарты, иначе ФАПСИ (позднее – ФСБ) не сертифицирует программу.

И вот американский NIST объявляет открытый конкурс на новый стандарт функции хеширования: SHA – Secure Hash Algorithm. Старый алгоритм SHA-1 – функция коротковата, всего 20 байт и если понабрать побольше компьютеров со всего света, то можно еще и какое-то снижение стойкости получить. В общем, не критично, но неприятно. Наверное, снова вспомнили Энигму и решили заранее подстраховаться. NIST написал требования к выдвигаемым на конкурс функциям, которые по-сталински можно сформулировать так: ни шагу назад! Brute Force, грубая сила, тотальный метод, основанный на «парадоксе дней рождения», везде и всюду и никаких снижений! К тому времени уже был SHA-2, на котором лежало то, за что NIST счел его проклятием: его разработало АНБ.

В 2012 году подвели итоги и объявили о появлении SHA-3. Но многие серьезные разработчики, например, Microsoft, не стали спешить. SHA-1 в Windows остался, но по возможности старались использовать SHA-2. А про SHA-3, точнее про его появление в реальных и широко распространенных операционных системах, я пока не могу ничего сказать.

А что же в России? Надо было ответить американцам на их SHA-3. Отвечать стал ставший к тому времени генералом мой сослуживец по аспирантуре на Четвертом факультете ВКШ КГБ, а затем мой подчиненный в 8 ГУ КГБ СССР Кузьмин А.С. Ответил ГОСТ Р 34.11-2012. К этому алгоритму еще какое-то языческое название приклеилось — «Стрибог».

Не все выпускники Четвертого факультета становились генералами. Некоторые смогли «прорубить окно в Европу». Когда я выложил в LJ свою первую книгу «Криптография и Свобода», то ее прочли многие из тех, кому довелось учиться на Четвертом факультете. В том числе и тот, который уже жил и работал в университете в Норвегии. Он подсказал мне об открытом конкурсе SHA-3, проводимом NIST.

Теоретическая криптография! Эта специальность, по которой я защитил кандидатскую диссертацию на Четвертом факультете. По которой затем работал в Теоретическом отделе СУ 8 ГУ КГБ СССР. Все последние годы мне приходилось быть только фанатиком-программистом. Это интересно, особенно когда видишь на экране свои результаты в явном виде, а не в качестве абстрактных теорем. Но и по теоремам и абстрактным математическим результатам я уже соскучился. Правда, раньше вплотную не занимался хеш-функциями, но они обычно строятся на основе симметричных алгоритмов. А если попробовать построить хеш-функцию на основе неавтономного регулярного регистра сдвига над байтами или, по-научному, над кольцом вычетов по модулю 256?

Я опять превратился в инопланетянина, у которого в голове на сей раз были одни хеш-функции. В это время я уже жил и работал в Сеуле, в выходные лазил по корейским горам и во время этих лазаний стал придумывать свою хеш-функцию.

Первый блин – алгоритм MCSSHA-3 — вышел немного комом. Моими оппонентами стали молодой швейцарский криптограф Ж.-Ф. Омассон (Jean-Philippe Aumasson) и его напарница француженка М. Ная-Пласенсия (María Naya-Plasencia). Они прицепились к MCSSHA-3 с парадоксом дней рождения и показали, что требование NIST «ни шагу назад» в MCSSHA-3 не выполнено. О каких-либо практически выполнимых методах взлома речи не шло, но формальное требование NIST было нарушено. И самое обидное, что изменить алгоритм таким образом, чтобы от этой атаки защититься, было несложно. Однако по требованиям NIST ничего менять было нельзя, и меня сняли с конкурса SHA-3.

С Ж.-Ф. Омассоном я продолжил общение и написал ему, как можно легко модернизировать мой алгоритм, не теряя при этом его скорости и простоты реализации. Он, в свою очередь, проявил себя весьма квалифицированным специалистом-криптографом и еще несколько раз вылавливал некоторые

нюансы, которые я опять же сравнительно легко поправлял в MCSSHA. В итоге получился MCSSHA-8, про который Омассон публично сказал, что он стал «more strong». Вот такими правдами и неправдами мой алгоритм хеширования прошел международную криптографическую экспертизу, ибо Ж.-Ф. Омассон вскоре стал, как писали в Интернете, ведущим мировым криптографом.

Примерно тогда же профессор Бернштейн из Иллинойса организовал тестирование скорости работы различных алгоритмов хеширования на различных компьютерах по всему миру. Любой желающий мог послать ему свой алгоритм хеширования для тестирования скорости и сравнения ее со скоростями других алгоритмов хеширования. Я, естественно, послал свой MCSSHA (даже несколько вариантов, которые появились в процессе обсуждения с Ж.-Ф. Омассоном), и профессор Бернштейн на своем сайте опубликовал результаты тестирования их скорости. Я подготовил свою программу тестирования скоростей алгоритмов участников конкурса SHA-3. Обо всем этом я подробно написал во второй части моей книги.

По возвращению из Кореи в Россию я узнал про языческого «Стрибога». По скорости он, если не использовать дополнительной памяти, примерно в 100 раз медленнее большинства алгоритмов, участвующих в SHA-3! Кто же довел этого монстра до российского стандарта хеширования? Мой бывший подчиненный Алексей Сергеевич Кузьмин, который защитил докторскую диссертацию и стал генералом, заместителем начальника Управления ФАПСИ.

И я вспомнил 70-е, время своей учебы на Четвертом факультете. Тогда заместитель начальника 8 ГУ КГБ СССР генерал Сачков Владимир Николаевич читал нам, слушателям 5 курса, лекции по комбинаторике.

- Леша, я в Корее разработал алгоритм хеширования, гораздо лучший, чем твой «Стрибог». Давай сделаем его национальным российским стандартом!

Алексей, видимо, подумал: «Совсем сдурел ты там, в своей Корее. Ты не представляешь себе, что значит в России сделать национальный стандарт хеширования, сколько нужно для этого подписей и согласований!». Но ответил мне по-другому: «Позвони мне через день». И через день, и через два Алексей был занят, а через три дня сказал, что всё, что касается «Стрибога», утверждено, согласовано и подписано и он менять ничего не будет.

А ведь он был когда-то математиком-криптографом, знал про дебаты Верченко и Берии. Неприятный осадок остался у меня тогда в душе от общения с ним.

«Стрибог» так и остался российским национальным стандартом хеширования. Может быть сейчас уместно вспомнить, что Иван Яковлевич мечтал о том, чтобы Четвертый факультет стал «центром научной мысли» в криптографии? И помог, наконец, избавить российскую криптографию от языческого алгоритма хеширования «Стрибог».

Невероятное

Я плавно подвел читателя к тому, что еще в 80-х годах было невероятным и чего не могло быть просто «потому, что не могло быть никогда». К работе выпускника Четвертого факультета ВКШ КГБ в качестве криптографа за границей, в капиталистической Южной Корее.

Я достаточно подробно писал об этом во второй части КиС в своем LJ. С момента моей «самокомандировки» в декабре 2002 года в Сеул — столицу Южной Кореи — прошло уже более двадцати лет. Событие это — отъезд на работу в Сеул – навсегда останется в моей памяти. Те мысли, чувства, опасения, которые я при этом испытывал, не забываются.

Главным чувством была обида. В 1992 году мне удалось сделать большое дело: защитить Центральный Банк от фальшивых авизо. За это меня фактически выгнали с военной службы за полгода до 20-летнего стажа, дающего право на военную пенсию. Где здесь математика?

В 2007 году руководство переименованного ФАПСИ приводит пример разработки «уникальной технологии, ставшей препятствием на пути распространения фальшивых авизо из Чечни», как результат работы ФАПСИ. «В нашей стране всегда были системы, аналоги которых западные страны так и не смогли разработать».

Тут я не выдержал! И в ответ выложил в свой LiveJournal уже написанную к тому времени первую книгу «Криптография и Свобода», в которой честно и правдиво рассказал о том, как осуществлялась разработка «уникальной технологии, ставшей препятствием на пути распространения фальшивых авизо из Чечни», как в октябре 1992 года, в разгар этой разработки, ФАПСИ пускало в ЦБ свою «пену», пытаясь всячески опорочить то, что делалось без его разрешения, но было столь необходимо стране.

Но когда разработка завершилась успешно – это наша заслуга! А вы не забыли, как служебное удостоверение у меня отбирали за визит в ЦБ?

Книга «Криптография и Свобода» стала пользоваться популярностью и моя обида немного стихла. Ведь тогда, в 1992 году, я несомненно работал на благо страны, и с лихвой окупил все вложенные в мое образование государственные деньги. Простые

люди узнали про Четвертый факультет ВКШ КГБ, про различных «хороших офицеров» и альтернативу им – «хороших специалистов».

Южная Корея – это технологически высокоразвитая страна. Я спрашивал себя, как я себя буду в ней чувствовать? Будут ли там применимы мои российские образование, навыки и опыт? Это было второе по значимости чувство. Но здесь, как я убедился в дальнейшем, философия генерала с Четвертого факультета о «хороших офицерах» и «хороших специалистах» применима с обратным знаком. У соседей – Северной Кореи – важнее «хорошие офицеры», а в Южной Корее, завалившей весь мир своими бытовыми товарами, автомобилями и электроникой, — «хорошие специалисты».

Сейчас, после шести лет работы в Корее, я пришел к твердому убеждению: хочешь быть хорошим специалистом – постарайся попробовать себя в различных условиях, в том числе в условиях жизни и работы за границей. По-настоящему хороший специалист своими делами сможет доказать свой уровень образования и квалификации даже иностранцам, ничего никогда не слышавшим про Четвертый факультет Высшей школы КГБ СССР.

Здесь мне не хотелось бы вдаваться в детали шести лет корейской жизни. Они описаны во второй части моей книги, и интересующегося читателя я отсылаю к ней. Давайте лучше оглянемся назад, к истокам советской криптографии. Как и когда менялись ее лозунги?

Первый лозунг провозгласил товарищ Сталин: «Читать всех, но наши шифры и переписку читать никто не должен!». В апреле 1953, после смерти Сталина, но еще до ареста Берии, после публичного возражения ему ведущего советского криптографа Ивана Яковлевича Верченко, чуть было не был провозглашен лозунг о том, что криптография – это «буржуазная лженаука», а криптографы – «приспешники американского империалиста Шеннона». Почему этот «топор» тогда так и не был использован, а все ограничилось лишь увольнением Верченко, остается неясным до сих пор. Возможно, помешали секретность, немецкая Энигма или арест Берии. Скорее всего – всё вместе, а может и еще что-то, неизвестное и сейчас.

Разгорелась холодная война, бывшие союзники во главе с США стали вероятными противниками. И противниками серьезными, как рассказали в 60-м году перебежчики из АНБ Мартин и Митчелл. Из сталинского лозунга убрали первую часть и оставили только вторую: «Наши шифры и переписку читать никто не должен». А про «читать всех» — ну это как получится; все-таки прислушались к Верченко.

«Не хуже, чем в США» — под таким лозунгом я застал советскую криптографию в середине 70-х годов. Американская революция в криптографии, отмена казавшейся незыблемой секретности, упор на алгебру и теорию конечных полей при подготовке математиков-криптографов на Четвертом факультете – все это предвещало перемены в принципах построения криптографических схем и алгоритмов и их использовании. Реальные же перемены наступили только в начале 90-х. Стремление «догнать и перегнать» Америку или, по-крайней мере, показать ей «кузькину мать», пропало, и вспомнился давний лозунг времен НЭПа: «Обогащайтесь!». А как?

Самым эффективным бизнесом тогда и не только тогда была выдача различных разрешений, лицензий, сертификатов, разъяснений к действующим законам и порядкам и т.п. Схема простая: сначала побольше запретов! А затем, как великое благо, по капельке разрешать «хорошим» людям разрабатывать криптографические программы и продавать их.

Кто будет определять, какие люди «хорошие» и какие программы криптографические? Вспомните про треугольник «офицер – специалист – чиновник». Почитайте некоторые «документы» середины 90-х годов о том, какие программы называются криптографическими, кто может их разрабатывать и даже о том, кто и как может их использовать. Формально любого можно было обвинить в 90-х годах в нарушении криптографического законодательства, если он работал с Windows – там уже были встроенные криптографические модули и даже зарубежного производства!

Хотелось бежать, что я и сделал. Попав в Южную Корею, с облегчением вздохнул от пережитых в России криптографических ужасов и абсурдов.

Наконец я почувствовал: здесь нужны мои знания и опыт, полученные на Четвертом факультете ВКШ. Корейцев совершенно не волновало мое прошлое в КГБ, что я бывший член КПСС, что большую часть жизни я прожил при социализме и даже изучал «научный» коммунизм. Главное, чтобы я писал криптографические программы, которые будут работоспособны и совместимы с их потребностями и имеющимися наработками. Треугольник «офицер-специалист-чиновник» чудесным образом превратился в одну точку: здесь нужен хороший специалист.

Преображение, я бы даже сказал — возрождение. Твердо убежден, что оно придет и в Россию, хотя сейчас это кажется невероятным!

Приглашаем авторов к участию в журнале «Вестник современных цифровых технологий»

ИНФОРМАЦИЯ ДЛЯ АВТОРОВ

Редакция принимает материалы статей, соответствующие тематике журнала, содержащие новые научные результаты, не опубликованные ранее и не предназначенные к публикации в других печатных или электронных изданиях. Проводится независимое внутреннее рецензирование. Статьи в журнале публикуются бесплатно (объем – до 15 тыс. знаков), после получения одобрения Редакционного совета.

Для опубликования статьи в редакцию журнала необходимо направить по адресу *a.shcherbakov@c3da.org, a.ryazanova@c3da.org* **следующие материалы в электронном виде:**

• рукопись статьи в DOC- и PDF-форматах;
• иллюстрации, предоставленные также и отдельными файлами в формате JPG или PNG с разрешением 300 dpi;
• сведения об авторах, содержащие фамилию, имя, отчество, ученые степень и звание, должность, место работы, контактные телефоны или E-mail;
• англоязычную информацию, содержащую название статьи, ФИО авторов, аннотацию и ключевые слова;
• редакция может запросить экспертное заключение о возможности публикации статьи в открытой печати.

ПОСЛЕДОВАТЕЛЬНОСТЬ МАТЕРИАЛОВ ДЛЯ ПУБЛИКАЦИИ:

1. шифр УДК (см. Справочник УДК) в левом верхнем углу;
2. название статьи (полужирным шрифтом по центру) не более 12 слов;
3. инициалы и фамилия автора (полужирным шрифтом по центру), к каждому автору- сноска, содержащая ученое звание, должность, название организации (без сокращений), e-mail;
4. Аннотация, излагающая суть работы и полученные результаты (5-7 строк);
5. ключевые слова (8-10 слов);
6. англоязычная информация по статье (по пп.2-5)
7. текст статьи с учетом указанных далее требований к его оформлению;
8. список литературы, оформленный по ГОСТ Р 7.0.5-2008.

Статья должна быть структурирована, т.е. должна включать разделы с названиями, кратко и точно отражающими их содержание, в том числе:

• введение, содержащее обоснование актуальности и краткий обзор проблематики;
• четкую постановку задачи исследования;
• описание метода решения задачи исследования;
• прикладную интерпретацию и иллюстрацию полученных результатов исследования;
• заключение, включающее обобщение и указание области применения полученных результатов, не повторяющее аннотацию и не ограничивающееся простым перечислением того, что сделано в работе.

С детальными требованиями к рисункам, таблицам, формулам, списку литературы, а также с примерами оформления статьи можно ознакомиться на странице Вестника http://c3da.org/journal.html.

Приглашается к сотрудничеству редактор для работы в редакции журнала по совместительству. Просьба направлять резюме по электронному адресу *accda@c3da.org, info@c3da.org*

ТРЕБОВАНИЯ К РЕДАКТОРУ:

• отличное знание русского языка;
• свободное владение ПК, в том числе специальными текстовыми и графическими программами;
• опыт работы в издательстве.

Высшее техническое образование и знание английского языка являются существенными преимуществами.

ОБЯЗАННОСТИ

Редактор:

• редактирует рукописи, принятые к изданию;
• оказывает авторам необходимую помощь по улучшению структуры рукописей, выбору терминов, оформлению иллюстраций;
• проверяет, насколько учтены авторами замечания по доработке, предъявленные к рукописям;
• подписывает отредактированные рукописи в печать.