

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

ISSN 2686-9373

**ВЕСТНИК СОВРЕМЕННЫХ ЦИФРОВЫХ
ТЕХНОЛОГИЙ**

15. 2023 (ИЮНЬ)

ВЕСТНИК

**СОВРЕМЕННЫХ
ЦИФРОВЫХ
ТЕХНОЛОГИЙ**

НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ



Главный редактор

д.т.н., проф., академик РАЕН

Щербаков А.Ю.

Ученый секретарь Редакционного совета

Рязанова А.А.

Верстка Груздева Н.В.



www.c3da.org

**№15
ИЮНЬ 2023**

ISSN 2686-9373

Издатели: *Российский государственный социальный университет
Ассоциация РКЦФА*

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

E-mail: accda@c3da.org, info@c3da.org
www.c3da.org



Подписано в печать 30.06.2023 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

Главный редактор – Щербаков Андрей Юрьевич, доктор технических наук, профессор, заведующий кафедрой когнитивно-аналитических и нейро-прикладных технологий РГСУ, президент Ассоциации специалистов в области развития криптовалют и цифровых финансовых активов (Ассоциации РКЦФА).

Председатель Редакционного Совета – Сигов Александр Сергеевич, академик Российской академии наук, доктор физико-математических наук, член Научного совета при Совете Безопасности РФ, президент Российского технологического университета МИРЭА, заслуженный деятель науки Российской Федерации, почётный работник высшего профессионального образования РФ.

Сопредседатель Редакционного Совета – Хазин Андрей Леонидович, ректор Российского государственного социального университета, академик Российской академии художеств.

Сопредседатель Редакционного Совета – Алиев Джомарт Фазылович, доктор философии в области бизнес-права (PhD), доктор делового администрирования в области финансов (DBA), кандидат экономических наук, первый проректор Российского государственного социального университета.

Сопредседатель Редакционного Совета – Елизаров Георгий Сергеевич, доктор технических наук, директор ФГУП «НИИ «Квант», академик Академии Криптографии РФ.

Ученый секретарь Редакционного Совета – Рязанова Алина Александровна, вице-президент Ассоциации РКЦФА по международному сотрудничеству, ведущий специалист Научно-образовательного центра социальной аналитики Российского государственного социального университета.

Гриняев Сергей Николаевич, доктор технических наук, декан Факультета комплексной безопасности ТЭК РГУ нефти и газа (НИУ) имени И.М. Губкина.

Запечников Сергей Владимирович, доктор технических наук, доцент, профессор Института интеллектуальных кибернетических систем Национального исследовательского ядерного университета «МИФИ», Вице-президент Ассоциации РКЦФА по научной работе.

Кириченко Татьяна Витальевна, доктор экономических наук, профессор, заместитель заведующего кафедрой безопасности цифровой экономики РГУ нефти и газа (НИУ) имени И.М. Губкина.

Комзолов Алексей Алексеевич, доктор экономических наук, профессор, заведующий кафедрой безопасности цифровой экономики РГУ нефти и газа (НИУ) имени И.М. Губкина.

Конявский Валерий Аркадьевич, доктор технических наук, заведующий кафедрой Московского физико-технического института (МФТИ).

Сенаторов Михаил Юрьевич, доктор технических наук, почетный эксперт Ассоциации РКЦФА.

Шилова Евгения Витальевна, доктор экономических наук, профессор кафедры экономики знания Высшей школы современных социальных наук МГУ имени М.В. Ломоносова.

Егоров Владимир Ильич, кандидат физико-математических наук, заместитель директора Национального центра квантового интернета.

Мачихин Дмитрий Сергеевич, эксперт по вопросам противодействия отмыванию доходов и финансированию терроризма (ПОД/ФТ), учета и комплаенса цифровых финансовых активов и валют, член профильного комитета при Государственной Думе РФ.

Правиков Дмитрий Игоревич, кандидат технических наук, заведующий кафедрой комплексной безопасности критически важных объектов РГУ нефти и газа (НИУ) имени И.М. Губкина.

Терпугов Артем Евгеньевич, кандидат экономических наук, Проректор Государственного университета управления.

РЕДАКЦИОННОЕ ПРИМЕЧАНИЕ

Пятнадцатый номер «Вестника современных цифровых технологий» преимущественно посвящен различным аспектам современных сетевых технологий, в том числе таким достаточно новым задачам, как создание и эксплуатация программно-определяемых сетей.

Весьма обширный раздел «Практические аспекты цифровых технологий» открывает статья коллектива авторов **«Угрозы безопасности информации для программно-определяемых сетей»**, которая посвящена актуальной проблеме безопасности информации для программно-определяемых сетей (Software Defined Networking, SDN). В статье рассмотрена технология SDN, определены компоненты программно-определяемых сетей и группы угроз для них, предложено использование квантовых технологий для решения некоторых проблем безопасности для указанных сетей.

В статье **«Методы оптимизации структуры квантовых сетей для обеспечения централизованного управления ключами»** Алексея Сантьева рассматривается задача оптимизации структуры квантовых сетей для обеспечения централизованного управления ключами при интеграции квантовых сетей с масштабными информационными системами на примере интернета вещей. Автор предлагает модернизировать методы построения квантовых сетей, расширить сценарии их применения и использовать квантово-стойкие методы защиты каналов связи.

Подход «суверенного интернета» рассмотрен в статье **«Принципы организации безопасного интернета на примере системы TheOoL»** Алексея Ненашева. В работе предложены принципы построения системы частного интернета, включающей оверлейный протокол передачи данных, бессерверный хостинг и облачные вычисления, а также бессерверную поисковую машину и интегрированную систему платежей. Система частного интернета рассматривается на примере проекта TheOoL - универсальной распределенной децентрализованной операционной системы. Управление сетевыми взаимодействиями выполняет инновационный протокол информационного взаимодействия и контроля топологии на базе технологий распределенного реестра.

Раздел завершает статья Сергея Велигодского и Натальи Милославской **«Технологии, обеспечивающие функционирование центров управления сетевой безопасностью информационно-телекоммуникационных сетей, и оценка уровня их зрелости»**. Целью статьи является определение современных технологий, обеспечивающих функционирование центров управления сетевой безопасностью (ЦУСБ) информационно-телекоммуникационных сетей (ИТКС) организаций, их вклада в поддержку выполнения соответствующих процессов и предоставления услуг по управлению сетевой безопасностью ИТКС, а также общего уровня зрелости ЦУСБ.

В текущем выпуске мы открываем раздел «Современные цифровые технологии: обзоры, мнения, дискуссии».

В качестве флагамена раздела представляем читателю весьма интересный и принципиально новый подход к изучению и оценке социальных процессов и явлений, изложенный Джомартом Алиевым в работе, которую он удачно и остроумно назвал **«Социальной физикой 5.0»**. Начиная с глубокого экскурса в историю вопроса, автор предлагает в качестве одного из базовых понятий рассмотреть категорию энтропии и вводит ряд совершенно новых и важных принципов, включая принцип процессинга энтропии и энтропийного поля.

Рецензия Эдуарда Пройдакова на книгу Михаила Лысачева и Александра Прохорова «Искусственный интеллект. Анализ, тренды, мировой опыт», поможет читателю разобраться в обширном материале книги, касающемся самых разных вопросов, связанных с тематикой искусственного интеллекта, от технических вопросов, включая методы и ИИ-технологии, до вопросов применения ИИ-систем, их проектирования и необходимой для этого бизнес-аналитики разного уровня.

Раздел «Цифровое искусство» представлен статьей художницы и дизайнера Варвары Ахремко **«Нейросеть и дизайнер»**, затрагивающей вопросы использования нейросетей в изобразительном искусстве и графическом дизайне. Статью иллюстрируют работы автора.

В разделе «Литература о цифровых технологиях» представляем нашим читателям рассказ **«Искусственный интеллект»** Егора Федорова, в котором автор выразил оригинальный взгляд на роль и место искусственного интеллекта в человеческой истории и эволюции.

СОДЕРЖАНИЕ

1. ПРАКТИЧЕСКИЕ АСПЕКТЫ ЦИФРОВЫХ ТЕХНОЛОГИЙ

В.И. Егоров, А.А. Сантьев, А.Ю. Щербаков – Угрозы безопасности информации для программно-определяемых сетей

V.I.Egorov, A.A. Santev, A.Yu. Shcherbakov – Information security threats for software-defined networks4

А.А. Сантьев – Методы оптимизации структуры квантовых сетей для обеспечения централизованного управления ключами

A.A. Santev – Methods for optimizing the structure of quantum networks to ensure centralized key management12

А.В. Ненашев – Принципы организации безопасного интернета на примере системы TheOoL

A.V. Nenashev – Principles of formation a safe internet on the example of system TheOoL20

С.С. Велигодский, Н.Г. Милославская – Технологии, обеспечивающие функционирование центров управления сетевой безопасностью информационно-телекоммуникационных сетей, и оценка уровня их зрелости

S.S. Veligodskiy, N.G. Miloslavskaya – Technologies ensuring the operation of network security centers of information and telecommunication networks and their maturity level assessment30

2. СОВРЕМЕННЫЕ ЦИФРОВЫЕ ТЕХНОЛОГИИ: ОБЗОРЫ, МНЕНИЯ, ДИСКУССИИ

Д.Ф. Алиев – Социальная физика 5.042

Э. М. Пройдаков – О книге «Искусственный Интеллект. Анализ, тренды, мировой опыт»69

3. ЦИФРОВОЕ ИСКУССТВО

Варвара Ахремко – Нейросеть и дизайнер70

4. ЛИТЕРАТУРА О ЦИФРОВЫХ ТЕХНОЛОГИЯХ

Егор Федоров – Искусственный интеллект75

УДК: 004.75, 004.41

Угрозы безопасности информации для программно-определяемых сетей

V.I.Egorov, A.A. Santev, A.Yu. Shcherbakov

Information Security Threats for Software-Defined Networks

Abstract. The article is devoted to the consideration of actual information security threats for software-defined networks (SDN). The SDN technology is considered, the components of software-defined networks and specific threats to SDN networks are identified, the use of quantum technologies is proposed to solve some security problems for these networks.

Keywords: software-defined network, quantum technologies, information security threats, threat model, network controller, application correctness, isolated software environment.

В.И. Егоров¹А.А. Сантьев²А.Ю. Щербаков³

¹Кандидат физико-математических наук, директор лаборатории квантовых коммуникаций, ведущий инженер лидирующего исследовательского центра «Национальный центр квантового интернета Университета ИТМО.

E-mail: viegorov@itmo.ru

²Инженер лидирующего исследовательского центра «Национальный центр квантового интернета» Университета ИТМО, научный сотрудник ООО «СМАРТС-Кванттелеком».

E-mail: aasantev@itmo.ru

³Доктор технических наук, заведующий кафедрой когнитивно-аналитических и нейро-прикладных технологий РГСУ, ведущий научный сотрудник Государственного университета управления.

E-mail: x509@ras.ru

Аннотация. Статья посвящена рассмотрению актуальных угроз безопасности информации для программно-определяемых сетей (Software Defined Networking, SDN). Рассмотрена технология SDN, определены компоненты программно-определяемых сетей, специфические угрозы для сетей SDN, предложено использование квантовых технологий для решения некоторых проблем безопасности для указанных сетей.

Ключевые слова: программно-определяемая сеть, квантовые технологии, угрозы информационной безопасности, модель угроз, контроллер сети, корректность приложений, изолированная программная среда.

ВВЕДЕНИЕ

Современные технологии практически в любой области демонстрируют нам, с одной стороны, потребность в быстром росте и адаптации к изменяющимся условиям и требованиям, а с другой — показывают некоторое упрощение принципов, связанное с ростом вычислительной мощности управляющих этими технологиями вычислительных устройств. Например, 3D-печать расплавляемым пластиком оставляет инженера в недоумении, почему эта технология не появилась двадцать или тридцать лет назад. Аналогичная история наблюдается и с телекоммуникационным оборудованием.

Это объясняется, в том числе, технологическим контекстом и свойствами развития и внедрения технологий во времени. Если обратиться к историям крупных компаний, можно заметить, что путь от разработки до высокой прибыли все время сокращался. Например, ветерану рынка информационных технологий компании AOL Inc. (сокр. от англ. America Online Incorporated; AOL Inc. — американский медийный конгломерат, поставщик он-

лайн-служб и электронных досок объявлений) для привлечения миллиона клиентов понадобилось 9 лет, Facebook для достижения той же цели понадобилось 9 месяцев, а онлайн-сервису DrawSomething — уже всего 9 дней [1].

Интересно и то, что AOL Inc., изначально крупнейший в США интернет-провайдер, во время своего расцвета в начале 2000-х годов был приобретён самым крупным медиальным концерном Time Warner Inc. В дальнейшем компания утратила прежние позиции, что повлияло на её стоимость и привело к массовым увольнениям сотрудников. К концу 2015 года стоимость AOL была в 15 раз ниже, чем у Time Warner. Весьма возможно, что такой результат как раз и был связан с провалами в стратегии предоставления услуги и развития телекоммуникационного оборудования.

ТРЕНДЫ РАЗВИТИЯ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

В настоящее время особенно значимыми являются

ся следующие тренды развития корпоративных сетей и сетей центров обработки данных:

- рост объемов трафика и изменение его структуры в сторону передачи видео и унифицированных коммуникаций (от англ. Unified communications, UC) — технологий, представляющих собой интеграцию таких услуг реального времени, как мгновенные сообщения (чат), информация о присутствии (presence), телефония (включая IP-телефонию), видеоконференция, совместная работа над документами, управление вызовами и распознаванием речи с унифицированными почтовыми системами;
- необходимость поддержки мобильных пользователей (BYOD — от англ. Bring Your Own Device, приноси свое собственное устройство — корпоративная политика, предполагающая использование сотрудниками собственных устройств при работе с корпоративными ресурсами. Как правило, политика BYOD распространяется на смартфоны, но она также может применяться по отношению к планшетами и ноутбукам);

- создание высокопроизводительных кластеров для обработки и хранения больших данных (big data);

- виртуализация для предоставления облачных сервисов (Cloud Bursting — по определению Amazon — в облачных вычислениях «разрыв облака» — конфигурация, которая настраивается между частным и общедоступным облаками для удовлетворения пиковых потребностей в ИТ. Если организация, использующая частное облако, достигает 100 процентов своей ресурсной емкости, избыточный трафик направляется в общедоступное облако, поэтому прерывания работы служб не происходит).

При этом телекоммуникационная сеть в классическом ее виде (в первую очередь с точки зрения управления) может быть ограничивающим фактором развития вычислительной инфраструктуры. Классические подходы, в частности, на основе виртуализации сетей, на сегодняшний день тоже не соответствует уровню развития виртуализации серверов и систем хранения данных.

Что касается использования терминов VLAN (аббр. от англ. Virtual Local Area Network — виртуальная локальная сеть), VRF (аббр. от англ. Virtual Routing and Forwarding instance — виртуальная маршрутизация и пересылка), в данном случае терминология не устоялась: у компании Cisco это VRF, в Huawei — VPN-instance (Virtual Private Network), в Juniper — Routing Instance. При этом суть технического решения — виртуальный маршрутизатор, например, в VirtualBox на одном физическом сервере реализуются несколько виртуальных серверов, в

данном случае на одном физическом маршрутизаторе существует несколько виртуальных маршрутизаторов.

Недостатком существующих телекоммуникационных сетей является их статичность и несоответствие как быстрой динамике технического масштабирования сети, так и потребностям развития бизнеса, а распределенное управление устройствами традиционных сетей достаточно сложное и не всегда эффективное.

ОТ КЛАССИЧЕСКОЙ СЕТИ К ПРОГРАММНО-ОПРЕДЕЛЯЕМОЙ

Таким образом, возникает идея новой технологии или подхода к построению информационных сетей, позволяющая решить перечисленные выше проблемы — Software Defined Networking, сокр. SDN (от англ. программно-конфигурируемая сеть).

Программно-конфигурируемая сеть (также программно-определяемая сеть) — сеть передачи данных, в которой уровень управления сетью отделен от устройств передачи данных и реализуется программно; таким образом, она представляет собой одну из форм виртуализации вычислительных ресурсов.

Современное сетевое устройство (роутер или коммутатор) логически состоит из трех взаимосвязанных компонент.

1. Уровень управления включает интерфейс командной строки — инструмент для работы пользователя с программой с помощью команд (или CLI — аббр. от англ. Command Line Interface), встроенный веб-сервер или API и протоколы управления. Задача этого уровня — обеспечить управление устройством.

2. Уровень управления трафиком — это различные алгоритмы, задачей которых является автоматическая реакция на свойства изменения потока передачи данных (трафика).

3. Передача трафика — функционал, обеспечивающий физическую передачу данных.

Возможно модернизировать сетевую архитектуру с решением следующих задач: централизовать управление трафиком, отделив управление от устройств, и централизовать управление устройствами. В результате «новый» роутер или коммутатор будет обслуживать только поток данных (уровень передачи трафика DATA PLANE) и в силу этого становится более просто реализуемым и, соответственно, более дешевым.

Конечно, полностью ликвидировать «интеллект» сетевого устройства не получится, но его условно

можно заменить некоторой таблицей переадресации (forwarding table).

Все «интеллектуальные» функции управления (MANAGEMENT PLANE и CONTROL PLANE) в этом случае переносятся в отдельное центральное устройство, называемое контроллером SDN.

В результате становятся реализуемыми следующие свойства сети:

- разделение функций передачи трафика и функций управления (включая контроль как самого трафика, так и осуществляющих его передачу устройств);
- единый, стандартный и открытый интерфейс между устройствами управления и передачи (существуют различные SDN протоколы, наиболее распространенный получил название OpenFlow);
- централизованное управление сетью (контроллер SDN);
- виртуализация физических ресурсов сети;
- возможности программирования как оборудования (оборудование – контроллер SDN), так и приложений (API — контроллер SDN);
- динамическая реакция на изменения в сети;
- оптимизация передачи трафика (L2/3) через большее количество резервных путей;
- эффективная настройка сети;
- существенное сокращение времени развертывания приложений на сетевой инфраструктуре;
- упрощение и типизация управления сетевыми устройствами;
- сокращение стоимости владения оборудованием и затрат на управление подсетями;
- централизованное применение политик маршрутизации и безопасности, увеличение средней пропускной способности и производительности сети;
- простота управления: производится управление целыми сетями, а не сетевыми устройствами;
- открытые, основанные на стандартах протоколы, обеспечивающие взаимодействие различного сетевого оборудования между собой;
- контроллер SDN, поддерживающий открытый интерфейс программирования (API), который позволяет программировать его извне, создавая среду для автоматизации и контроля, а также масштабировать функционал для будущих и перспективных приложений;
- возможность для приложений запрашивать определенные требования к сети;
- видимость и подконтрольность всего трафика сети контроллеру SDN.

Помимо возможностей классического управления сетью прямыми командами системного адми-

нистратора к контроллеру, контроллер SDN поддерживает запуск на своих вычислительных ресурсах приложений управления сетью.

Каждое SDN-приложение представляет собой интерфейс для управления сетью и ее оптимизации под конкретное бизнес-приложение (к примеру Microsoft Lync), и его основная роль — изменение сети в реальном времени под текущие нужды обслуживаемой программы. В случае Microsoft Lync это может быть, к примеру, изменение качества сети (QoS) между двумя абонентами для передачи HD видеозвонка в реальном времени без задержек или создание VPN тоннеля между двумя абонентами.

Таким образом, программно-определяемые сети [2] — это сетевая парадигма, обеспечивающая динамическую, гибкую и программно эффективную конфигурацию сетей для оптимизации сетевого контроля и управления посредством разделения команд управления и данных.

При этом SDN можно разделить на три основных архитектурных уровня:

- уровень инфраструктуры, представляющий собой совокупность сетевого оборудования (различные сетевые коммутаторы, маршрутизаторы, механические переключатели для линий связи и т. д.), непосредственно обеспечивающие передачу сетевых данных;
- уровень управления, который непосредственно реализует функции по централизованному управлению сетевым оборудованием, в том числе построением и конфигурацией маршрутов передачи данных в режиме реального времени, в том числе по командам оператора и в автоматизированном режиме в зависимости от автоматического определения контроллером реализации заранее установленных иных событий (повышенная нагрузка на определенные сегменты сети, аварийные события и необходимость резервирования и т.д.);
- уровень приложений, представляющих собой набор приложений, для обеспечения функционирования которых необходимо использование сетевой инфраструктуры.

Уровень управления в SDN-сети выполняет связующую функцию между уровнем инфраструктуры и уровнем приложений, поскольку, с одной стороны, данный уровень предназначен для централизованной и автоматизированной балансировки сетевой нагрузки на инфраструктурном уровне в зависимости от частоты запросов приложений, а с другой стороны — позволяет ограничивать и оптимизировать частоту запросов пользовательских приложений при повышенной нагрузке на сетевую

инфраструктуру или ее недоступности.

Интерфейс взаимодействия уровней инфраструктуры и управления SDN-сети принято называть южным интерфейсом (от англ. Southbound Interface), а интерфейс взаимодействия уровней управления и приложений SDN-сети принято называть северным интерфейсом (от англ. Northbound Interface). Для реализации южного интерфейса используются

специализированные интерфейсы SDN-протоколов, например, наиболее распространенный интерфейс — OpenFlow API (существуют и другие аналогичные SDN-интерфейсы). Для северного интерфейса обычно реализуют совместимые с конкретными пользовательскими приложениями различные REST API интерфейсы. Схематичное изображение типовой архитектуры SDN-сети представлено на рис. 1.

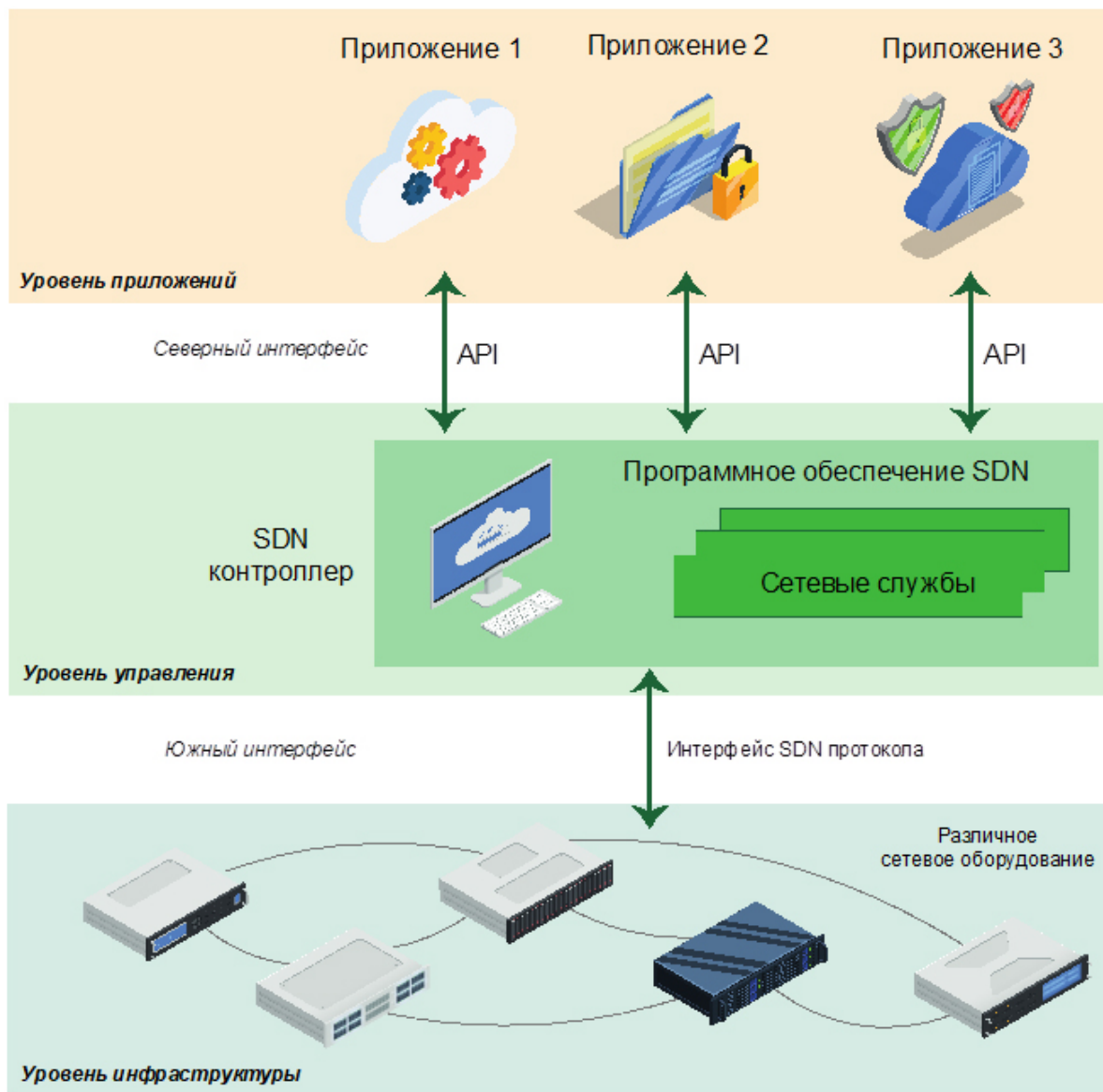


Рис. 1. Типовая архитектура SDN сети

С одной стороны, SDN предоставляет решения для клиентов с высокими запросами к сети, управляя непредсказуемыми схемами трафика данных и обеспечивая быструю реконфигурацию сети. Кроме того, технология может использоваться для повышения уровня сетевой виртуализации и безопасности.

С другой стороны, SDN подвержена не только многим традиционным угрозам сетевой безопас-

ности, но и вводит новые уязвимости в системе безопасности, в первую очередь из-за своей логически централизованной инфраструктуры и функций управления. Весьма важной угрозой является возможность запуска приложений на контроллере SDN.

Все эти факторы на новом уровне актуализируют проблему доверенности и защищенности телекоммуникационных систем, обозначая целый на-

бор новых угроз на всех этапах жизненного цикла SDN-сети.

ТИПИЗАЦИЯ УГРОЗ ДЛЯ SDN-СЕТЕЙ

В соответствии с [2] можно выделить следующие основные классы атак на SDN-сети:

- атаки непосредственно на SDN-контроллер (в том числе, использующие ошибки и уязвимости в операционной среде и приложениях контроллера);
- атаки на управляемые контроллером SDN устройства;
- атаки на каналы взаимодействия контроллера и управляемых им устройств;
- атаки, связанные с восстановлением конфигурации сети по косвенной информации (например,

- по времени прохождения пакетов);
- атаки, связанные с подменой или имитацией управляемых устройств с локальным или удаленным доступом к ним;
- атаки, связанные с работой пользователей SDN-сети;
- атаки, связанные с уязвимостью протоколов работы управляющих приложений с SDN-контроллером.

В статье [2] также была предложена более детальная классификация атак на SDN-сети с разделением возможных видов атак по архитектурным уровням SDN-сетей, на которые может быть оказано воздействие. Адаптация предложенной в данной работе классификации угроз для разных архитектурных уровней SDN-сетей представлена в таблице 1.

Таблица 1

Классификация угроз для разных архитектурных уровней SDN сетей

Уровень SDN сети	Описание атаки	Возможные последствия атаки
Приложения	Получение полного контроля над пользовательским приложением	Получение полного контроля над приложением, прекращение его функционирования
	Использование вредоносного пользовательского приложения	Формирование запросов для выполнения системных команд SDN-сети (некорректные запросы, поиски бэкдоров или DdoS атак через северный интерфейс)
	Воздействие на сетевые службы	Манипуляция содержимым IP-пакетов каналов сетевых служб, нарушение их целостности, доступности и/или конфиденциальности, возможность подмены реализующего приложение сетевого устройства и т. д.
	Эксплуатация уязвимостей северного интерфейса	Использование уязвимостей API для воздействия на пользовательское приложения, нарушения конфиденциальности, целостности и доступности канала взаимодействия SDN-контроллера и приложения
Управление	Обход межсетевых экранов интерфейсов	Отправка несанкционированных сообщений через межсетевой экран с целью дальнейшей эксплуатации уязвимостей SDN-контроллера или нарушение его доступности
	Заражение SDN контроллера	Отправка сторонних запросов на SDN-контроллер для получения информации о конфигурации SDN-сети с возможным дальнейшим изменением конфигураций сети (например, получение информации и изменение конфигурации сети при создании сторонних LLDP запросов)
	Перехват местоположения хоста	Установление сетевого адреса хоста для организации сетевой подмены SDN-контроллера для получения контроля над сетевым взаимодействием контроллера
	Эксплуатация уязвимостей сетевой операционной системы	Использование неправильных конфигураций SDN-контроллера, принудительное завершение работы контроллера, перенаправление информационных потоков контроллера, подмена входных данных для перевода контроллера в непредсказуемое состояние
	Засорение информационных каналов контроллера	Широковещательная рассылка ip-пакетов с искаженными форматами данных для искажения таблицы коммутации или обеспечения недоступности южного интерфейса SDN-контроллера

Уровень SDN сети	Описание атаки	Возможные последствия атаки
Управление	Искажение данных о состоянии сетевого оборудования, управляемого SDN-контроллером	Подделка информационных сообщений от сетевого оборудования для предоставления контроллеру необъективной информации о состоянии, режиме работы и конфигурации сетевого оборудования, что приводит к снижению производительности SDN-контроллера и сетевой инфраструктуры (вплоть до полного отказа)
	Вывод из строя отдельного сетевого устройства	Воздействие на часть ПО в конкретном сетевом устройстве, отвечающая за взаимодействие с SDN контроллером и выполнение его команд, например, при подмене направляемых устройству таблиц коммутации и переводу устройства в неконтролируемое состояние
	Подслушивание информационных каналов SDN контроллера	Нарушение конфиденциальности и целостности данных информационных каналов SDN контроллера (в особенности южного интерфейса) при отсутствии их криптографической защиты или при ненадежной криптографической защите
	Атака человек посередине	Реализация атаки человек посередине для интерфейсов SDN-контроллера (в особенности южного интерфейса)
Инфраструктура	Реализация DoS/DDoS атаки	Обеспечение потери связи между одним или несколькими сетевыми устройствами, что приводит к недоступности сегмента сети
	Перехват контроля над сетевым устройством	Получение данных для обеспечения идентификации и аутентификации SDN-контроллера в сетевом устройстве, использование этих данных для подключения устройства к стороннему (нелегитимному) SDN-контроллеру
	Искажение входных данных канала взаимодействия с SDN-контроллером	Искажение команд управления или внедрение ложных управляющих команд, поступающих непосредственно на конкретное сетевое устройство для обеспечения его нестабильной или некорректной работы
	Искажение выходных данных управляющего канала сетевого оборудования	Искажение данных о состоянии сетевого оборудования или его запросов SDN-контроллеру. Увеличение времени отклика сетевого устройства путем увеличения сетевой задержки или обеспечения потери части ip-пакетов, что приводит к снижению стабильности работы сетевого устройства
	Атака с использованием побочных каналов	Осуществление атаки с использованием побочных каналов для получения сведений, позволяющих реализовать другие атаки на сетевое оборудование или SDN-контроллер

При адаптации технологии SDN для использования в российском телекоммуникационном сегменте необходимо учитывать следующие дополнительные угрозы и риски, связанные со следующими факторами:

- недоверенность операционной среды и приложений SDN-контроллеров зарубежного производства;
- потенциальное наличие каналов скрытого воздействия на SDN-контроллер и управления им, заложенных недружественным производителем и поставщиком;
- обновление ПО контроллера SDN и управляе-

мых устройств (возможность внедрения разрушающих и перехватывающих программных воздействий при обновлении ПО);

- техническое обслуживание аппаратной и программной компоненты контроллеров SDN и управляемых устройств зарубежными специалистами;
- использование зарубежных криптографических алгоритмов на каналах управления и передачи данных (угроза применения недостаточно стойких криптографических алгоритмов, несовершенных или уязвимых протоколов аутентификации, несовершенных или специально ослабленных алгоритмов выработки, хранения и обмена ключами);

- угрозы, связанные с ремонтом (в том числе и гарантийным обслуживанием) и заменой оборудования.

НОВЫЕ ПОДХОДЫ К ФОРМУЛИРОВАНИЮ МОДЕЛЕЙ УГРОЗ

Принципиально новым шагом в теории и практике компьютерной безопасности стало появление документа «Методика оценки угроз безопасности информации» (документ ФСТЭК вступил в действие с 05.02.2021) [3].

В рамках разработки моделей угроз безопасности информации для SDN-сетей необходимо решить следующие задачи:

а) определить негативные последствия, которые могут наступить от реализации (возникновения) угроз безопасности информации в SDN-сетях;

б) провести инвентаризацию ресурсов реальной SDN-сети и определить возможные объекты воздействия угроз безопасности информации;

в) определить источники угроз безопасности информации и оценить возможности нарушителей по реализации угроз безопасности информации;

г) оценить способы реализации (возникновения) угроз безопасности информации в SDN-сети;

д) оценить возможности реализации (возникновения) угроз безопасности информации и актуальность угроз безопасности информации для SDN-сети конкретной конфигурации;

е) оценить сценарии реализации угроз безопасности информации в SDN-сетях, сопряженных системах и обслуживаемых клиентских устройствах.

В соответствии с [4] в настоящее время отменена «Методика определения угроз для ИСПДн 2008 года». Важно заметить, что документ [3] не рассматривает угрозы утечки по техническим каналам и не является предметом моделирования техногенных угроз.

Согласно статистике [4] 67 % документов, направляемых в ФСТЭК, возвращаются на доработку. Даются следующие типовые замечания по рассмотрению регулятором (ФСТЭК) моделей угроз безопасности информации:

- не в полном объеме определяются негативные последствия для видов (рисков) ущерба, а также объекты воздействия;

- не оцениваются объективно и адекватно виды нарушителей, которые могут реализовывать угрозы безопасности информации.

Важным моментом является то, что внутренние пользователи не признаются актуальными нару-

шителями. Для SDN-сетей это замечание особенно важно.

Кроме того, не в полном объеме рассматривается описание сценариев реализации угроз безопасности информации.

В том случае, если для реализации информационно-телекоммуникационной инфраструктуры центра обработки данных, на которой размещается государственная информационная система или объект КИИ, используется технология SDN, оценка угроз безопасности для данного вида сетей должна быть сопряжена с категорированием всего объекта и согласованием с регулятором не только моделей угроз и нарушителя, но и всего комплекса мер реализации системы информационной безопасности.

ПРИМЕНЕНИЕ ТЕХНОЛОГИИ ПОСТРОЕНИЯ SDN-СЕТЕЙ В ЗАДАЧАХ РАЗРАБОТКИ КВАНТОВЫХ СЕТЕЙ

Одним из перспективных направлений для применения технологии построения SDN-сетей являются активно развивающиеся в настоящий момент квантовые сети. В настоящий момент в России появились несколько пилотных участков квантовых сетей. Однако технология построения квантовых сетей требует проведения дальнейших исследований для решения целого ряда задач, к числу которых относятся задачи эффективного управления квантовыми сетями.

В настоящее время многие параметры сетевого оборудования, входящего в состав квантовых сетей, задаются при первичной настройке сети и остаются постоянными в процессе работы, при этом любое изменение посредством системы управления хоть и может осуществляться централизованно, но требует ручных действий со стороны администратора.

При разработке отдельных пилотных участков квантовых сетей и их эксплуатации необходимость внесения ручных действий при управлении не является существенной проблемой. Однако количество необходимых для администрирования параметров будет существенно возрастать при масштабировании данной технологии и появлении большего числа участков квантовых сетей, увеличении числа абонентов квантовых сетей, а также при обеспечении межвендорного взаимодействия для сегментов квантовых сетей, выполненных на разном оборудовании.

В таком случае применение технологии SDN для решения задач управления квантовыми сетями сможет обеспечить возможность автоматизирован-

ного принятия решений реконфигурации квантовых сетей, что в свою очередь создаст условия для построения масштабируемых квантовых сетей как магистрального, так и городского масштаба.

К наиболее очевидным сценариям применения технологии SDN в задачах управления квантовыми сетями можно отнести:

- управление коммутацией каналов в абонентской сети топологии «звезда» для поочередного соединения абонентских модулей системы квантового распределения ключей (КРК) с модулем КРК, расположенным в центральном узле;

- резервирование каналов связи при регистрации попыток вмешательства в квантовый канал или обрыва линий связи, посредством которых реализован квантовый канал;

- оптимизацию и резервирование маршрутов распределения квантово-защищенных ключей (КЗК) при наличии в квантовой сети альтернативных маршрутов между целевыми узлами квантовой сети при обрыве квантового канала на отдельных участках квантовых сетей или выходе из строя оборудования, обеспечивающего формирование КЗК.

Помимо применения технологии SDN для управления устройствами, отвечающими за сетевую маршрутизацию или коммутацию квантовых каналов, можно выделить задачи, связанные с автоматическим управлением криптографическими средствами, обеспечивающими формирование КЗК. В частности, при существенном увеличении числа абонентов в квантовой сети может возникнуть необходимость в динамическом формировании виртуальных каналов между сетевыми устройствами с возможностью управления параметрами данных каналов, например, их пропускной способностью.

Первые работы, показывающие возможность применения технологии SDN для квантовых сетей, были представлены различными научными группами, а в настоящий момент данный вопрос является предметом стандартизации Европейского института телекоммуникационных стандартов. Однако для

применения данной технологии, помимо решения актуальных угроз безопасности для самой технологии SDN, должны быть учтены новые угрозы, связанные с конкретными сценариями интеграции данной технологии в квантовые сети.

ЗАКЛЮЧЕНИЕ

В статье рассмотрены как типовые угрозы, характерные для всего круга управляемых телекоммуникационных сетей, так и специфические угрозы для сетей SDN.

Авторы также полагают, что квантовые технологии позволяют принципиально усилить защищённость SDN-сетей за счёт следующих свойств: доверенности системы квантового распределения ключей и возможности реализовать всю платформу SDN как консистентную (однородную) и замкнутую путем формирования квантовых зашифрованных каналов для каждого узла, а также использования аппаратных решений, включая квантовые датчики случайных чисел.

Предлагается ориентироваться на создание полностью доверенных и импортозамещенных реализаций сетей с использованием сертифицированной операционной среды для контроллера и узлов с применением преимущественно отечественных СКЗИ.

Кроме того, предлагается реализовать механизмы изолированной программной среды для контроллера SDN, что поднимет уровень безопасности и свойств сети до теоретически гарантированного.

Весьма актуальной и серьёзной является и проблема анализа корректной работы приложений для контроллера SDN, для решения которой авторы предлагают создать консорциум, включающий Национальный технологический центр цифровой криптографии (НТЦ ЦК) и Институт точной механики и оптики (ИТМО).

СПИСОК ЛИТЕРАТУРЫ

1. Сетевые технологии SDN – Software Defined Networking. URL: <https://habr.com/ru/companies/muk/articles/251959/> (дата обращения: 12.05.2023)
2. Rahouti M., Xiong K., Xin Y., Jagatheesaperumal S.K., Ayyash M., Shaheed M. SDN Security Review: Threat Taxonomy, Implications, and Open Challenges // IEEE Access, vol. 10. 2022. P. 45820-45854. doi: 10.1109/ACCESS.2022.3168972.
3. Методика оценки угроз безопасности информации. URL: <https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g> (дата обращения: 12.05.2023)
4. Гефнер И.С. Практика реализации методики оценки угроз безопасности информации. URL: https://www.tbforum.ru/hubfs/TBF/2022/Presentations_LIVE/Гефнер_TBF_2022_hall4_1602.pdf?hslang=ru (дата обращения: 12.05.2023).

УДК: 004.75, 004.41

Методы оптимизации структуры квантовых сетей для обеспечения централизованного управления ключами

A.A. Santev

Methods for Optimizing the Structure of Quantum Networks to Ensure Centralized Key Management

Abstract. In this paper, we consider the problem of optimizing the structure of quantum networks to ensure centralized key management when integrating quantum networks with large-scale information systems using the example of a set of Internet of things devices. Solving the problem of ensuring the security of digital services using methods for constructing quantum networks can both modernize the methods for constructing quantum networks and expand the scenarios for their use, and offer quantum-resistant methods for protecting communication channels in Internet of Things systems. The proposed structure based on a quantum network as part of a key management server will significantly increase security in the formation and storage of keys.

Keywords: quantum key distribution, quantum-protected key, cryptographic information security tool, module for trusted storage of user keys, Internet of things device.

A.A. Сантьев

Инженер лидирующего исследовательского центра «Национальный центр квантового интернета» Университета ИТМО, научный сотрудник ООО «СМАРТС-Кванттелеком»
E-mail: aasantev@itmo.ru

Аннотация. В настоящей работе рассматривается задача оптимизации структуры квантовых сетей для обеспечения централизованного управления ключами при интеграции квантовых сетей с масштабными информационными системами на примере набора устройств интернета вещей. Решение проблемы обеспечения безопасности цифровых сервисов с использованием методов построения квантовых сетей способно как модернизировать методы построения квантовых сетей и расширить сценарии их применения, так и предложить квантово-стойкие методы защиты каналов связи в системах интернета вещей. Предлагаемая структура на базе квантовой сети в составе сервера управления ключами существенно повысит безопасность при формировании и хранении ключей.

Ключевые слова: квантовое распределение ключей, квантово-защищенный ключ, средство криптографической защиты информации (СКЗИ), модуль доверенного хранения пользовательских ключей, устройство интернета вещей.

ВВЕДЕНИЕ. АКТУАЛЬНОСТЬ РАССМАТРИВАЕМОЙ ТЕХНИЧЕСКОЙ ЗАДАЧИ

В настоящий момент активное развитие получает технология квантового распределения ключей, с использованием которой реализуются квантовые сети на основе доверенных промежуточных узлов. На данном этапе развития технологий построения квантовых сетей был опубликован ряд международных стандартов в рамках деятельности Международного союза электросвязи [1] и Европейского института телекоммуникационных стандартов [2], а также ожидается публикация проектов отечественных стандартов и методических рекомендаций, однако актуальные исследовательские задачи в части методов построения квантовых сетей остаются и по сей день.

В многоуровневой структуре квантовых сетей можно выделить три основных вида устройств [3,4]:

- модули квантового распределения ключей

(далее – модули КРК), обеспечивающие выработку квантовых ключей (далее – КК) для СКЗИ-Распределителей;

- СКЗИ-Распределители, выполняющие функции по формированию квантово-защищенных ключей (далее- КЗК) и управлению их жизненным циклом;

- СКЗИ-Потребители, являющиеся потребителями КЗК и сопряженные с СКЗИ-Распределителями.

Данная структура квантовой сети позволяет выполнять базовый функционал, заключающийся в выдаче КЗК СКЗИ-Потребителям, однако имеет ряд характерных недостатков:

- СКЗИ-Распределители выполняют полный жизненный цикл по формированию КЗК, в том числе формирование исходных криптографических ключей (компонент итогового КЗК) и хранение сформированного КЗК до востребования СКЗИ-Потребителями, в силу чего компрометация КЗК возможна при воздействии на один из СКЗИ-Потребителей, так как не обеспечивается централизованное надежное формирование и хранение КЗК в отдельных

доверенных аппаратных модулях безопасности и централизованное управление жизненным циклом КЗК;

– запрос и выдача КЗК осуществляется в один короткий промежуток времени для одной пары СКЗИ-Потребителей, синхронизирующих свои запросы к СКЗИ-Распределителям, с которыми они сопряжены, в силу чего каждый СКЗИ-Потребитель должен направлять отдельные запросы для получения парных ключей, соответствующих разным парным СКЗИ-Потребителям;

– формирование криптографического контейнера для выдачи КЗК осуществляется с использованием общего криптографического ключа, известного каждой конкретной паре СКЗИ-Распределителя и СКЗИ-Потребителя, в силу чего возможно обеспечение взаимодействия СКЗИ-Потребителя только с определенными СКЗИ-Распределителями, с которыми есть общий ключ.

Перечисленные недостатки могут повлиять на масштабируемость квантовых сетей при их интеграции с масштабными информационными системами, которые включают большое число разнородных устройств, которым требуется получение ключей для криптографической защиты каналов связи и которые имеют многоуровневую иерархическую структуру.

Наиболее ярким примером таких систем являются системы интернета вещей со значительно возрастающим числом подключенных абонентов – устройств интернета вещей (далее – УИВ), которые в общем случае могут быть подвижными и большую часть времени находиться на значительном удалении от узлов квантовых сетей, при котором невозможно установление соединения с ними для получения КК или КЗК.

В связи с этим возникает необходимость разработки архитектуры безопасности систем интернета вещей, в основе которой обеспечение безопасности цифровых сервисов реализуется с использованием методов построения квантовых сетей. Решение данной проблемы способно как модернизировать методы построения квантовых сетей и расширить сценарии их применения, так и предложить квантово-стойкие методы защиты каналов связи в системах интернета вещей.

В настоящей работе предлагаются методы оптимизации структуры квантовых сетей для реализации централизованной инфраструктуры управления ключами при интеграции квантовых сетей с масштабными информационными системами. Рассматриваемые методы заключаются в уточнении состава платформы, которая включает набор УИВ,

квантовую сеть и сервер управления ключами (в состав которого также входит один из узлов квантовой сети), выполняющий функционал по управлению жизненным циклом симметричных ключей, выдаваемых СКЗИ-Потребителям в составе УИВ.

1. ПРЕДЛАГАЕМЫЙ СОСТАВ ПЛАТФОРМЫ НА БАЗЕ КВАНТОВОЙ СЕТИ

Предлагается выделить следующие элементы платформы:

– узлы квантовой сети (далее – УКС), посредством которых осуществляется ключевой транспорт для выдачи ключей. В состав УКС входят модули КРК, сопряженные с СКЗИ-Распределителями;

– УИВ, являющиеся потребителями ключей. В состав УИВ входят СКЗИ-Потребители, взаимодействующие с СКЗИ-Распределителями в составе УКС;

– сервер управления ключами, обеспечивающий реализацию функций по управлению жизненным циклом ключей, генерируемых и используемых в составе платформы.

В составе сервера управления ключами предлагается выделить следующие элементы платформы:

– сервер аутентификации и криптографических сервисов (далее – САКС), посредством которого осуществляется аутентификация УИВ и обработка запросов УИВ на предоставление ключей, а также аутентификация СКЗИ-Распределителей, входящих в состав УКС, с которыми происходит взаимодействие САКС в рамках функционирования платформы;

– модуль доверенного хранения пользовательских ключей (далее – МДХПК), осуществляющий управление жизненным циклом ключей (формирование, хранение, выдача в защищенном виде, стирание);

– центр регистрации (далее – ЦР) УИВ, в котором осуществляется первичная регистрация УИВ. ЦР может представлять собой центр выработки первичных парно-выборочных ключей (далее – ЦВК) и автоматизированное рабочее место (АРМ), формирующий ID для регистрируемых УИВ. В общем случае в составе платформы может быть несколько ЦВК и АРМ с общей распределенной базой данных, наделенных правами на регистрацию УИВ в составе платформы;

– центр управления конфигурацией платформы (далее – ЦУКП), в котором осуществляется управление статусом тех или иных симметричных ключей (активация и деактивация), полученных УИВ от УКС. Как следствие, возможно управление статусом сое-

динений между УИВ в рамках платформы.

В настоящей работе рассматривается пример функционирования платформы на базе квантовой сети, состоящей из пяти УКС. При этом в рассматриваемом случае УКС₃ сопряжен с составными частями сервера управления ключами, к которым относятся САКС, МДХПК, ЦР и ЦУКП, что необходимо для осуществления передачи ключей от данных элементов платформы к точкам подключения УИВ. В общем случае САКС, МДХПК, ЦР и ЦУКП необходимо рассматривать как отдельные устройства. Точками подключения УИВ для выдачи ключей должны являться непосредственно УКС, но не обязательно все УКС – в структуре квантовой сети могут быть выделены целевые УКС, обеспечивающие выдачу ключей потребителям, и промежуточные УКС, обеспечивающие только передачу ключей до целевых УКС. В рассматриваемом в работе примере целевыми УКС являются УКС₁ и УКС₅, а УКС₂ и УКС₄ являются промежуточными УКС, обеспечивающими трансфер КЗК от УКС₃ до УКС₁ и УКС₅.

2. ЭТАП ПРЕДВАРИТЕЛЬНОГО ФОРМИРОВАНИЯ КЛЮЧЕЙ В КВАНТОВОЙ СЕТИ

На данном этапе функционирования платформы осуществляется формирование КК между УКС.

В таком случае будут сформированы следующие КК:

- КК₁₂ между УКС₁ и УКС₂;
- КК₂₃ между УКС₂ и УКС₃;
- КК₃₄ между УКС₃ и УКС₄;
- КК₄₅ между УКС₄ и УКС₅;

После формирования КК также осуществляется формирование КЗК между УКС₃, который сопряжен с элементами платформы, и двумя целевыми УКС:

- КЗК₁₃ между УКС₁ и УКС₃;

- КЗК₃₅ между УКС₃ и УКС₅.

Данные КЗК являются служебными КЗК, так как впоследствии будут использоваться только для передачи служебной информации УКС, между которыми они сформированы. В УКС₃ за хранение данных КЗК отвечает САКС.

Диаграмма последовательности этапа предварительного формирования ключей в квантовой сети представлена на рис. 1.

3. РЕГИСТРАЦИЯ УСТРОЙСТВ В СОСТАВЕ ПЛАТФОРМЫ НА БАЗЕ КВАНТОВОЙ СЕТИ

Процесс регистрации УИВ представляет собой следующую последовательность действий и процедур:

1. Регистрируемый УИВ направляет ЦР запрос на его регистрацию в составе платформы;

2. ЦР формирует для регистрируемого УИВ уникальный ID, а также симметричный ключ защиты интерфейса получения ключей, обозначаемый КХ_i, для регистрируемого УИВ. В формируемый набор входят парные ключи для УИВ и каждого из целевых УКС, к которым данному УИВ разрешено обращаться для получения ключей. Число таких узлов может задаваться непосредственно в ЦР при регистрации. Каждый из ключей набора имеет также собственный уникальный идентификатор. Также УИВ формирует симметричный ключ аутентификации KAuth_i, посредством которого будет осуществляться аутентификация УИВ при его взаимодействии с такими элементами платформы как САКС и ЦУКП (в более общем случае для взаимодействия УИВ с САКС и ЦУКП могут быть сформированы отдельные ключи аутентификации).

3. Сформированные для УИВ уникальный ID, первичный ключ защиты интерфейса получения ключей

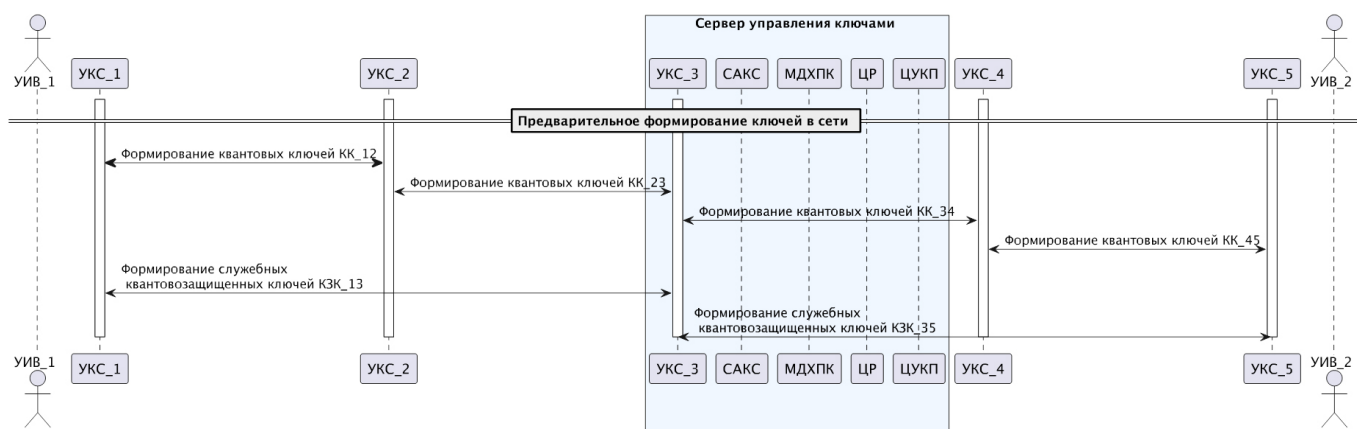


Рис. 1. Диаграмма последовательности этапа предварительного формирования ключей в квантовой сети

чей KX_i и ключ аутентификации $KAAuth_i$ передаются УИВ в доверенной зоне ЦР в открытом виде или вне доверенной зоны ЦР с защитой на пароле, полученном альтернативным каналом передачи информации (доставка смарт-карты с паролем и т.д.).

4. После подтверждения со стороны УИВ получения уникального ID, набора первичных парных ключей защиты интерфейса KX и ключа аутентификации $KAAuth_i$ осуществляется занесение уникального ID и ключа KX_i в МДХПК, а в САКС и ЦУКП осуществляется передача уникального ID УИВ и ключа $KAAuth_i$.

Данная процедура регистрации УИВ применяется по отношению ко всем УИВ.

4. ФОРМИРОВАНИЕ МАТРИЦЫ ПАРНЫХ КЛЮЧЕЙ УСТРОЙСТВ В СОСТАВЕ ПЛАТФОРМЫ НА БАЗЕ КВАНТОВОЙ СЕТИ

Перед рассмотрением процедуры запроса ключей со стороны УИВ при взаимодействии с одним из целевых УКС необходимо описать процедуру формирования матрицы парных ключей УИВ KZK^{matrix} , осуществляемую МДХПК. В обозначении матрицы используется аббревиатура КЗК, поскольку входящие в состав данной матрицы ключи в дальнейшем будут передаваться по цепочке УКС так же, как и исходные ключи для формирования КЗК передаются по цепочке УКС в известных схемах формирования КЗК.

При генерации матрицы парных ключей УИВ KZK^{matrix} для определения количества ключей, вхо-

дящих в данную матрицу, необходимо исходить из числа уже зарегистрированных в составе платформы УИВ и числа УИВ, которые потенциально могут быть зарегистрированы в составе платформы за время жизни генерируемых ключей (за время, по истечении которого УИВ придется обращаться к УКС для получения новых ключей).

В рассматриваемом случае предположим, что в момент времени генерации матрицы парных ключей всех УИВ KZK^{matrix} в составе платформы уже зарегистрировано n УИВ, и каждый УИВ имеет порядковый номер от 1 до n : $УИВ_1, УИВ_2, УИВ_3, \dots, УИВ_n$. Также предположим, что в составе платформы дополнительно может быть зарегистрировано j УИВ, при этом каждый из этих УИВ будет иметь порядковый номер $УИВ_{n+1}, УИВ_{n+2}, \dots, УИВ_m$, где $m=n+j$.

Каждая строка матрицы парных ключей УИВ $KZK_{ID_{УИВ}}^{matrix}$ должна содержать набор ключей, предназначенный для одного УИВ, и включать в себя набор парных ключей данного УИВ с каждым из уже зарегистрированных УИВ ($n-1$ ключей) и УИВ, которые потенциально могут быть зарегистрированы в составе платформы (j ключей).

Рассмотренное предварительное формирование матрицы парных ключей УИВ позволит избежать необходимости обращения УИВ для получения ключа, сформированного для данного УИВ и парного ему УИВ, поскольку назначенные разным УИВ ключи уже содержатся в строке матрицы, предназначенной конкретному УИВ. Диаграмма последовательности для этапа формирования матрицы парных ключей УИВ показана на рис. 2.

Структура матрицы парных ключей УИВ показана на рис. 3.



Рис. 2. Диаграмма последовательности этапа формирования матрицы парных ключей УИВ

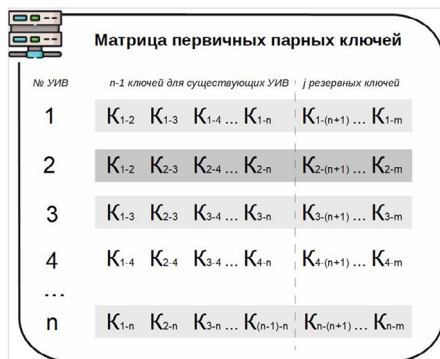


Рис. 3. Структура матрицы парных ключей УИВ

5. ПРОЦЕДУРА ЗАПРОСА И ВЫДАЧИ КЛЮЧЕЙ УСТРОЙСТВАМ ПЛАТФОРМЫ НА БАЗЕ КВАНТОВОЙ СЕТИ

При запросе ключей УИВ должен обратиться к одному из целевых УКС, к которому ему было разрешено обращаться при регистрации в ЦР. В общем случае перечень разрешенных целевых УКС может меняться (расширяться или уменьшаться) и после регистрации УИВ, путем рассылки от ЦУКП к УИВ информационных сообщений при изменении перечня разрешенных целевых УКС (целостность данных сообщений может гарантироваться с использованием ключа аутентификации $KAuth_i$, известного УИВ и ЦУКП).

В отличие от традиционного представления процедуры выдачи КЗК в квантовых сетях, когда парным потребителям одновременно выдается один КЗК или набор КЗК, но предназначенный только для данной пары потребителей, в предлагаемом методе осуществляется выдача УИВ (СКЗИ-потребителю в его составе) набора парных ключей, предназначенных для разных пар УИВ, при этом:

- для любых двух УИВ на сети получаемые ими наборы ключей будут отличаться, совпадать в данных наборах будет только ключ, предназначенный для пары из двух рассматриваемых УИВ;

- каждый УИВ может получать предназначенный ему набор ключей вне зависимости от парных УИВ, в любой момент времени, но для использования ключей в паре УИВ каждый УИВ из пары должен получить свой набор ключей.

Процедура запроса парных ключей УИВ со стороны одного из УИВ представляет следующую последовательность действий и процедур:

1. УИВ направляет запрос целевому УКС на получение парных ключей УИВ, содержащий сообщение вида $Key_request = Im(['Request', ID_УИВ], KAuth_i)$, в которое входит информация о запросе и ID запрашивающего УИВ, а также вычисленная на ключе аутентификации УИВ $KAuth_i$ имитовставка;

2. Получивший запрос УКС осуществляет проверку полученного запроса в САКС для его валидации в виде сообщения $Valid_request = Im(Key_request, KZK_j)$, в которое входит непосредственно запрос УИВ и вычисленная для него имитовставка на служебном КЗК (в рассматриваемом случае $j=13$ для УКС₁ и $j=35$ для УКС₃₅);

3. САКС сперва осуществляет аутентификацию УКС, приславшего сообщение валидации, по вычисленной на ключе KZK_j имитовставке, а затем —

аутентификацию запрашивающего ключи УИВ по вычисленной на ключе $KAuth_i$ имитовставке (в более общем случае в этой и дальнейших операциях могут быть использованы другие теоретико-информационные или вычислительно стойкие методы аутентификации).

4. В случае успешного прохождения процедур аутентификации УКС и УИВ САКС отправляет в МДХПК команду на отправку контейнера с ключами в УКС, из которого пришло сообщение валидации (передается ID УИВ и ID целевого УКС, к которому с запросом обратился УИВ). После получения команды МДХПК осуществляет формирование контейнера для строки матрицы парных ключей УИВ $KZK_{ID_УИВ}^{matrix}$, предназначенной соответствующему УИВ, на ключе защиты интерфейса получения ключей KX_i : $Key_container = Enc(KZK_{ID_УИВ}^{matrix}, KX_i)$.

5. Сформированный контейнер МДХПК передает в САКС, который вычисляет имитовставку контейнера $Key_container$ на ключе $KAuth_i$ для аутентификации сообщения с контейнером в УИВ $Key_container_message = Im(Key_container, KAuth_i)$, а также вычисляет имитовставку для сообщения $Key_container_message$ на служебном КЗК_j для аутентификации данного сообщения в целевом УКС: $Valid_response = Im(Key_container_message, KZK_j)$.

6. САКС инициализирует передачу сообщения $Valid_response$ по цепочке УКС до целевого УКС, к которому с запросом обращался УИВ.

7. УКС 1 по имитовставке на KZK_j осуществляет аутентификацию САКС, после чего производит выдачу сообщения $Key_container_message$, которое содержит в себе контейнер $Key_container$ со строкой матрицы парных ключей УИВ $KZK_{ID_УИВ}^{matrix}$.

8. УИВ осуществляет получение строки матрицы парных ключей УИВ, осуществляя аутентификацию САКС по имитовставке, вычисленной на ключе $KAuth_i$, после чего раскрывает контейнер $Key_container$ с использованием ключа защиты интерфейса KX_i , который известен УИВ с момента регистрации в ЦР.

Предложенная структура позволяет исключить доступ входящих в состав УКС СКЗИ-Распределителей к ключам из матрицы KZK^{matrix} , поскольку СКЗИ-Распределители в составе УКС осуществляют передачу только ключевых контейнеров, сформированных для отдельных строчек матрицы парных ключей УИВ $KZK_{ID_УИВ}^{matrix}$. Таким образом, на этапе всего жизненного цикла ключей в открытом виде они доступны только МДХПК и УИВ, для которого они предназначены. Кроме того, формируемые в МДХПК ключевые контейнеры также обеспечивают защиту ключей при их передаче между целевыми УКС

и УИВ (СКЗИ-Распределителем и СКЗИ-Потребителем, входящих в их состав).

Дополнительно может быть использован механизм, в соответствии с которым САКС и СКЗИ-Потребитель в составе УИВ будут формировать производные сеансовые ключи аутентификации и защиты интерфейса между целевым УКС и УИВ, и данные ключи будут передаваться от САКС в УИВ с защитой на служебных КЗК – таким образом будет решена проблема необходимости предварительного распределения парно-выборочных ключей между УКС (СКЗИ-Распределителем в его составе) и УИВ (СКЗИ-Потребителем в его составе), тогда все сообщения в канале между ними будут передаваться с дополнительной защитой, в том числе сформированные ключевые контейнеры на известном только МДХПК и УИВ ключе. Это приводит к тому, что УИВ могут обращаться к произвольному УКС, не имея предварительно распределенного ключа между собой, а в САКС данное соединение будет разрешено или запрещено в зависимости от конфигураций платформы, установленных в ЦУКП.

Предлагаемая структура также позволяет обеспечить разработку МДХПК в виде отдельного аппаратного модуля безопасности, что существенно повысит безопасность при формировании и хранении ключей, предназначенных для УИВ. Кроме того, в более общем случае возможна реализация в рамках одной платформы нескольких МДХПК, в том числе разделенных по иерархическим уровням, где аппаратный МДХПК с более высоким уровнем привилегий сможет агрегировать ключи от остальных МДХПК по каналам связи, защищенным с помощью КК или КЗК.

6. УПРАВЛЕНИЕ КОНФИГУРАЦИЕЙ ПЛАТФОРМЫ НА БАЗЕ КВАНТОВОЙ СЕТИ

По мере получения парных ключей УИВ $KZK_{\text{УИВ}}^{\text{matrix}}$ разными УИВ должно осуществляться информирование УИВ, получивших предназначенные им ключи $KZK_{\text{УИВ}}^i$ ранее, о факте получения парных ключей теми УИВ, с которыми они могут сформировать пары (имеют общий ключ в своих наборах $KZK_{\text{УИВ}}^i$). Функции по информированию должен осуществлять ЦУКП. Данные сообщения можно рассматривать как активацию ключей для конкретной пары УИВ. Аутентификация ЦУКП в УИВ может осуществляться

с использованием ключей $KAAuth_i$ при проверке вычисленных на данных ключах имитовставок для передаваемых сообщений: $Key_activation = \text{Im}([\text{ID_key}_{12}, \text{«Key_status_on»}], KAAuth_i)$.

После того, как УИВ получили сообщения об активации общих для УИВ ключей $KZK_{\text{УИВ}_12}^i$, они могут осуществлять защищенный обмен сообщениями с использованием данных ключей, в том числе формировать производные ключи для их разделения на ключи шифрования и ключи имитовставок, а также разделять ключи на направления их применения: $Message_i = \text{Enc}(\text{Info}_i, KZK_{\text{УИВ}_12}^i)$.

Из ЦУКП можно осуществлять управление статусом уже активированных ключей $KZK_{\text{УИВ}}^i$, рассылая сообщения об их деактивации. Деактивация может осуществляться в соответствии с принятым регламентом функционирования платформы, например при появлении информации о возможной компрометации одного из УИВ, его удалении из состава платформы или при иных сценариях. Информирование о деактивации ключей может осуществляться в виде сообщений, аналогичных сообщениям об активации ключей: $Key_deactivation = \text{Im}([\text{ID_key}_{12}, \text{«Key_status_off»}], KAAuth_i)$.

Важно отметить, что для каждого УИВ может осуществляться деактивация одного или нескольких отдельных ключей, входящих в имеющийся у них набор парных ключей УИВ $KZK_{\text{УИВ}}^i$. При этом другие ключи данного набора могут оставаться активными. При необходимости, после деактивации того или иного ключа может быть возможна его повторная активация. Кроме того, может осуществляться автоматическая деактивация ключей по истечению времени жизни выданных ключей или диагностике иных событий, связанных с УИВ или платформой в целом, или замена деактивированных ключей на резервные ключи, входящие в состав полученной УИВ строки матрицы ключей $KZK_{\text{УИВ}}^i$.

Схематичное изображение примера реализации процедур выдачи предназначенных разным УИВ наборов парных ключей $KZK_{\text{УИВ}}^i$ и управления конфигурацией платформы показаны на рис. 4.

С учетом того, что аутентификацию УИВ и принятие решения о том, разрешено ли запрашивающему ключи УИВ их предоставлять, осуществляет САКС, ему также должны быть известны актуальные сведения о том, каким УИВ из состава платформы разрешено или запрещено обеспечивать выдачу ключей. Для этих целей должно быть обеспечено дополнительное взаимодействие САКС и ЦУКП.

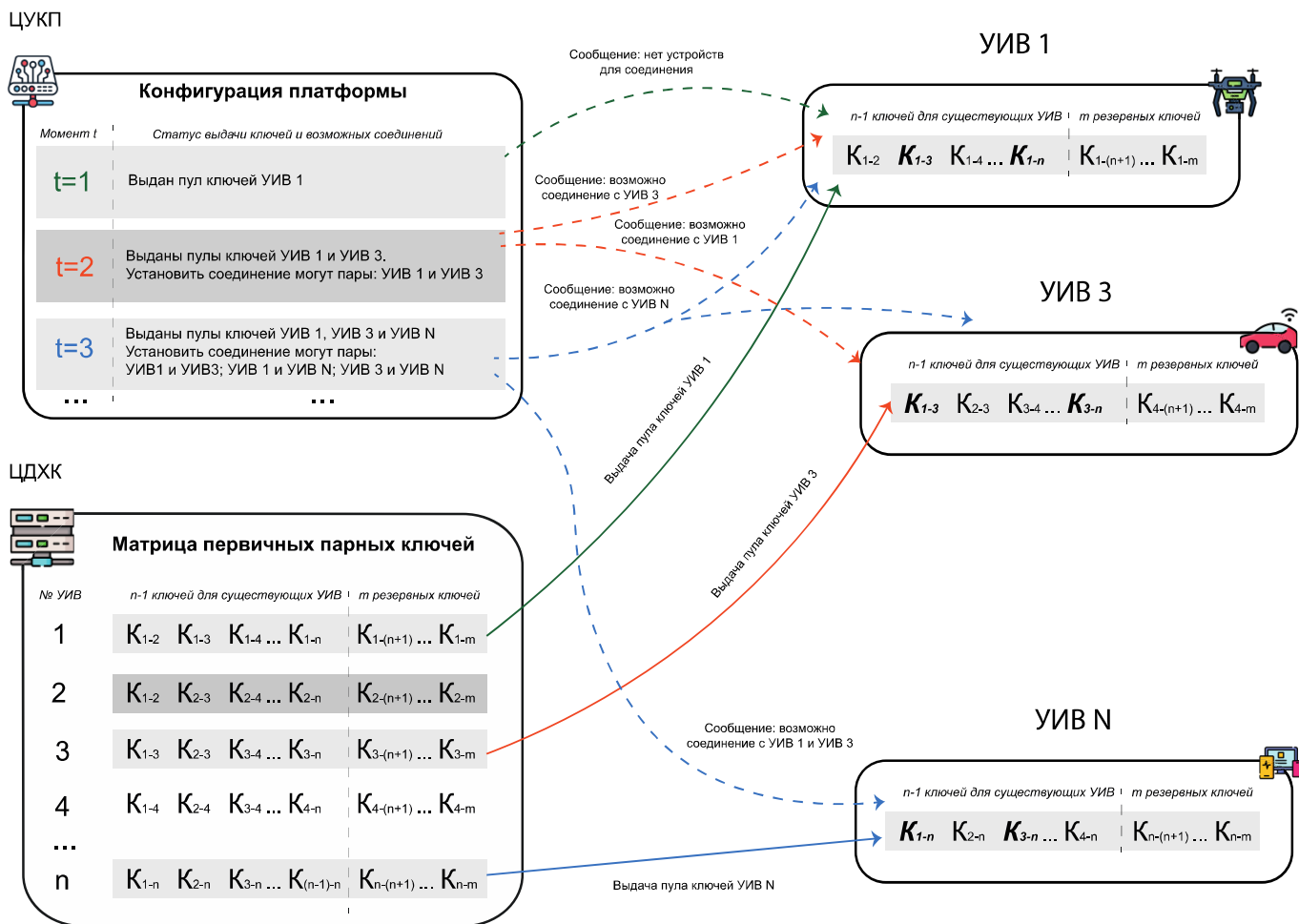


Рис. 4. Пример реализации процедур выдачи предназначенных разным УИВ наборов парных ключей $KZK_{ID_{УИВ}}^i$ и управления конфигурацией платформы

ЗАКЛЮЧЕНИЕ

Предлагаемые методы заключаются в разработке структуры квантовой сети, подразумевающей выделение дополнительных элементов, таких как сервер аутентификации и криптографических сервисов, модуль доверенного хранения пользовательских ключей, центр регистрации и центр управления конфигурацией платформы, а также в разработке с учетом предлагаемой структуры принципов функционирования квантовой сети и устройств, выступающих в роли потребителей выдаваемых квантовой сетью ключей. Данные методы позволяют решить ряд актуальных задач, а именно: перенести функции по формированию и хранению квантово-защищенных ключей (до их передачи по цепочке узлов квантовой сети) в отдельные аппаратные

модули безопасности для исключения взаимодействия СКЗИ-Распределителей в составе узлов квантовой сети с данными ключами в открытом виде, уйти от необходимости направления отдельного запроса каждой парой СКЗИ ключа с синхронизацией этих запросов для их осуществления в один заданный промежуток времени, а также отказаться от необходимости предварительного распределения общих симметричных ключей между конкретной парой СКЗИ-Распределителей и СКЗИ-Потребителей.

Предлагаемая структура может быть применена для обеспечения взаимодействия подвижных устройств интернета вещей с СКЗИ-Потребителем в составе с произвольным узлом квантовой сети с СКЗИ-Распределителем после прохождения процедуры регистрации на платформе, включающей в свой состав квантовую сеть.

СПИСОК ЛИТЕРАТУРЫ

1. International Telecommunication Union (ITU). Y series: Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities. Y.3800-Y.3999: Quantum key distribution network. URL: <https://www.itu.int/rec/T-REC-Y.3800-201910-I/en> (дата обращения: 16.05.2023)
2. Quantum key distribution (QKD); common criteria protection profile - pair of prepare and measure quantum key distribution modules. URL: https://www.etsi.org/deliver/etsi_gs/QKD/001_099/016/01.01.01_60/gs_QKD016v010101p.pdf (дата обращения: 16.05.2023)
3. Верещагина Е.В., Егоров В.И., Сантьев А.А., Хоружников С.Э., Щербаков А.Ю. Современное состояние методологии построения защищенной квантовой сети // Вестник современных цифровых технологий. 2021. № 7. С. 6-14.
4. Жилиев А.Е. Методика построения сетей квантового распределения ключей смешанной топологии: специальность 05.13.19 «Методы и системы защиты информации, информационная безопасность»: диссертация на соискание ученой степени кандидата наук / Жилиев Андрей Евгеньевич; Томский государственный университет систем управления и радиоэлектроники.- Томск, 2022.- 240 с.

УДК: 004.056

Принципы организации безопасного интернета на примере системы TheOoL*

A.V. Nenashev

Principles of Formation a Safe Internet on the Example of System TheOoL

Abstract. The paper proposes the principles of building a private Internet system, including an overlay data transfer protocol, serverless hosting and cloud computing, a serverless search engine, as well as an integrated payment system. The private Internet system is considered on the example of the TheOoL project developed by the author with the support of the Innovation Promotion Fund – a universal distributed decentralized operating system designed to protect distributed computing. TheOoL system isolates private networks over the Internet without limiting the possibility of useful interaction between them. Additional security is provided by built-in subsystems of cryptographic protection and protection against unauthorized access using biometrics. Network interaction management is performed by an innovative protocol for information interaction and topology control based on distributed registry technologies. This system offers the user high performance and total protection of personal data, including the suppression of the user's "digital footprint".

Keywords: peer-to-peer networks, decentralized computing, distributed ledger systems, serverless search engines, serverless access control systems, private internet.

А.В. Ненашев

Доцент Самарского государственного
технического университета,
директор ООО ТХЕООЛ.
E-mail: nenashev.sgtu@rambler.ru

Аннотация. В работе предложены принципы построения системы частного интернета, включающей оверлейный протокол передачи данных, бессерверный хостинг и облачные вычисления, бессерверную поисковую машину, а так же интегрированную систему платежей. Система частного интернета рассматривается на примере разрабатываемого автором при поддержке «Фонда содействия инновациям» проекта TheOoL - универсальной распределенной децентрализованной операционной системы, предназначенной для защиты распределенных вычислений. Система TheOoL изолирует частные сети поверх Интернет без ограничения возможностей полезного взаимодействия между ними. Дополнительную безопасность обеспечивают встроенные подсистемы криптографической защиты и защиты от несанкционированного доступа с применением биометрии. Управление сетевыми взаимодействиями выполняет инновационный протокол информационного взаимодействия и контроля топологии на базе технологий распределенного реестра. Пользователю эта система

предлагает высокую производительность и тотальную защиту персональных данных, включая подавление «цифрового следа» пользователя.

Ключевые слова: одноранговые сети, децентрализованные вычисления, системы распределенного реестра, бессерверные поисковые машины, бессерверные системы управления доступом, частный интернет.

ВВЕДЕНИЕ

Жизнь современного общества невозможно представить себе без интернета, электронной почты и социальных сетей. Компании, занятые в области информационных технологий, разрабатывают и предлагают нам различные сервисы, улучшающие нашу жизнь, реализующие и совершенствующие ее логистику, поставляя на дом все необходимое, начиная от товаров и услуг и заканчивая рабочим местом. Наблюдается устойчивый процесс слияния виртуального пространства интернета и ментального пространства индивидов, наполняющих симу-

лякры виртуального мира реальным содержанием, благодаря чему этот мир становится важной составляющей социально-политической и экономической жизни общества [1].

Работы по внедрению технологий «Индустрии 5.0», ключевыми составляющими которой являются технологии BigData, IoT(Internet of Things) и IoE(Internet of Everything) и адаптивные когнитивные системы, приводят к слиянию виртуального и реального пространства [2, 3]. Здесь вся собранная в физическом пространстве информация в виде Big Data отправляется в киберпространство, анализируется системами искусственного интеллекта (ИИ). ИИ находит оптимальные с его точки зрения решения задач для производственного или финансового про-

* Работа выполнена по заказу TheOoL LLC, Samara, Russia и при содействии «Фонда содействия развитию малых форм предприятий в научно-технической сфере» (Фонд содействия инновациям), Москва, Россия, договор №4716ГС1/79594 от 13.09.2022.

цесса и направляет обратно в физическое пространство [4, 5]. Иначе говоря, широкое применение технологий «Индустрии 5.0», с точки зрения кибербезопасности, потенциально позволяет покушаться через сети общего пользования не только на приватность, но и на физическую безопасность каждого человека, бизнеса и государства.

В современном мире кибербезопасность стала приоритетной задачей человечества. Подтверждает это мнение тот факт, что мировые расходы на информационную безопасность (продукты и услуги) в 2020 году достигли \$138 млрд., ежегодный рост расходов составляет 6% [6]. Существенный вклад в формирование кибер-угрозы вносит общая уязвимость современных сетевых и программных технологий, а так же неконтролируемый сбор и оборот технических и личных сведений в сети [7]. Таким образом, задача сокрытия технической информации о сети, узлах сети и сведений о пользователях сети от злоумышленника приобретает все большую актуальность.

ПРОБЛЕМЫ ПРИВАТНОСТИ И БЕЗОПАСНОСТИ ПОЛЬЗОВАТЕЛЕЙ СЕТИ ИНТЕРНЕТ

Известно, что основные уязвимости сетей, работающих на базе протоколов из стека TCP/IP, заложены при создании системы в 1981 как наследие разработанной еще в 1969 году ARPANet [8-10]. Изначально IP-сети – открытые и децентрализованные с полным отсутствием политики безопасности. В них отправитель идентифицируется исключительно по его IP-адресу, а процедура аутентификации выполняется на этапе соединения – в дальнейшем подлинность принимаемых пакетов не проверяется. Такой подход к реализации сетевого протокола позволяет злоумышленнику анализировать топологию сети, используя, например, Internet Control Message Protocol (ICMP) и Internet Group Management Protocol (IGMP) (Multicast Listener Discovery (MLD) в TCP/IP v6) [9 – 11], за счет прослушивания портов, открытых на узлах сети протоколами и приложениями верхних уровней модели OSI/ISO, определить какие операционные системы и приложения исполняются на конкретных узлах сети, собрать сведения об их аппаратном обеспечении [9, 12]. Сбор такого рода информации позволяет локализовать узлы, потенциально интересные для атаки по принадлежности целевой жертве и/или наличию возможных уязвимостей.

В противоположность сетям большинство современных систем хранения и обработки данных повторяют архитектуру корпораций-пользователей и построены в централизованной архитектуре [13] или имеют центры управления, контроль над которыми

либо вывод их из строя (осуществление атаки типа «отказ в обслуживании») зачастую является основной целью атаки. Перехват контроля осуществляется в основном через программные уязвимости либо с применением методов социальной инженерии, реже – с использованием аппаратных уязвимостей. Очевидно, что в этой ситуации обладание сведениями о принадлежности узлов и их программном и аппаратном обеспечении существенно облегчает задачу потенциального злоумышленника [5, 14, 15].

В целях разрешения противоречия между архитектурой IP сети и потребностями современных информационных систем (ИС) и повышения удобства работы пользователей разработано много программ (ПО), предназначенных для централизации управления сетью и программной инфраструктурой, построения частных сетей и т.п. Каждый программный продукт аккумулирует сведения о работе узлов и пользователей сети и использует эти сведения для облегчения работы ИС и управления сетью. Одновременно со своей основной функцией они имеют собственные «встроенные» уязвимости и существенно усложняют процесс управления ИС, предъявляя повышенные требования к квалификации технического персонала сетей и ИС, что в свою очередь ведет к ошибкам администрирования и существенно повышает вероятность образования уязвимостей ИС при их внедрении [9, 12]. Помимо этого, серверы такого ПО сами представляют собой потенциальный объект атаки.

Поверх сетевых протоколов, операционных систем узлов и всевозможных служб и сервисов надстроено множество узкоспециализированных подсистем кибербезопасности, нацеленных на устранение той или иной уязвимости, либо класса уязвимостей. Такой подход к построению системы киберзащиты современных ИС влечет за собой: проблемы интеграции защитных подсистем с программным обеспечением ИС, общесистемным программным обеспечением и друг другом; многократное снижение производительности ИС; служит источником уязвимостей безопасности информации за счет случайных или преднамеренных ошибок при внедрении и управлении системами безопасности [12, 14, 15].

Таким образом, проблемы безопасности и конфиденциальности данных «генетически» заложены в архитектуре современного интернета. В результате уже привычными стали утечки персональных данных пользователей, взломы хранилищ данных и хищения денежных средств. В 2019 г. облачный сервис Cloud4U подготовил краткий обзор утечек информации [16], согласно которому утечки допустили крупнейшие социальные сети, торговые, финансовые и производственные компании. Крупнейшие поисковые системы благополучно индексируют и предо-

ставляют неограниченный доступ к разглашенной таким образом информации [16, 17].

Несмотря на известные проблемы безопасности сети Интернет продолжается внедрение сервисов IoT и IoE. Повсеместно внедряются системы «умного дома», оснащенные камерами и автоматикой для управления электроснабжением, отоплением и физическим доступом в помещения, в том числе в массовом бюджетном жилье [19]. Автоматические системы для управления объектами повышенной опасности: беспилотный транспорт, промышленные роботы, интегрированные с автоматическими складами, автоматическими логистическими системами, беспилотным транспортом и системами планирования ресурсов предприятия (ERPS) [20, 21]. Это в свою очередь расширяет спектр возможных угроз вплоть до угрозы физической безопасности людей и объектов бытовой и промышленной инфраструктуры.

Сложившаяся ситуация создает предпосылки для нарушения не только таких основных прав человека и гражданина, как неприкосновенность переписки, свобода совести и убеждений, свобода получать и распространять информацию, но и его права на жизнь и здоровье. Данная тенденция порождает спрос на приватность в сети, как со стороны отдельных индивидов, так и организаций различного рода (от технологических и финансовых до политических).

На удовлетворение этого спроса работает несколько десятков команд разработчиков. По нашему мнению, наиболее близко к решению проблемы обеспечения приватности в сети Интернет (в части транспортной подсистемы) подошли разработчики проекта невидимого интернета I2P, который представляет собой оверлейную сеть, функционирующую поверх открытого интернета на базе протоколов TCP/IP. I2P обеспечивает наилучшую среди существующих продуктов анонимность, устойчивость сети за счет одноранговой архитектуры с распределенным хранением метаданных, использования криптографии и алгоритма работы сети, обеспечивающего регулярную смену маршрутов взаимодействия и разделения трафика между входящим и исходящими туннелями. Сам протокол взаимодействия довольно надежен и имеет всего несколько известных уязвимостей, позволяющих компрометировать соединения либо сеть, что может привести к нарушению приватности пользователя [22].

При этом следует отметить, что существующие уязвимости позволяют полностью раскрыть сеть I2P при наличии достаточных вычислительных ресурсов у атакующей стороны. Другим недостатком I2P является фактическое отсутствие готовых пользовательских приложений, позволяющих использовать сеть I2P без специальных технических познаний и неудобно. Поэтому суточная аудитория проекта не превышает 45000 пользователей.

В то же время наиболее популярное техническое решение для анонимного взаимодействия в сети TOR Project имеет ежедневную аудиторию в 1,5 млн. не смотря на большое количество уязвимостей, которые позволяют компрометировать защищенные соединения с использованием относительно небольших вычислительных мощностей [23], хорошо известны заинтересованным пользователям Интернет. Фактически TOR обеспечивает только мнимую приватность, но наличие собственного клиентского приложения TOR – browser, обеспечивающего легкую установку TOR и быстрый доступ к «скрытым» ресурсам привлекают пользователей.

Был проведен анализ популярных анонимных сетей с точки зрения удобства использования. В результате было выявлено несколько проблем. Основная проблема – это медленная относительно «открытого Internet» работа размещенных в этих сетях сайтов, здесь имеется ввиду субъективно медленное открытие даже «легких» html страниц с минимальными размерами графических объектов и отсутствием интерактивной анимации.

Это происходит из-за отсутствия в экосистеме приватного интернета протоколов доверенного приватного хостинга, что делает большинство качественных хостинг-провайдеров потенциальной точкой утечки данных и приводит к использованию для нужд защищаемых ресурсов серверов и каналов связи, не обеспечивающих должной производительности.

Вторая по значимости проблема – это фактическое отсутствие единого каталога ресурсов, предназначенных для публикации общей информации, и фактическое отсутствие поисковых систем, работающих с сайтами в анонимных сетях. И снова причиной является отсутствие доверенного протокола организации поисковых каталогов. Каталогизация и поиск ресурсов отданы на откуп сторонним централизованным сервисам, использование которых также вносит уязвимость в работу приватной сети.

Таким образом, современные приватные сети не обеспечивают достаточного качества пользования и должной защищенности пользователей и владельцев сайтов, оставаясь при этом уязвимыми к техническим атакам.

На наш взгляд, проблема построения защищенной, обеспечивающей приватную работу пользователей, сети заключается не столько в применении каких-либо систем и средств защиты или криптографии, сколько в существующей парадигме построения информационных систем. Эта парадигма заключается в главенстве сети и технической составляющей сети (ее узлов) над информацией, жесткой привязке информации к определенным узлам или группам (кластерам) узлов сети и изначальной открытости сети.

Всё остальное – системы аутентификации, авторизации, криптографии, межсетевое экранирования и анонимизации и т.д. – представляет собой разрозненные надстройки, которые усложняют систему, понижают ее полезную производительность и повышают сложность ее конфигурирования и управления, что в свою очередь создает дополнительные уязвимости и существенно увеличивает трудозатраты на администрирование и разработку информационных систем [5, 24].

ОСНОВНЫЕ ТРЕБОВАНИЯ К СИСТЕМЕ ПРИВАТНОГО ИНТЕРНЕТА

Как правило, архитектура и топология сетей интересуется только технических специалистов (программистов, системных инженеров, специалистов по кибербезопасности) и разного рода злоумышленников. Большинство пользователей ИС, исключая перечисленные категории, не интересуется архитектурой сетей, их топологией или то, на каких именно узлах хранится интересующая их информация либо выполняются необходимые для них вычисления. Пользователи работают с информацией. Запрашивают информацию, вводят информацию либо дают задания на вычисление новой информации на базе существующей. Это касается как пользователей – людей, так и программных автоматов, задействованных в процессах информационного обмена между ИС.

Для решения рассмотренных в настоящей работе проблем, мы предлагаем осуществить качественный переход от информационной компьютерной сети (Internet) к облаку данных и вычислений на основе приватной защищенной децентрализованной экосистемы (Privacy-oriented and Secure Decentralised Ecosystem, PSDE), построенной на принципах:

1. Первичности пользовательской информации: алгоритмы взаимодействия пользователя с сетью должны реализовывать непосредственную работу с пользовательской информацией через упорядоченную информационную картотеку без взаимодействия с узлами сети, либо ее техническими службами. Сама процедура работы с информационной картотекой должна быть максимально унифицирована и стандартизирована.

2. Живучести пользовательской информации: информация не может быть потеряна, уничтожена или заблокирована никаким способом кроме прямой команды на уничтожение информации от пользователя, который ее опубликовал, либо лица, специально им уполномоченного.

3. Доступности пользовательской информации: весь доступный пользователю контент автоматичес-

ки попадает в информационную картотеку пользователя. Для каждого пользователя формируется индивидуальная информационная картотека.

4. Защищенности пользовательской информации: пользователь сам решает какую персональную информацию и какой контент сети, созданный им, будет раскрыт другим пользователям. Он же определяет и взаимосвязи между опубликованными им данными. Изначально вся информация считается закрытой и доступной только самому пользователю – владельцу. Фактически принцип предполагает так же возможность анонимной публикации контента и сокрытие фактов чтения контента. Тут следует отметить, что сведения об общей статистике чтения контента и оценках контента, не раскрывая при этом читателей и оценщиков, должны предоставляться владельцу контента для оценки релевантности информации для ее целевой аудитории.

5. Хранения пользовательской информации «везде и нигде»: принцип следует из необходимости обеспечения живучести и защищенности пользовательской информации и предполагает распределенное хранение и обработку информации в сети, организованные таким образом, чтобы ни одно устройство сети не обладало ни одной конечной единицей контента полностью. Любой документ в сети должен быть разделен на части достаточно малые, чтобы обеспечить невозможность восстановления целого по его части. И затем эти части должны быть распределены между узлами сети так, чтобы ни один узел не владел больше чем одной такой частью.

6. Полной абстракции пользователей от метаданных, технической информации, процессов функционирования сети: принцип предполагает полную, с точки зрения пользователя, независимость пользовательской информации от ее физических и логических носителей. Иначе говоря, пользователь должен получать непосредственный доступ к полезному контенту, минуя обращение к какому-либо узлу или адресу сети, через единую упорядоченную информационную картотеку.

7. Полного сокрытия от пользователей метаданных и технической информации: принцип предполагает блокировку любых возможностей анализа топологии и структуры сети и полное сокрытие технической информации о работе сети и ее программного обеспечения, в том числе и от технических специалистов. Исполнение этого принципа предполагает автоматическое выполнение всех сервисных мероприятий сети и программ.

Единственным исключением должны быть сведения о состоянии аппаратного обеспечения узлов, которые должны транслироваться в каталог пользователя – владельца устройства. Это необходимо, чтобы обеспечить функциональную возможность контроля за техническим состоянием устройств и

обеспечением их своевременного ремонта или замены, поскольку реализовать «саморемонт» аппаратной части в текущих условиях не представляется возможным. Вторая функция такого исключения - контроль общей нагрузки на аппаратных мощностях для их своевременного увеличения. Соккрытие метаданных означает отсутствие у кого-либо из пользователей любой информации о точных местах хранения частей документов.

В обобщенной архитектуре частного и безопасного Интернета за реализацию принципов 1-5 отвечает PSDE, которую будем рассматривать в реализации PSDE TheOoL Project [5, 25], который также отвечает за соккрытие от пользователей метаданных системы хранения и обработки. За реализацию принципов 6, 7 отвечают PSDE TheOoL и защищенный сетевой протокол (SecNP) в качестве которого считаем возможным использовать любую реализацию I2P из существующих.

ПРИВАТНАЯ ЗАЩИЩЕННАЯ ДЕЦЕНТРАЛИЗОВАННАЯ ЭКОСИСТЕМА THEOOL.NET

PSDE TheOoL представляет собой децентрализованное вычислительное облако, которое обеспечивает пользователям бессерверный хостинг, распределенное облачное хранилище, среду для исполнения децентрализованных приложений (например, децентрализованной аудио- и видеосвязи). В качестве отдельного децентрализованного приложения в PSDE встроена платежная система, которая необходима, чтобы исключить нарушение конфиденци-

альности пользователя через цепочку платежей, проходящих в сторонних платежных системах.

Основная задача PSDE – предотвращение угроз конфиденциальности пользовательских данных и устранение угроз информационной безопасности (ИБ), нацеленных на серверы, центральные вычислительные узлы и абонентские места сети.

Технически PSDE представляет собой распределенную операционную систему, каждый узел которой отдает свои вычислительные ресурсы (подсистему хранения, центральный и графический процессоры, оперативную память) системе и не имеет самостоятельного значения. Однако узлы отличаются по функциональному назначению. В системе определены узлы абонента (AN – abonent node) и технические узлы (TN – technical node), которые могут выполнять функции узла хранения и вычислений (SCN – storage & computational node), узла метаданных (MN – metadata node), консенсуса распределенного реестра (DLCN – distributed ledger consensus node) и узла поисковой системы (SSN – search system node). Назначение технического узла определяется автоматически алгоритмами PSDE и может быть переопределено в любой момент времени в зависимости от потребностей сети. При наличии достаточных ресурсов, технический узел может выполнять несколько функций одновременно.

Для реализации заявленных принципов построения частного Internet PSDE была спроектирована авторами в четырехуровневой архитектуре (рис.1), компоненты которой размещены на узлах системы в соответствии с картой размещения программных модулей четырехуровневой архитектуры PSDE (Табл.1).

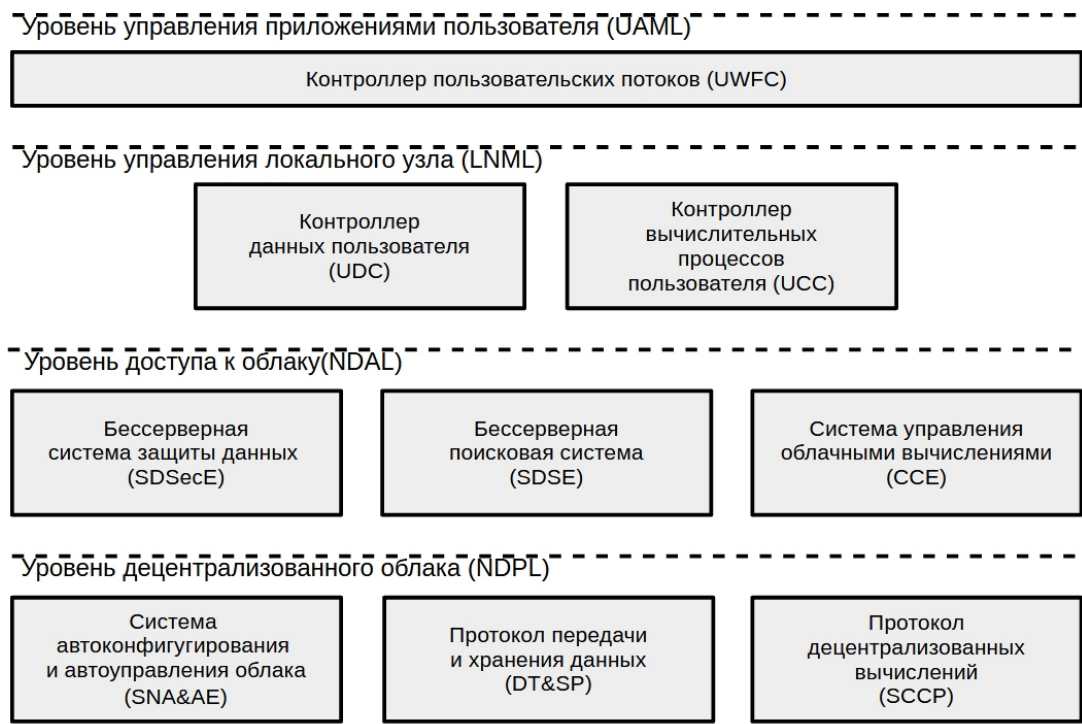


Рис. 1. Программная архитектура PSDE

Карта размещения компонентов программной архитектуры на узлах PSDE

№ уровня	Уровень архитектуры	ID компонента	Компонент	Abonent Node	Tecnical Node			
					SCN	MN	DLCN	SSN
1	UAML	1.1	UWFC	Y	SA	SA	SA	SA
2	LNML	2.1	UDC	Y	SA	SA	SA	SA
		2.2	UCC	Y	N	N	N	SA
3	NDAL	3.1	SDSecE	N	N	Y	Y	N
		3.2	SDSE	N	N	Y	N	Y
		3.3	CCE	N	Y	Y	Y	N
4	NDPL	4.1	SNA&AE	N	LM	Y	Y	LM
		4.2	DT&SP	N	Y	Y	Y	Y
		4.3	SCCP	N	Y	Y	Y	N
Y – присутствует N – отсутствует SA – специализированное приложение LM – локальный модуль								

Уровни 1 и 2 программной архитектуры предназначены в основном для реализации AN, но их компоненты функционируют и на TN в качестве специализированных приложений, предназначенных, для организации и централизации управления и мониторинга состояния аппаратной частью TN со стороны их владельцев. Это необходимо для управления центрами обработки данных с AN владельца и наемного технического персонала. При выполнении TN роли SSN компонент 2.2- UCC используется для распределения вычислительных заданий на обработку поисковых запросов абонентов между узлами SCN. Уровни 3 и 4 программной архитектуры предназначены строго для реализации TN.

Непосредственное хранение данных осуществляется на четвертом уровне таким образом, что любой пользовательский блок данных (файл) разделяется на N одинаковых пакетов, шифруется и отправляется на хранение на K различных узлов сети (K - коэффициент избыточности) в зашифрованном виде. Перечень узлов хранения блоков помещается в блок метаданных, который в свою очередь шифруется и отправляется на хранение. Никто, включая владельца, не знает, на каких узлах в конкретный момент времени хранятся части файла, кроме подсистемы, имеющей доступ к метаданным. На этом же уровне функционируют автоматические алгоритмы обслуживания PSDE.

Поскольку PSDE представляет собой децентрализованную систему, в которой полностью устранены любые централизованные сервисы и органы управления, в том числе контролирующие доступ к данным и платежам, ее можно представить как де-

централизованную автономную систему (DAO) [26].

Ядром системы бессерверной безопасности и управления PSDE, как любой DAO, является распределенный реестр (блокчейн). В блокчейн TheOoL функции управления неразрывно связаны с встроенной платежной системой. Этот блокчейн обслуживает две взаимосвязанные распределенные базы данных. Первая – база данных дескрипторов безопасности SDSecE (рис.1) – обеспечивает контроль за доступом к данным, а так же децентрализованный алгоритм применения и изменения дескрипторов безопасности за счет безопасного и надежного алгоритма консенсуса, аналогичного классическому для распределенных реестров Proof Of Work (PoW) алгоритма [27]. В отличие от классического PoW, в PSDE решена проблема производительности. Моделирование PSDE и последующие испытания модели показали производительность, сравнимую с централизованными системами [28].

Вторая – база умных контрактов и платежей – непосредственно связана с встроенной платежной системой и обслуживает взаимодействия пользователя и PSDE. С точки зрения PSDE любая задача, поставленная пользователем перед PSDE, – это умный контракт (специальный скрипт), который определяет роли и вознаграждения отдельных узлов PSDE в рамках этой задачи. При этом бенефициарами вознаграждений будут владельцы этих узлов, которые при этом не допущены к процессу ее (задачи) исполнения, либо к сведениям, связанным с ней. В этом смысле PSDE обеспечивает полную абстракцию пользователя и инфраструктуры. Для сокращения вычислительной нагрузки в качестве алгоритма

консенсуса для распределенного реестра умных контрактов и платежей выбран алгоритм «доказательство доли владения» (Proof Of Stake) [29, 30].

Пользователям PSDE доступны роли потребителей контента, поставщиков контента и поставщиков ресурсов. Под ресурсами мы будем понимать вычислительные ресурсы (аппаратные серверы), которые пользователи PSDE предоставляют в арен-

ду для хранения и обработки контента. Под пользователями (рис.2) мы понимаем любую сущность, которая имеет уникальный идентификатор пользователя PSDE (Unique User Identifier, UUIд), от имени которого исполняются роли пользователей и наделены полномочиями на совершение операций в PSDE, где каждая операция представляет собой умный контракт между двумя и более UUIд.

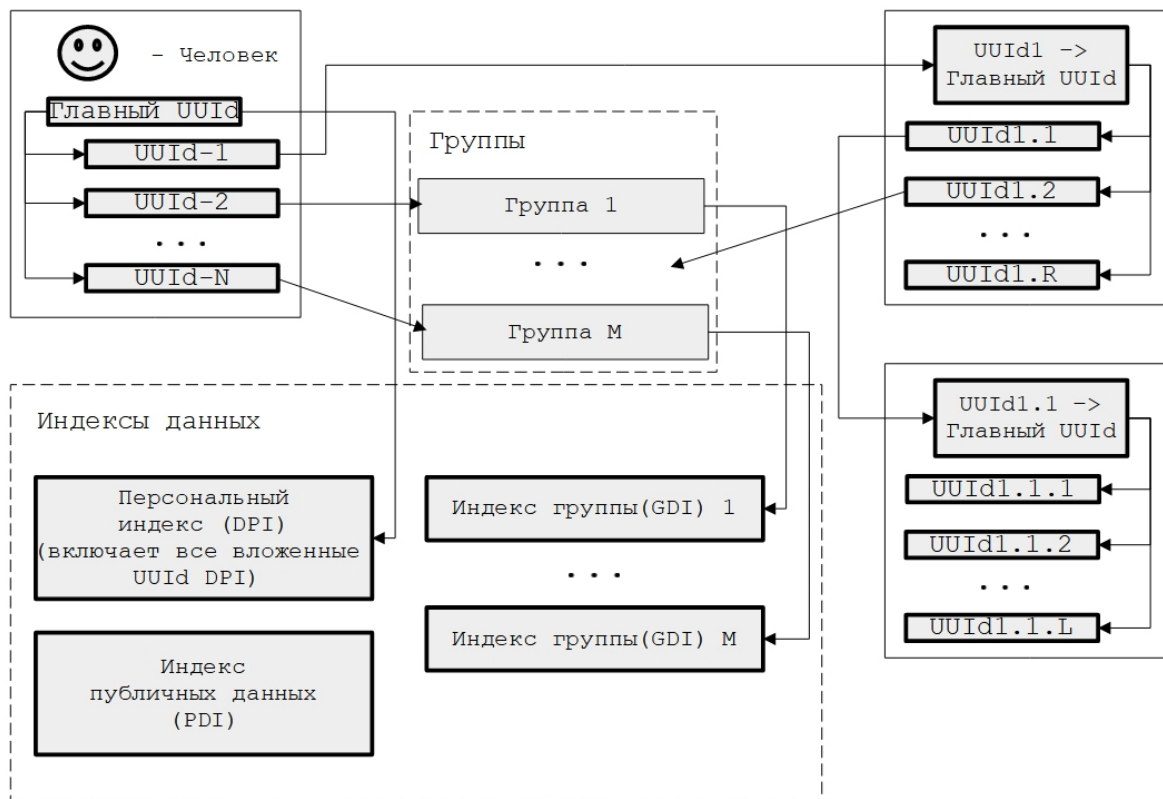


Рис. 2. Пользователи, группы и механизм доступа к данным

Это могут быть пользователи люди, специализированные алгоритмы или программные аватары устройств IoT. UUIд могут объединяться в иерархические группы со сложными правилами взаимной подчиненности и взаимной автоматической передачи прав доступа к генерируемому ими контенту на основании специализированного умного контракта участника группы, где прописываются правила взаимодействия между членами группы. При этом в группу может включаться, по решению пользователя, как главный UUIд пользователя, так и специально генерированный вторичный UUIд. Это позволяет пользователю самостоятельно формировать роли для разных сетевых взаимодействий. Например, он может иметь различные, взаимно не пересекающиеся профили для бизнес-групп его нанимателя, для социальных сетей и чтения или публикации личного контента, фактически отдельные уникальные цифровые личности для разных ситуаций.

Таким образом, пользователь полностью сам управляет тем «цифровым следом», который он желал бы оставить при выполнении той или иной задачи. С точки зрения его контрагентов каждый UUIд – полностью уникальный и самостоятельный. PSDE не дает никакой возможности выявить взаимосвязи между основным и подчиненными UUIд. Сведения о взаимной подчиненности UUIд хранятся в PSDE в зашифрованном виде в информационной единице, доступ к которой и сведения о существовании которой имеет только главный UUIд.

Контент (пользовательские данные) мы будем понимать в самом широком смысле, как разного рода текстовую, графическую, мультимедиа информацию и исполняемые алгоритмы. При размещении исполняемых алгоритмов на их содержимое PSDE накладывает ряд ограничений и требований, подробному описанию которых будет посвящена отдельная работа. Для целей настоящей статьи до-

статочно упомянуть, что на момент её написания прототип подсистемы распределенных вычислений PSDE поддерживает программные модули на языке Python 3.x с ограниченным набором популярных библиотек, оснащенные специальными строками документации и декораторами.

Дополнительно мы введем понятие особо защищаемой информации (specially protected information, SPI) к которой отнесем персональные данные и идентификаторы пользователей, сведения о сетевой активности пользователей, сведения о принадлежности контента и/или ресурсов тому или иному пользователю или группе пользователей, контракты пользователей, независимо от того, исполняются обязательства по ним полностью онлайн или частично оффлайн.

Доступ к контенту осуществляется через специальный упорядоченный информационный каталог с набором индексов (рис.1), которые составляют основу для работы децентрализованной поисковой машины TheOoL. В PSDE каждому UUID доступны три типа индексов данных: персональные индексы (Data Personal Index, DPI), привязанные к каждому UUID пользователя, содержат сведения о данных, опубликованных в монопольном режиме, в том числе минимально необходимые SPI; групповые (Group Data Index, GDI), содержат сведения о данных, предназначенных для использования в конкретной группе пользователей и доступны только участникам этой группы; единый для всех пользователей PSDE публичный индекс (Public Data Index, PDI).

Добавление в индекс новых записей происходит при размещении пользователем контента в PSDE. В индексную запись автоматически вводится идентификатор блока данных, его пользовательское наименование (например, название документа) и, для контента классов текстовой информации и исполняемых алгоритмов, запускается алгоритм автоиндексирования. Для исполняемых алгоритмов в индекс собираются объявленные в строках документации ключи, а для текстовой информации в качестве индексных ключей отбираются наиболее часто повторяющиеся слова и фразы, а так же фразы, совпадающие с уже существующими ключами в доступных UUID индексах, что позволит обеспечить наилучшую классификацию блока данных в едином каталоге PSDE.

На следующем шаге пользователю предлагается самостоятельно отредактировать индекс блока данных и определить, к какой из доступных ему индексов (DPI, GDI или PDI) будет помещена индексная запись. По умолчанию запись будет добавлена

в DPI текущего UUID пользователя.

SPI, неразрывно связанные с блоком данных, содержат сведения о принадлежности определенному UUID и смарт-контракт PSDE размещаются только в DPI UUID владельца блока данных. Сгенерированному смарт-контракту PSDE присваивается идентификатор и его тело вместе с идентификатором отправляется в пул публичных оферт – заказов PSDE в обезличенном виде, где эту оферту автоматически принимают поставщики ресурсов.

Фактически смарт-контракт PSDE содержит параметры обработки и хранения блока данных: срок хранения, параметры исполнения (для исполняемого алгоритма), коэффициент избыточности, желаемую скорость доступа, количество одновременных обращений и т. п. При этом поставщики ресурсов лишены доступа к любой информации о владельце контента. Со стороны поставщиков ресурсов в исполнении смарт-контракта всегда участвует некоторое множество поставщиков, среди которых блок данных распределяется «кусками», не более одной части каждому. Фактически поставщик ресурсов знает только требования к обработке и хранению конкретного «куска» и не имеет никакого представления, ни какому конкретно блоку данных этот «кусочек» принадлежит, ни тем более какой UUID является владельцем этого блока данных. Таким образом, SPI, связанные с данными, никогда не передаются другим участникам сети. Исключением может быть ситуация, когда необходимо защитить свое авторство и право на тот или иной контент.

Для этой ситуации мы предусмотрели систему пользовательских SPI. Пользователь может самостоятельно создать в системе необходимые ему наборы SPI с привязкой к определенным UUID и использовать их по мере необходимости. Например для фиксации своих авторских прав, или идентифицированного взаимодействия с работодателем, если работа в ИС, построенной на базе PSDE. Такие SPI могут, строго по подтвержденному волеизъявлению пользователя, передаваться в GDI и даже PDI. Для подтверждения воли пользователя на публикацию SPI используется усложненная процедура аутентификации.

ЗАКЛЮЧЕНИЕ

Таким образом, предлагаемая система приватного интернета полностью реализует заявленные принципы: обеспечивает абстракцию пользователя и сетевой инфраструктуры, полностью скрывает инфраструктуру и данные от стороннего наблюда-

теля, позволяет строить безопасные распределенные сети непосредственно поверх публичной сети Интернет без применения дополнительных систем защиты, поскольку сама выполняет функции межсетевого экранирования, туннелирования и криптографической защиты трафика.

Полное исключение доступа к пользовательским данным и вычислениям со стороны владельцев инфраструктуры позволяет решить проблему доверия к облачному сервису и без опаски размещать узлы TN на высокопроизводительном оборудовании и

широких по полосе пропускания каналах передачи данных, что существенно повысит качество сервисов приватной сети, позволит использовать самые современные программные и мультимедийные технологии.

Наличие встроенной системы каталогизации и поиска позволяет доводить информацию до целевой аудитории без нарушения приватности владельца контента и потребителя. Фактически PSDE TheOoL – это система, в которой исключена возможность атаки «человек посередине».

СПИСОК ЛИТЕРАТУРЫ

1. Силаева В.Л. Подмена реальности как социокультурный механизм виртуализации общества: Дис. на соискание ученой степени канд. филос. наук : 09.00.11 : Москва, 2004, 115 с.
2. Питкевич П.И. Методы объединения, сокращения размеров и обработка больших данных // Инженерный вестник Дона, 2021. №12. URL: ivdon.ru/ru/magazine/archive/n12y2021/7338 (дата обращения: 01.03.2023).
3. Менциев А.У., Айгумов Т.Г., Эмирова Г.А. Анализ характеристик и функциональных возможностей устройств IoT // Инженерный вестник Дона, 2023. №2 URL: ivdon.ru/ru/magazine/archive/n2y2023/8191 (дата обращения: 01.03.2023).
4. Общество 5.0 – цифровизация экономического роста по-японски. URL: controlengrussia.com//rynok//obshhestvo-5-0-po-yaponski (дата обращения: 01.03.2023).
5. Nenashev A., Khryashchev V. The Economics of Introducing the Peer-to-peer System of Storage and Processing of Protected Information at an Enterprise // XXI International Conference Complex Systems: Control and Modeling Problems (CSCMP). IEEE, 2019. С. 769-772.
6. Gartner Forecasts Worldwide Security and Risk Management Spending to Exceed \$150 Billion in 2021. URL: gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-managem (дата обращения: 01.03.2023).
7. Пашинская А. Кто и как следит за вами в интернете. URL: dw.com/ru/кто-и-как-следит-за-вами-в-интернете/a-40712694 (дата обращения: 01.03.2023).
8. Таненбаум Э., Ван Стеен М. Распределенные системы. Принципы и парадигмы. СПб.: Питер, 2003. 877 с.
9. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. СПб.: Питер, 2016. 992 с.
10. Möller Ch., Amouroux A. The Media Freedom Internet Cookbook. Vienna: OSCE, 2004. 274 с.
11. Gont F. ICMP attacks against TCP (draft-gont-tcpm-icmp-attacks-01). URL: tools.ietf.org/id/draft-gont-tcpm-icmp-attacks-01.txt (дата обращения: 01.03.2023).
12. Анин Б.Ю. Защита компьютерной информации. СПб.: БХВ-Петербург, 2000. 384 с.
13. Баронов В.В., Калянов Г.Н., Попов Ю.Н., Титовский И.Н. Информационные технологии и управление предприятием. М.: АйТи, 2009. 328 с.
14. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. М.: Радио и связь, 2001. 376 с.
15. Защита информации в компьютерных системах // под ред. д-ра экон. наук Е.В. Стельмашонок, канд. физ.-мат. наук И.Н. Васильевой. СПб.: Изд-во СПбГЭУ, 2017. 163 с.
16. Нашумевшие утечки данных пользователей за январь – апрель 2019. URL: habr.com/ru/company/cloud4y/blog/452880/ (дата обращения: 01.03.2023).
17. Благовещенский А. Яндекс объяснил утечку паспортов и билетов россиян. URL: rg.ru/2018/07/17/iandeks-obiasnil-utechku-pasportov-i-biletov-rossiian.html (дата обращения: 01.03.2023).
18. Google сообщила об утечке данных более 52 млн пользователей из-за ошибки. URL: rbc.ru/technology_and_media/11/12/2018/5c0f033a9a794766b04420a5 (дата обращения: 01.03.2023).
19. Умные квартиры с голосовым помощником Алиса. URL: xn--b1afabvedwejl1a2e.xn--p1ai/rnews/635 (дата обращения: 01.03.2023).

20. Фадеичев С. Беспилотный транспорт может массово использоваться в России через восемь лет. URL: tass.ru/ekonomika/6165233 (дата обращения: 01.03.2023).
21. Warehouse Robotics Market. URL: marketsandmarkets.com/Market-Reports/warehouse-robotic-market-128876258.html (дата обращения: 01.03.2023).
22. Egger C., Schlumberger J., Kruegel C., Vigna G. Practical Attacks against the I2P Network // Lecture Notes in Computer Science. 2013. Т. 8145. С. 432-451.
23. Casenove M., Miraglia A. Botnet over tor: The illusion of hiding" // 6th International Conference Cyber Conflict (CyCon 2014). 2014. С. 273-282.
24. Hryashev V.V., Nenashev A.V. Efficiency of the implementation of the peer-to-peer distributed system for securable information storage and processing (TheOoL Project) // Modeling of systems and processes. 2021. №3. С. 82-89.
25. TheOoL White Paper. URL: theool.net/doc/TheOoLWhitePaper.pdf (дата обращения: 01.03.2023).
26. Schillig M. Some Reflections on the Nature of Decentralized (Autonomous) Organizations. URL: ssrn.com/abstract=3915843 (дата обращения: 01.03.2023).
27. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. URL: http://bitcoin.org/bitcoin.pdf (дата обращения: 01.03.2023).
28. Nenashev A.V., Tolstenko A.Y., Oleshko R.S. Model of the peer-to-peer distributed system for securable information storage and processing without traffic prioritization (THEOOL project) // CEUR Workshop Proceedings. 2021. Т. 2899. С. 141-150.
29. Li W., Andreina S., Bohli J.M., Karamé G. Securing Proof-of-Stake Blockchain Protocols // Lecture Notes in Computer Science, Т. 10436. С. 29-315.
30. Saleh F. Blockchain without Waste: Proof-of-Stake // The Review of Financial Studies. 2021. Т. 34. №3. С. 1156–1190.

УДК 004.056.5

Технологии, обеспечивающие функционирование центров управления сетевой безопасностью информационно-телекоммуникационных сетей, и оценка уровня их зрелости

S.S. Veligodskiy, N.G. Miloslavskaya

Technologies Ensuring the Operation of Network Security Centers of Information and Telecommunication Networks and Their Maturity Level Assessment

Abstract. The goal of the paper is to identify modern technologies that ensure the functioning of Network Security Centers (NSCs) of Information and Telecommunication Networks (ITCNs) of organizations, and their role in ensuring the implementation of relevant ITCN network security management (NSM) processes and the provision of services to consumers inside and outside the organization. The place of these technologies among other NSC functioning components, namely, the typical ITCN NSM processes and services implemented in the NSC, as well as the general NSC maintenance and staffing, is shown. Using the developed by the authors NSC ITCN maturity model, built on the basis of a generalization of the best practices for creating maturity models for various assessment objects, a formalized model for assessing the maturity level of technologies used in the NSC ITCN is presented.

Keywords: network security center, information and telecommunications network, technology, maturity model, maturity level assessment areas.

С.С. Велигодский¹Н.Г. Милославская²

¹Инженер, Национальный исследовательский ядерный университет "МИФИ".

E-mail: sveligodsky@gmail.com

²Ph.D. (UK), д.т.н., доцент, профессор,

Национальный исследовательский ядерный университет «МИФИ».

E-mail: NGMiloslavskaya@mephi.ru

Аннотация. Целью статьи является определение современных технологий, обеспечивающих функционирование центров управления сетевой безопасностью (ЦУСБ) информационно-телекоммуникационных сетей (ИТКС) организаций, и их вклада в поддержку выполнения соответствующих процессов и предоставления услуг по управлению сетевой безопасностью (УСБ) ИТКС потребителям внутри и вне организации и общий уровень зрелости ЦУСБ. Показано место этих технологий среди других составляющих функционирования ЦУСБ, а именно, процессов УСБ и услуг по УСБ типовой ИТКС, реализуемых в ЦУСБ, а также организационного и кадрового обеспечения ЦУСБ. С использованием разработанной авторами модели зрелости ЦУСБ ИТКС, построенной на основе обобщения лучших практик создания моделей зрелости для различных

объектов оценки, представлена формализованная модель оценки уровня зрелости технологий, применяемых в ЦУСБ ИТКС.

Ключевые слова: центр управления сетевой безопасностью, информационно-телекоммуникационная сеть, технологии, модель оценки уровня зрелости, направления оценки уровня зрелости.

ВВЕДЕНИЕ

Центры управления сетевой безопасностью (ЦУСБ) [1] привлекают все большее внимание, поскольку информационно-телекоммуникационные сети (ИТКС) используются субъектами критической информационной инфраструктуры (КИИ) Российской Федерации (государственными органами и учреждениями, юридическими лицами, индивидуальными предпринимателями, работающими в сфере здравоохранения, транспорта, связи, энергетики, финансов, оборонной, добывающей и химической промышленности и т.д.) для поддержки их деятельности [2]. Согласно ГОСТ Р ИСО/МЭК 27033-1-2011 [3], сетевая безопасность ИТКС органи-

зации включает в себя «безопасность устройств, безопасность деятельности по управлению этими устройствами, приложениями, предоставляемыми услугами и конечными пользователями, в дополнение к безопасности информации, передаваемой по линиям связи».

Известно три уровня управления сетевой безопасностью (УСБ) ИТКС [1]. На уровне оперативного управления анализом собранных данных занимается Центр мониторинга безопасности (ЦМБ) (*Security Operations Center, SOC*) (термин введен компанией Cisco в 2005 г.), в чьи функции входит мониторинг относящихся к информационной безопасности (ИБ) ИТКС организации событий и выделение инцидентов ИБ. На тактическом уровне определяются методы и способы обеспечения ИБ (ОИБ), осуществляет-

ся планирование и реализация Политики ИБ ИТКС и разработка поддерживающей ее организационно-распорядительной документации (ОРД), а также проводится выработка корректирующих и предупреждающих воздействий на ИТКС. Здесь располагается известный с 2010 г. Центр интеллектуальной безопасности (ЦИБ) (*Security Intelligence Center*), способный управлять инцидентами ИБ в ИТКС и проводить их расследование. Уровень стратегического управления предназначен для постановки целей, задач, определения направлений и выбора приоритетов в ОИБ ИТКС на длительную перспективу в поддержку основной деятельности организации. На этом уровне находится Центр интеллектуального управления сетевой безопасностью (ЦИУСБ) [1] (идея впервые представлена Н.Г.Милославской в 2016 г.), способный прогнозировать развитие ситуации в ИТКС за счет внедрения новых технологий и подходов к ОИБ и выявления тенденций появления новых угроз ИБ с применением интеллектуальных методов.

Эволюция ЦУСБ началась с 90-х годов XX века с появления подразделений или групп (ГРИИБ) с раз-

ными названиями (например, *Computer Emergency Response Team – CERT* и *Computer Security Incident Response Team – CSIRT*), предоставляющих кадровую поддержку и услуги по выявлению событий ИБ и реагированию на инциденты ИБ. ЦМБ имеет специальные средства защиты информации (СЗИ) и квалифицированный персонал, осуществляющий мониторинг событий ИБ в ИТКС с *SIEM*-системой 1.0 (*Security Information and Event Management* – управление информацией и событиями безопасности) в качестве ядра. ЦИБ с *SIEM*-системой 2.0 способен управлять инцидентами ИБ за счет использования ИБ-аналитики и обработки больших данных. ЦИУСБ объединяет ЦИБ с функциональными возможностями сетевого операционного центра (СОЦ) (*Network Operations Center, NOC*), озерами данных (*data lakes*) и интеллектуальной обработки быстрых данных с *SIEM*-системой 3.0. Таким образом, ЦУСБ прошли путь от мониторинга инцидентов ИБ (ЦМБ) через управление инцидентами ИБ (ЦИБ) к обеспечению упреждающей (*proactive*) настраиваемой (адаптивной) сетевой безопасности (ЦИУСБ) (рис. 1) [1].

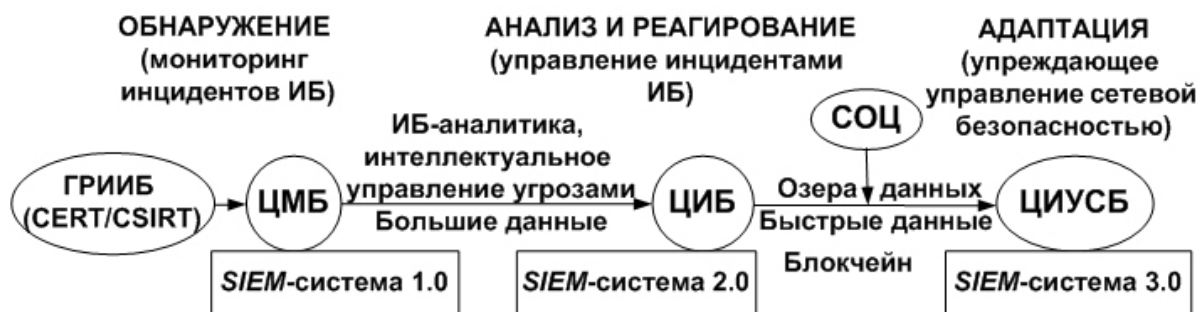


Рис. 1. Эволюция ЦУСБ согласно [1]

Данная картина была дополнена Калияперумалом Л.Н. в [4] (рис. 2). До 1995 г. были известны только СОЦ, управляющие сетевыми устройствами и выполняющие анализ вредоносного ПО. В задачи собственного ЦУСБ организаций до 2000 г. входила обработка предупреждений о вирусах, обнаружение вторжений и фильтрация трафика межсетевыми экранами (МЭ).

В 2000 г. мониторинг доступности сменился мониторингом с последующим реагированием. После выхода в 2005 г. стандартов ISO/IEC по управлению ИБ (УИБ) к целям ЦУСБ добавились слежение за соблюдением нормативных требований с применением МЭ с динамической фильтрацией пакетов, защита от спама, управление уязвимостями и предотвращение вторжений. В 2007-2013 гг. появились решения для упреждающего мониторинга – это *SIEM*-системы, системы предотвращения утечки

данных (*Data Loss Prevention, DLP*), средства обнаружения целенаправленных постоянных угроз (*Advanced Persistent Threats, APTs*) и управления журналами регистрации событий (ЖРС) (*log files*), а также управляемые услуги безопасности (*Managed Security Service*).

Гибридные ЦУСБ с *SIEM*-системами следующего поколения с меньшим количеством ложных срабатываний, средствами анализа поведения пользователей и угроз ИБ на основе машинного обучения, «песочницей» (*sandbox*), реверс-инжинирингом, обеспечением безопасности в облаке и другими технологиями – тренд 2013-2015 гг.

С 2015 г. началась эпоха упреждающего мониторинга с автоматизацией, когда платформы и средства сбора данных об угрозах, информационный поиск в открытых источниках (*Open Source Intelligence, OSINT*), ИБ-аналитика (*Security Intelligence*) стали

основой ОИБ, позволяющей заблаговременно обнаруживать и устранять скрытые угрозы. Центр киберзащиты (*Cyberdefense Center*) или киберобъединения (*Cyberfusion Center*), центр реагирования на киберугрозы (*Cyber Threat Response Center*), объединенный операционный центр (*Joint Operations Center*) — лишь часть новых названий ЦУСБ, предоставляющих такие услуги, как: мониторинг, обнаружение, сортировка событий ИБ; анализ вредоносного ПО, реверс-инжиниринг, цифровая криминалистика; управление платформой анализа угроз ИБ; поиск угроз ИБ на основе тактик, техник и процедур (*Tactics, Techniques and Procedures, ТТР*); управление контентом, угрозами и уязвимостями; соблюдение соответствия требованиям; отчетность и уведомление; обучение; управление идентификацией и доступом.

На основе анализа информационных источников в данной работе ставится цель определения современных технологий, обеспечивающих функционирование ЦУСБ ИТКС организаций, и их вклада в поддержку выполнения процессов и предоставления услуг по УСБ ИТКС потребителям внутри и вне организации и общий уровень зрелости ЦУСБ.

1. ОСНОВНЫЕ КОМПОНЕНТЫ ЦУСБ

Основой эффективного функционирования ЦУСБ являются пять взаимосвязанных компонентов, определенных в результате анализа сложноорганизованных систем, к которым относится ЦУСБ [1] (рис. 2):

- организационное обеспечение (оргструктура с процессами и технологиями управления деятельностью и ОРД) (сокращенно ОФ);
- должным образом разработанные, внедренные, контролируемые и совершенствуемые процессы УСБ ИТКС (сокращенно ПУСБ);
- стабильно предоставляемые потребителям услуги по УСБ ИТКС ожидаемого качества, поддер-

живающие требуемый уровень ИБ ИТКС в соответствии с применимыми требованиями по ОИБ (сокращенно УУСБ);

- используемые для этого технологии, реализованные в конкретных системах и помогающие персоналу ЦУСБ обеспечивать ИБ ИТКС и собственную ИБ рациональнее, опирающиеся на соответствующие меры ОИБ и автоматизацию для снижения трудоемкости выполнения рутинных операций и сокращения времени выполнения работ (сокращенно Т);

- кадровое обеспечение с привлечением высококвалифицированных специалистов [4] (сокращенно К).

При таком подходе классическая триада «люди-технологии-процессы» управления ИТ-услугами [5] расширяется за счет рассмотрения функционирования ЦУСБ в структуре ИТКС с точки зрения удовлетворения потребностей и поддержания основной деятельности организации при одновременном применении системного, процессного и сервисно-ориентированного подходов к УСБ ИТКС.

Суть получаемого при этом синергетического преимущества состоит в следующем. Процессы УСБ (их состав показан на рис. 3) являются связующим звеном между технологиями ОИБ и персоналом ЦУСБ, представляющим собой сложную систему и имеющим определенную организационную структуру и обеспечение для его функционирования. С процессами связана ответственность за выполнение отдельных задач ЦУСБ в рамках предоставления им услуг по УСБ ИТКС и детальный порядок их выполнения.

Состав реализуемых ЦУСБ процессов определяется границами предоставления услуг, их необходимым количеством и используемыми для этого технологиями, обеспечивающими ИБ ИТКС и самого ЦУСБ. В свою очередь, состав используемых технологий определяется перечнем необходимых услуг и всеми применимыми требованиями по ОИБ ИТКС в поддержку основной деятельности организации.

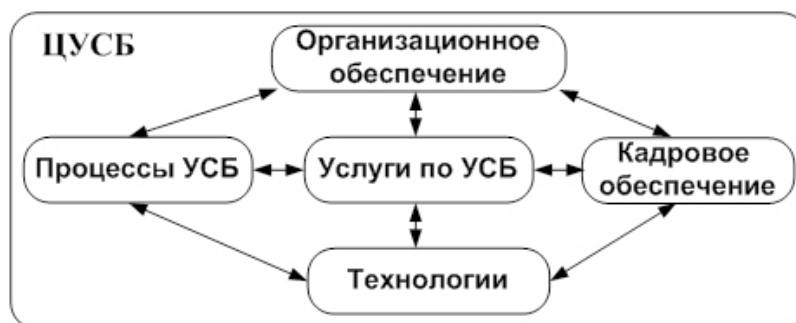


Рис. 2. Компоненты ЦУСБ

Таким образом на единой основе строится система-тика (классификация и систематизация), необходимая для упорядочивания знаний о сложноргани-

зованных взаимосвязанных объектах – процессах, услугах и технологиях для ЦУСБ (на основе [1]).

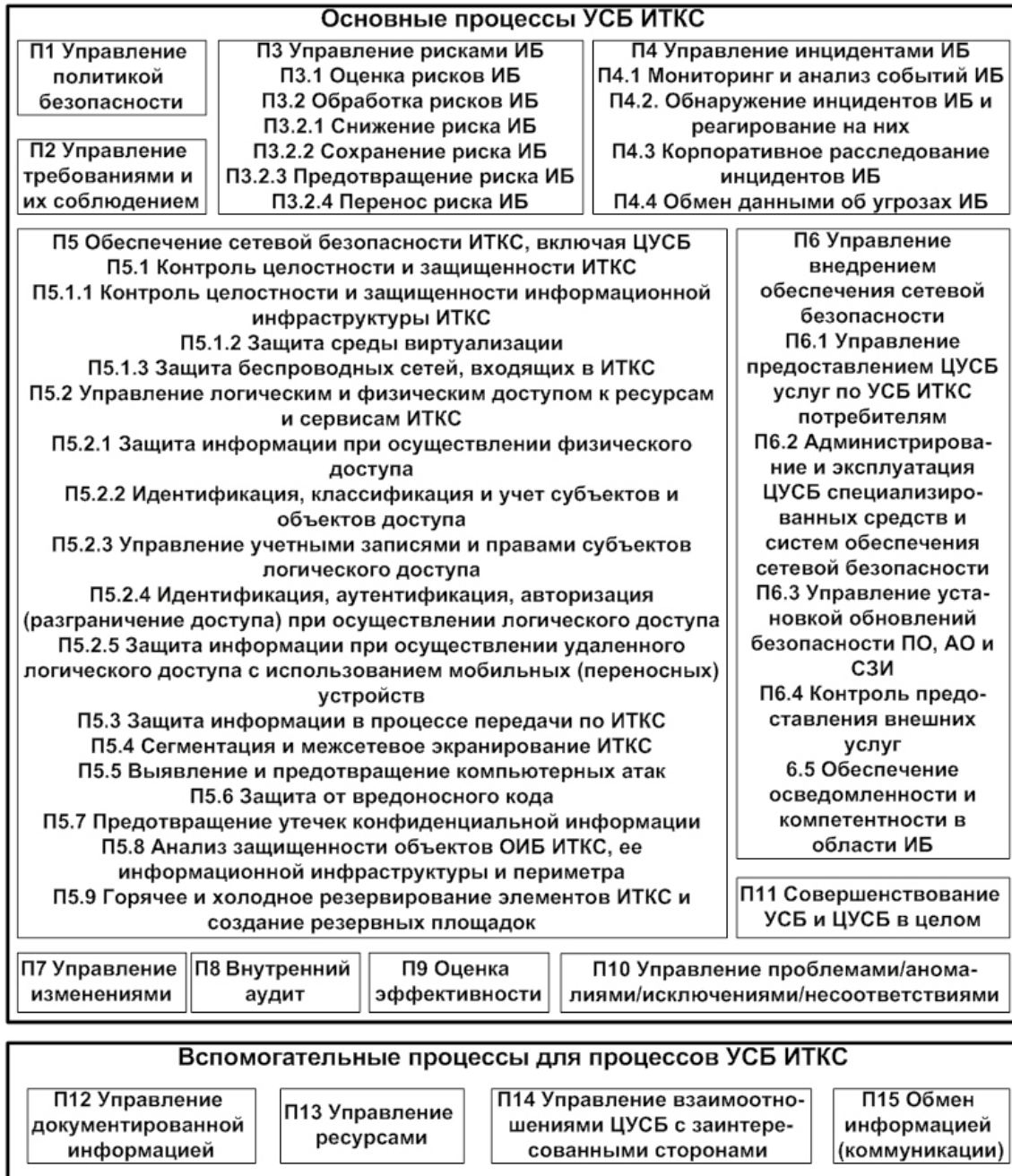


Рис. 3. Процессная модель ЦУСБ

2. ФОРМАЛИЗОВАННОЕ ПРЕДСТАВЛЕНИЕ МОДЕЛИ ЗРЕЛОСТИ ЦУСБ ИТКС

Введем определение *модели зрелости ЦУСБ ИТКС* как структурированного набора элементов, объединяющего информационную потребность

установления уровня зрелости ЦУСБ с их атрибутами (адаптировано на основе [6, 7]). Атрибуты – свойства или характеристики ЦУСБ, которые могут быть определены количественно или качественно вручную или автоматизированными средствами. Информационная потребность – знания (сведения), необходимые для управления целями, задачами, рисками и проблемами. Потребителями

информации могут выступать различные заинтересованные стороны: внутренние (собственники и органы управления, органы контроля, сервисные подразделения и т.п.) и внешние (органы надзора и регулирования, акционеры, инвесторы и т.п.) по отношению к организации, имеющей ЦУСБ. Пять компонентов ЦУСБ можно рассматривать как направления оценки (НО) уровня зрелости ЦУСБ.

Тогда модель зрелости $MЗ_{ЦУСБ}$ может быть представлена следующим кортежем, содержащим в себе пять кортежей для пяти НО уровня зрелости ЦУСБ:

$$MЗ_{ЦУСБ} = \{ЦУСБ, \{OO_{ОФ}, A_{ОФ}, ША_{ОФ}, M_{ОФ}, KOA_{ОФ}, \Phi_{ОФ}, ШУЗ_{ОФ}, УЗ_{ОФ}\}, \{OO_{ПУСБ}, A_{ПУСБ}, ША_{ПУСБ}, M_{ПУСБ}, KOA_{ПУСБ}, \Phi_{ПУСБ}, ШУЗ_{ПУСБ}, УЗ_{ПУСБ}\}, \{OO_{УУСБ}, A_{УУСБ}, ША_{УУСБ}, M_{УУСБ}, KOA_{УУСБ}, \Phi_{УУСБ}, ШУЗ_{УУСБ}, УЗ_{УУСБ}\}, \{OO_T, A_T, ША_T, M_T, KOA_T, \Phi_T, ШУЗ_T, УЗ_T\}, \{OO_K, A_K, ША_K, M_K, KOA_K, \Phi_K, ШУЗ_K, УЗ_K\}, \Phi_{ЦУСБ}, ШУЗ_{ЦУСБ}, ИУЗ_{ЦУСБ}\}, \quad (1)$$

где $ЦУСБ, OO_{НО}$ – множество объектов оценки – ЦУСБ в целом и отдельно каждое НО – $OO = \{oo1, oo2, \dots, ooL\}$, причем L может быть различным для пяти НО – $L1, L2, L3, L4$ и $L5$;

$A_{НО}$ – множество атрибутов более мелких объектов оценки в рамках каждого НО, подлежащих оценке – $A = \{a1, a2, \dots, aN\}$, причем N может быть различным для пяти НО – $N1, N2, N3, N4$ и $N5$;

$ША_{НО}$ – эталонные шкалы для каждого НО как упорядоченные совокупности эталонных значений, которые могут принимать атрибуты объектов оценки данного НО – $SA = \{sa1, sa2, \dots, saN\}$;

$M_{НО}$ – множество методов оценки атрибутов объектов оценки для каждого НО – $M = \{m1, a2, \dots, mN\}$, причем в общем случае M будет различным для всех пяти НО – $M1, M2, M3, M4$ и $M5$ и может быть больше (для оценки одного и того же атрибута применимы несколько альтернативных методов оценки), меньше (к некоторым атрибутам применяются одинаковые методы оценки) или равно (для каждого атрибута применяется свой уникальный метод оценки) соответствующему N ;

$KOA_{НО}$ – критерии оценки значений для атрибутов объектов оценки для каждого НО – $KOA = \{koa1, koa2, \dots, koaN\}$, причем в общем случае N будет различным для всех пяти НО – $N1, N2, N3, N4$ и $N5$;

$\Phi_{НО}$ – функции или методы, объединяющие полученные результаты оценки для всех атрибутов объектов оценки каждого НО в общий показатель уровня зрелости данного НО или числовое значение оценки, характеризующее уровень его зрелости (далее для краткости используется словосочетание

«показатель уровня зрелости»);

$ШУЗ_{НО}$ – эталонные шкалы уровней зрелости для каждого НО;

$УЗ_{НО}$ – результаты оценки для каждого НО в виде конкретного уровня зрелости оцениваемого НО;

$\Phi_{ЦУСБ}$ – функция или метод, обобщающая полученные значения уровней зрелости НО в показатель итогового уровня зрелости ЦУСБ;

$ШУЗ_{ЦУСБ}$ – эталонная шкала уровней зрелости ЦУСБ;

$ИУЗ_{ЦУСБ}$ – итоговый результат оценки в виде конкретного уровня зрелости оцениваемого ЦУСБ.

$MЗ_{ЦУСБ}$ отражает, как выбранные для каждого из пяти НО атрибуты объектов оценки могут быть оценены и преобразованы в результаты оценки, служащие основой для принятия решений об уровне зрелости данного НО.

В качестве единой эталонной шкалы для каждого атрибута установим шкалу со значениями от «0» до «1» с равным шагом как доли от максимального значения или характеристики атрибута:

«неудовлетворительно» (не достигается/не существует или крайне мало свидетельств достижения/существования, не зафиксирован письменно) – в диапазоне 0-0,19(9),

«мало» (в основном или в значительной степени не достигается/не существует, некоторые аспекты достижения атрибута непредсказуемы; зафиксирован письменно, но не формализован каким-либо образом) – в диапазоне 0,2-0,39(9),

«удовлетворительно» (частично достигается/существует, формализован, заверен и опубликован) – в диапазоне 0,4-0,59(9),

«хорошо» (в основном или в значительной степени с редкими исключениями достигается/существует, существуют некоторые недостатки достигаемых значений атрибутов; проверен и подлежит контролю) – в диапазоне 0,6-0,79(9) и

«отлично» (полностью или всегда достигается/существует; значительных недостатков, связанных с полученным значением атрибута, не выявлено) – в диапазоне 0,8-1.

Отметим, что значения границ интервалов могут быть умножены на 100, если при проведении оценки такой подход более понятен и нагляден для отображения ее результатов.

Значение для каждого частного i -го атрибута j -го объекта оценки одного из пяти НО из общего числа L , как правило, рассчитывается как среднее арифметическое значение субъективной оценки z_{aji} всех q_{ji} опрашиваемых лиц (их порядковые номера обозначены индексом q), мнение которых имеет равную значимость (в общем случае q_{ji} для разных атрибутов различны), по принятой шкале по формуле:

$$\overline{zaji} = \frac{\sum_{q=1}^{qji} zaji q}{qji} \quad (2)$$

В формулу можно ввести весовые коэффициенты, учитывающие степень компетентности опрашиваемых лиц, что усложнит дальнейшие расчеты и саму процедуру оценки, поскольку придется дополнительно определять эту компетентность, увеличивая временные и трудовые затраты на общую оценку уровня зрелости. В вырожденном случае, когда для получения значения атрибута можно опросить только одно лицо, среднее значение и будет равно значению, которое выставило это лицо.

Обобщенное групповое значение $3A_j$ для подмножества n_j всех атрибутов данной группы из всего множества атрибутов N j -го объекта оценки с различными весовыми коэффициентами $waji$ вклада значения каждого i -го атрибута в общую оценку объекта рассчитывается как сумма взвешенных значений по формуле:

$$3A_j = \sum_{i=1}^{n_j} (waji * \overline{zaji}) = \sum_{i=1}^{n_j} \left(waji * \left(\frac{\sum_{q=1}^{qji} zaji q}{qji} \right) \right), \quad (3)$$

где $\sum_{i=1}^{n_j} waji = 1$ и $\sum_{j=1}^L n_j = N$. Выбор весовых коэффициентов проводится один раз, например, путем опроса экспертов или на основе собранной статистики, и далее они меняться не должны.

Поскольку эталонная шкала устанавливает значения для атрибутов $zaji$ в диапазоне от «0» до «1», как и для весовых коэффициентов, то обобщенное значение для всех атрибутов одного объекта оценки также будет принимать значение от «0» до «1» (за счет того, что сумма всех весовых коэффициентов равна «1»). [При использовании значений в процентах обобщенное значение будет находиться в диапазоне от «0» до «100».]

Кроме группировки атрибутов по их принадлежности к одному объекту оценки, сами объекты также могут объединяться в некие смысловые группы.

Далее обобщенный результат оценки всех N атрибутов всех L объектов оценки одного НО преобразуется в показатель уровня зрелости ПУЗ этого НО как сумма взвешенных значений атрибутов групповых объектов $3A_j$ в диапазоне от «0» до «1» по формуле:

$$ПУЗ = \sum_{j=1}^L (wooj * 3A_j) = \sum_{j=1}^L (wooj * \sum_{i=1}^{n_j} (waji * \left(\frac{\sum_{q=1}^{qji} zaji q}{qji} \right))), \quad (4)$$

где $wooj$ – весовой коэффициент вклада значения атрибутов для j -го группового объекта оценки в

ПУЗ, причем $\sum_{j=1}^L wooj = 1$.

Для получения показателя уровня зрелости каждого НО в баллах полученное значение ПУЗ в диапазоне от «0» до «1» умножается на 100.

В формулу (4) можно было бы дополнительно ввести корректирующий коэффициент неравномерности, уравнивающий полученные групповые значения в случае их большого разброса, когда в одной группе они очень высокие, а в другой – очень низкие. Но при оценке уровня зрелости это представляется необоснованным, ибо основная задача оценки – выявить реальную картину и наихудшие результаты, подлежащие совершенствованию, а не усредненную («сглаженную») картину.

Также для каждого из результатов оценки и обобщенного показателя уровня зрелости ЦУСБ могут быть определены желательные тенденции их изменения при росте уровня зрелости. Таким образом, в МЗ ЦУСБ заложен систематически повторяющийся процесс оценки совершенствования ЦУСБ на основе выявления повышения результатов оценки уровня зрелости ЦУСБ.

Критерии принятия решения необходимы для определения конкретного уровня зрелости по соотвествию ему показателя уровня зрелости ЦУСБ.

Количество уровней зрелости для пяти НО для удобства дальнейшей интеграции в итоговый уровень зрелости ЦУСБ логично установить одинаковым. На основе лучших практик представляется обоснованным определить пять уровней зрелости каждого НО и ЦУСБ в целом с едиными названиями:

- **«начальный»** – в диапазоне 0-19,99(9) баллов, когда деятельность иерархически организованного ЦУСБ по УСБ ИТКС осуществляется хаотически, от случая к случаю, без единого подхода (так называемое «ситуационное управление» (*Ad hoc*); сами процессы УСБ непредсказуемы и слабо контролируемы;
- **«базовый и повторяемый»** – в диапазоне 20-39,99(9) баллов, когда одинаковые задачи по УСБ ИТКС решаются разными людьми схожими методами, но формализованные процедуры УСБ и распределение ответственности отсутствуют, что увеличивает вероятность ошибок; часто процессы УСБ появляются в ответ на определенные события, а затраты на них могут превышать выделенный бюджет;
- **«установившийся и отслеживаемый»** – в диапазоне 40-59,99(9) баллов, когда процедуры УСБ определены на уровне ЦУСБ (он может быть представлен как некий «конвейер по УСБ ИТКС», стандартизованы (формализуют существующую практику) и документированы, исполняются заблаговременно с управлением качеством, но возможно с превышением бюджета и не всегда прослеживаемыми отклонениями;

- **«управляемый и измеряемый»** – в диапазоне 60-79,99(9) баллов, когда ЦУСБ контролирует по целям и измеряет процессы УСБ по показателям и принимает меры, если они нерезультативны и неэффективны (но риск этого в тактической перспективе минимален, хотя и возможен в стратегической перспективе); могут использоваться инструменты их автоматизации;

- **«оптимизируемый и устойчивый»** – в диапазоне 80-100 баллов, когда процессы УСБ ИТКС, реализуемые ЦУСБ с сетевой организационной структурой, развиты в рамках заранее определяемого бюджета до уровня хорошей практики (риски в тактической и стратегической перспективах минимальны) в результате постоянных улучшений и сравнений, т.е. осуществляется управление изменениями, инновациями и знаниями.

Для перехода от первого уровня ко второму добавляется анализ и повторяемость, от второго к третьему – стандартизация и отслеживаемость, от третьего к четвертому – управляемость и измеряемость и от четвертого к пятому – устойчивость, оптимизируемость и постоянное совершенствование.

В качестве метода, объединяющего полученные значения уровней зрелости НО в показатель итогового уровня зрелости ЦУСБ, логично выбрать минимальное значение из показателей для всех пяти НО (согласно давно известному в ИБ принципу – «уровень ИБ всей системы не может быть выше уровня ИБ самого слабого ее звена»), а не их интегральное значение по какой-либо формуле. Кроме того, нельзя говорить о некоем математическом равенстве уровней зрелости всех пяти НО, но все они важны для достижения высокого уровня зрелости ЦУСБ.

При проведении исследования определены кортежи {ООно, Ано, ШАно, Мно, КОАно, ФНО, ШУЗНО, УЗНО} для каждого из пяти НО, но из-за ограниченного объема статьи в качестве примера рассмотрим только оценку уровня зрелости НО Т.

3. ТЕХНОЛОГИИ, ИСПОЛЬЗУЕМЫЕ ЦУСБ ПРИ ЕГО ФУНКЦИОНИРОВАНИИ

В данной работе принят традиционный взгляд на технологию как совокупность методов, приемов, режимов и способов работы, последовательность действий и процедур, а также средств, оборудования и прочего для достижения желаемого результата их применения в какой-либо отрасли деятельности (обобщено на основе [8, 9]). В широком смысле — это «применение научного знания для решения практических задач», в узком — это «ком-

плекс организационных мер, операций и приемов, направленных на изготовление, обслуживание, ремонт и/или эксплуатацию изделия с номинальным качеством и оптимальными затратами, и обусловленных текущим уровнем развития науки, техники и общества в целом». Технологии должны применяться там, где они способны стать инструментом, помогающим персоналу и поддерживающим процессы, результатом которых являются предоставляемые услуги.

Состав используемых в ЦУСБ технологий УСБ определяется перечнями реализуемых в ЦУСБ процессов УСБ ИТКС и соответственно предоставляемых услуг по УСБ ИТКС. Технологии УСБ во многом определяются более общими технологиями ОИБ, поскольку ОИБ включает в себя УСБ. При этом важно, что УСБ ИТКС как сложным организационно-техническим комплексом потребует применения интегрированных технологий УСБ – взаимосвязанной совокупности отдельных технологий обеспечения сетевой безопасности, а также интеграции средств, поддерживающих эти технологии. В качестве примера приведем лишь некоторые услуги для трех основных процессов УСБ ИТКС:

П1 Управление политикой безопасности:

T1.1 Технологии управления ОРД по УСБ ИТКС (интеграция с единым информационным пространством организации, организация хранилищ документов в области УСБ, управление жизненным циклом ОРД и т.п.);

T1.2 Автоматизированные средства (АвтС) управления ОРД по УСБ ИТКС (разработка и оценка рисков ИБ из-за некорректной разработки; не электронный документооборот);

T1.3 АвтС составления и ведения реестра ОРД...

П2 Управление требованиями и их соблюдением:

T2.1 Технологии управления выполнением нормативных и иных требований по ОИБ для ИТКС (идентификация, документирование, анализ, приоритизация требований, отслеживание выполнения, достижение соглашения по требованиям, управление изменениями, уведомление соответствующих лиц и т.п.);

T2.2 АвтС управления выполнением нормативных и иных требований по ОИБ для ИТКС (поиск несоблюдения требований и уязвимостей объектов ИТКС, выдача рекомендаций по устранению несоответствий и уязвимостей и т.п.);

T2.3 АвтС составления отчетности об управлении требованиями и их соблюдением...

П4.3 Корпоративное расследование инцидентов ИБ:

Т4.3.1 Технологии планирования расследования инцидентов ИБ и обоснованного выбора средств для корпоративного расследования инцидентов ИБ ИТКС;

Т4.3.2 Технологии получения, сохранения и проверки на неоспоримость собранных цифровых свидетельств инцидентов ИБ (компьютерно-техническая экспертиза; интервьюирование; наблюдение; сканирование; копирование; назначение приоритетов сбора свидетельств и расследования и т.п.);

Т4.3.3 Технологии защищенного хранения и поддержки целостности носителей информации со свидетельствами (резервное копирование, контрольные суммы и т.п.);

Т4.3.4 Технологии проведения экспертизы, анализа и обработки результатов анализа для понимания инцидента ИБ (выяснение причин и масштаба инцидента; установление внутренних нарушителей ИБ; статус расследования; экспертная поддержка расследования и сопровождение внешних расследований и т.п.);

Т4.3.5 Технологии составления сценариев инцидентов ИБ на основе полученных во время расследования знаний (синтез новых знаний; формализованные нотации описания сценариев и т.п.);

Т4.3.6 БД ИБ с централизованной ИБ-аналитической организацией;

Т4.3.7 АвтС составления отчетности о корпоративных расследованиях инцидентов ИБ.

Назовем также некоторые услуги для вспомогательного процесса УСБ ИТКС **П15 Обмен информацией (коммуникации):**

Т15.1 Технологии обмена информацией (надежная консолидированная электронная почта, IP-телефония, доступ в интернет и т.п.);

Т15.2 АвтС коммуникации рисков ИБ ИТКС;

Т15.3 АвтС согласования требований по ОИБ для объектов ОИБ в ИТКС;

Т15.4 АвтС предоставлению информации заинтересованным сторонам (НКЦКИ, ЦУСБ других организаций, СМИ, правоохранительным и судебным органам и т.д.);

Т15.5 АвтС защиты электронной почты;

Т15.6 АвтС, предоставляющие централизованную видимость расследования инцидентов ИБ и немедленный доступ к имеющимся свидетельствам;

Т15.7 АвтС предоставления отчетности об обмене информацией.

Даже по этому «урезанному» перечню видно, что в ЦУСБ внедряются различные технологические инновации, такие как автоматизация операций по УСБ и оркестрация для координации взаимодействия при осуществлении деятельности по УСБ

ИТКС. Это проявляется, например, в следующем:

- комплексная интеграция моделирования подлежащих защите активов, анализа их уязвимостей, выделения актуальных угроз ИБ и рисков ИБ для них и контекстного связывания с активами TI-платформ (*om Threat Intelligence*);

- интеграция источников данных мониторинга ИБ и ЖРС и разработка коннекторов для связи с источниками;

- управление вариантами использования для одного или нескольких устройств и сопоставление с ними угроз ИБ и соответствующих требований по ОИБ;

- совместный анализ поведения пользователей;

- управление потоками данных о событиях в ИТКС из различных источников (систем физической защиты, аутентификации, мониторинга и т.п.) и агрегирование этих потоков посредством SIEM/SOAR-систем, EDR/XDR-платформ, объединенной системы управления ЖРС, TI-платформы, информационных панелей собственной разработки, средства автоматизации рабочих процедур для централизованной и расширенной ИБ-аналитики больших относящихся к ИБ ИТКС данных;

- захват всех сетевых пакетов для дальнейшего расследования, как и совместный контекстный анализ событий на серверах и рабочих станциях пользователей;

- круглосуточный мониторинг аварийных сигналов с дублированием для последующего более детального анализа и автоматизированное преобразование сигналов тревоги от СЗИ в данные о компьютерных атаках;

- комплексная ИБ-аналитика, включая упреждающий поиск угроз ИБ с применением искусственного интеллекта, анализ сценариев инцидентов ИБ на основе MITRE ATT&CK и IoCs и контекстный анализ при рассмотрении всех имеющихся свидетельств;

- совместная визуализация данных из ЖРС, уязвимостей и произошедших инцидентов ИБ и т.п.

4. ОЦЕНКА УРОВНЯ ЗРЕЛОСТИ ТЕХНОЛОГИЙ, ПОДДЕРЖИВАЮЩИХ ФУНКЦИОНИРОВАНИЕ ЦУСБ

Кривая зрелости технологий для бизнеса «*Нуре Cycle*» предложена компанией Gartner еще в 1995 г. [10] и отображает стадии, через которые проходит любая технология. Кривая имеет пять фаз (рис. 4) [11]: «запуск» с ожиданием технологического про-

рыва, «пик завышенных ожиданий» (обычно нереалистичных), «пропасть разочарования» (из-за несоответствия завышенным ожиданиям), «склон просвещения» (с пересмотром идей и корректировкой

технологии) и «плато продуктивности» (когда она при применении дает признанные преимущества и эволюционирует).

ЦИКЛ ЗРЕЛОСТИ ТЕХНОЛОГИЙ

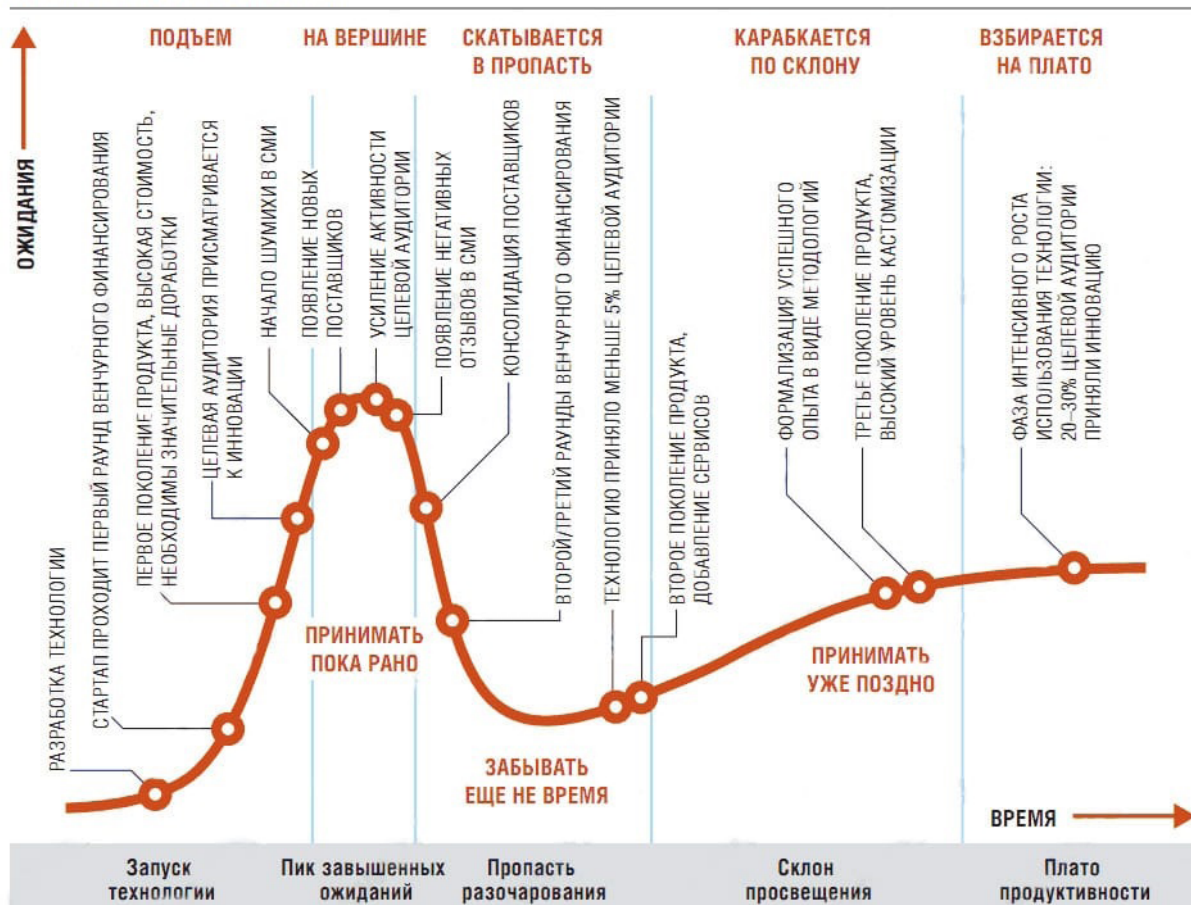


Рис. 4. Кривая зрелости технологий компании Gartner [11]

Также известен ГОСТ Р 58048-2017 [12], определяющий унифицированную методику оценки зрелости технологий и систем с их применением через соответствующие уровни готовности технологии (УГТ). Они используются «для оценки текущего состояния вновь разрабатываемых или приобретаемых технологий и компонентов сложных технических систем... при создании целевых и обеспечивающих систем», «перевода разрабатываемой технологии на следующую стадию жизненного цикла» и разработке планов совершенствования систем, их компонентов и соответствующих технологий производства. Такую оценку рекомендуется применять, начиная со стадии замысла, «при отборе ... технологии из ... доступных для последующего использования в целевой системе (анализ альтернатив)», что полностью применимо к ЦУСБ и ее системам. В случае низкого уровня зрелости технологии для создания системы с ее применением разрабатывается

план развития с указанием необходимых ресурсов, сроков и оценкой возможных рисков.

Определим все элементы модели зрелости (1) для кортежа T.

OO_T – множество объектов оценки в рамках направления T, разделенных на собственно технологии и АвтС с применением этих технологий (из-за ограниченного объема статьи их список не приводится): 11 групповых объектов (их количество – L41) и 4 групповых (их количество – L42). Общее количество объектов оценки по двум составляющим $L4=L41+L42=219+20=239$.

A_T – множество атрибутов объектов оценки $T - A = \{a1, a2, ..., aN4\}$. Применимость УГТ из [12] в качестве атрибута имеет ограничения, поскольку не определяет в полной мере техническое совершенство технологии и АвтС на ее основе, зависит от контекста применения (в разных АвтС одна и та же технология может иметь разные УГТ), опера-

ционного окружения и возможных архитектурных несоответствий (технология в одной АвТС может потребовать доработок при применении в другой). Чтобы устранить эти ограничения, для каждого объекта оценки УГТ оценивается отдельно на разных стадиях жизненного цикла технологии и АвТС с их применением, а именно, замысел, разработка, производство, применение, поддержка и выведение из эксплуатации [13].

Оценку уровня зрелости реализации технологий УСБ, направленных на непосредственное ОИБ ИТКС осуществляют отдельно для каждой технологии и АвТС, применяющих эти технологии. С учетом УГТ из [12] и стадий жизненного цикла из [11-13] предложены следующие атрибуты:

— для технологий: «Разработка и уточнение концепции технологии», «Подтверждение концепции технологии аналитическим и экспериментальным путем», «Испытание технологии в лабораторных условиях и окружении, близком к реальному», «Формулирование принципов и способов применения технологии», «Применение технологии в условиях эксплуатации», «Сопровождение технологии в процессе эксплуатации» и «Выведение технологии из эксплуатации»;

— для АвТС с применением технологий: «Разработка требований и проекта системы», «Разработка/доработка прототипа системы/реальной системы и рабочей документации для нее», «Тестирование прототипа системы в лабораторных условиях и окружении, близком к реальному», «Демонстрация возможностей прототипа системы в условиях эксплуатации», «Ввод в действие реальной системы и ее применение», «Сопровождение реальной системы в процессе эксплуатации» и «Выведение реальной системы из эксплуатации». Эти атрибуты для АвТС ЦУСБ определяются с учетом функциональной (АвТС самая простая в своем классе по функциональным возможностям или «продвинутая» (*Advanced*) или «нового поколения» (*Next Generation*)) и физической архитектуры АвТС и критических элементов технологии в ее составе. Примером того, что должно оцениваться для АвТС «SIEM-система» на стадии ее применения является реализации в ней следующих функций: непрерывное слежение за соблюдением всех применимых к ИТКС организации требований по ОИБ, поддержка централизованного управления политиками ИБ при обработке данных в ИТКС для различных сегментов и устройств, многопоточный сбор данных из ЖРС для их анализа, выполнение функций индикатора раннего предупреждения об угрозах ИБ и КА, использование информационных панелей (dashboards), отображающих процесс

управления ЦУСБ инцидентами ИБ в ИТКС, способы реагирования на выявленные инциденты ИБ и многое другое.

$ША_T$ – шкалы эталонных значений, которые могут принимать атрибуты объектов оценки $T - SA = \{sa1, sa2, \dots, saN4\}$: «**неудовлетворительно**» – технология и АвТС применяются в диапазоне 0-0,19(9), «мало» – в диапазоне 0,2-0,39(9), «**удовлетворительно**» – в диапазоне 0,4-0,59(9), «**хорошо**» – в диапазоне 0,6-0,79(9) и «**отлично**» – в диапазоне 0,8-1.

M_T – множество методов оценки атрибутов объектов оценки $T - M = \{m1, a2, \dots, mN4\}$, причем $N4$ может быть больше, меньше или равно $N4$. Доступными методами оценки атрибутов для направления T служат опросы и анкетирование уполномоченных лиц. Опросник (калькулятор) для оценки УГТ из [11] применим и к технологиям и АвТС с их применением, используемым в ЦУСБ. Например, для атрибута «Реальная АвТС подтверждена путем успешной эксплуатации (достижения цели)» необходимо ответить среди прочих на вопросы об установке системы, стабильности ее работы и завершении разработки всей документации на нее.

KOA_T – критерии оценки значений для атрибутов объектов оценки $T - KOA = \{koa1, koa2, \dots, koaN4\}$. Примером критерия оценки (счетных, основанных на наблюдаемых фактах или заполняемых анкетах) из всей совокупности требований может быть требование «Любое взаимодействие работников ЦУСБ с контролирующими органами фиксируется в электронном журнале взаимодействий». Сами критерии связаны со значениями границ диапазонов эталонной шкалы. Вывод об уровне зрелости конкретной технологии или АвТС делается на основе свидетельств, в качестве основных источников которых могут выступать ОРД организации, относящиеся к ОИБ ИТКС, устные высказывания работников, результаты наблюдений проводящих оценку уровня зрелости ЦУСБ, параметры конфигурационных настроек СЗИ, технические и программные средства сбора свидетельств типа ЖРС, отчеты об уязвимостях и проведенных тестированиях на проникновение и т.п.).

Φ_T – функция или метод, объединяющий полученные значения атрибутов всех объектов оценки T в общий показатель уровня зрелости T . При выборе такой функции необходимо руководствоваться следующими рассуждениями: если для оцениваемой технологии и АвТС с ее применением половина объектов оценки получили максимальный балл по эталонной шкале уровня зрелости, а остальные – низкий, то общий уровень зрелости этой технологии и

АвтС с ее применением в целом считать высоким или даже средним не представляется возможным. Уровень зрелости АвтС напрямую зависит от зрелости используемых в них технологий, чаще не одной, а нескольких, и корректности их интеграции в единой системе.

Приняв вклад 11 основных и 4 вспомогательных технологий в показатель уровня зрелости технологий зависимым от общего количества технологий и внося названия этих двух групп технологий в соответствующие индексы, получим формулу:

$$ПУЗ_T = 11/15(ПУЗ_{OT-T} + ПУЗ_{OT-АсмС}) + 4/15(ПУЗ_{BT-T} + ПУЗ_{BT-АсмС}), \quad (5)$$

$$\text{где } ПУЗ_{OT-T} = \sum_{j=1}^{11} (wootj1 * 3Atj1) = \sum_{j=1}^{11} (wootj1 * \sum_{i=1}^{ntj1} (watj1i * \left(\frac{\sum_{q=1}^{qtj1i} zatj1iq}{qtj1i} \right))),$$

$$ПУЗ_{OT-АсмС} = \sum_{j=1}^{11} (woosj1 * 3Asj1) = \sum_{j=1}^{11} (woosj1 * \sum_{i=1}^{nsj1} (wasj1i * \left(\frac{\sum_{q=1}^{qsj1i} zasj1iq}{qsj1i} \right))),$$

$$ПУЗ_{BT-T} = \sum_{j=1}^4 (wootj2 * 3Atj2) = \sum_{j=1}^4 (wootj2 * \sum_{i=1}^{ntj2} (watj2i * \left(\frac{\sum_{q=1}^{qtj2i} zatj2iq}{qtj2i} \right))),$$

$$ПУЗ_{BT-АсмС} = \sum_{j=1}^4 (woosj2 * 3Asj2) = \sum_{j=1}^4 (woosj2 * \sum_{i=1}^{nsj2} (wasj2i * \left(\frac{\sum_{q=1}^{qsj2i} zasj2iq}{qsj2i} \right))).$$

Для всех $wootj$, $3Atj$, $watji$, $zatjiq$ и $qtji$ для технологий и для всех $woosj$, $3Asj$, $wasji$, $zasjiq$ и $qsji$ для АвтС с применением технологий опустим индекс Т. При необходимости вклад основных технологий по сравнению со вспомогательными можно увеличить, но это будет не совсем оправданно, поскольку без наличия вспомогательных технологий или при их «незрелости» уровень зрелости основных гарантированно снизится.

$ШУЗ_T$ – эталонная шкала уровней зрелости Т, представленная в разделе 2.

$УЗ_T$ – результат оценки в виде одного из пяти возможных уровней зрелости Т – «начальный», «базовый и повторяемый», «установившийся и отслеживаемый», «управляемый и измеряемый» или «оптимизируемый и устойчивый», полученный после определения попадания $ПУЗ_T$ в один из интервалов эталонной шкалы уровней зрелости Т.

взаимными НО – организационное обеспечение, процессы УСБ ИТКС, предоставляемые услуги по УСБ ИТКС, поддерживающие процессы и услуги технологии и кадровое обеспечение. После этого определена модель зрелости $M_{ЦУСБ}^3$ как кортеж, содержащий в себе пять кортежей для пяти НО. Далее подробно описаны все элементы кортежа для НО Т – технологий и АвтС с их применением. Даны необходимые пояснения с примерами, показывающими их конкретное применение.

Представленные результаты работы универсальны, поскольку они могут быть применены при оценке ЦУСБ разного уровня зрелости с типовым набором объектов оценки. Изложенный подход к рассмотрению технологий и оценки уровня их зрелости может быть адаптирован под потребности конкретной организации (например, в части уточнения объектов оценки и их атрибутов), которая начинает построение своего ЦУСБ. В дальнейшем планируется создание методики применения разработанной модели.

ЗАКЛЮЧЕНИЕ

Представлено общее описание ЦУСБ ИТКС как объекта оценки уровня зрелости с пятью взаимос-

СПИСОК ЛИТЕРАТУРЫ

1. Милославская Н.Г. Научные основы построения центров управления сетевой безопасностью в информационно-телекоммуникационных сетях. М., Горячая Линия-Телеком, 2021. 431 с.
2. О безопасности критической информационной инфраструктуры Российской Федерации [федер. закон от 26 июля 2017 г. № 187-ФЗ: принят Гос. Думой 12 июля 2017 г.; одобрен Советом Федерации 19 июля 2017 г.]. 2017. 20 с.

3. ГОСТ Р ИСО/МЭК 27033-1-2011 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции. Введ. 2012-01-01. М., Стандартинформ, 2012. 73 с.
4. Kaliyaperumal L.N. The Evolution of Security Operations and Strategies for Building and Effective SOC. ISACA Journal, October 2021. Vol. 5. 9 p. URL: <https://www.isaca.org/resources/isaca-journal/issues/2021/volume-5/the-evolution-of-security-operations-and-strategies-for-building-an-effective-soc> (дата обращения: 07.04.2023).
5. Crowley C., Pescatore J. The Definition of SOC-cess? SANS 2018 Security Operations Center Survey. SANS, 2018. URL: <https://www.arista.com/assets/data/pdf/Whitepapers/Survey-SOC-2018-AwakeSecurity.pdf> (дата обращения: 07.04.2023).
6. ISO/IEC/IEEE 15939:2017 Systems and software engineering — Measurement process. 2017. 39 p.
7. ГОСТ Р ИСО/МЭК 27004–2021 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Мониторинг, оценка защищенности, анализ и оценивание. Введ. 2021-11-30. М., Стандартинформ, 2021. 46 с.
8. Сарыбеков М.Н., Сыдыкназаров М.К. Словарь науки. Общенаучные термины и определения, науковедческие понятия и категории: Учебное пособие. Издание 2-ое, доп. и перераб. Алматы: ТРИУМФ-Т, 2008. 504 с.
9. Кемеров В.Е., Азаренко С.А., Керимов Т.Х. Современный философский словарь. Академический проспект, 2015. 823 с.
10. Gartner Hype Cycle. Gartner, 1995. URL: <https://www.gartner.com/en/research/methodologies/gartner-hype-cycle> (дата обращения: 07.04.2023).
11. Кривая Гартнера: Как оценить возможности технологических инноваций для бизнеса. Bitobe, 2021. URL: <https://blog.bitobe.ru/article/krivaya-gartnera/> (дата обращения: 07.04.2023).
12. ГОСТ Р 58048-2017 Трансфер технологий. Методические указания по оценке уровня зрелости технологий. Введ. 2018-06-01. М., Стандартинформ, 2018. 38 с.
13. ГОСТ Р 57193-2016 Системная и программная инженерия. Процессы жизненного цикла систем. Введ. 2017-11-01. М., Стандартинформ, 2018. 95 с.

Социальная физика 5.0

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».*

ПРЕДИСЛОВИЕ

На начальном этапе формулирования научной парадигмы часто принято и считается хорошим тоном обратиться к классическому периоду Древней Греции. Следуя традиции, скажем, что первым, кто предположил, что живые объекты существуют по тем же законам, что и неживые, был Эпикур. И хотя во многом его убеждения явно проистекали из атомистики Демокрита, в чём-то он сильно разошёлся во взглядах со своим учителем, введя понятие непредсказуемого отклонения атомов и открыв, таким образом, дорогу человеческой свободной воле. Из-за малого числа дошедших до нас работ Эпикура сложно сказать, было ли его такое «особое мнение» как-то связано с аристотелевой «энтелехией» как пониманием внутреннего потенциала (силы) живых организмов, одновременного интегратора и цели, и результата. С некоторой уверенностью можно лишь утверждать, что Эпикур, помимо атомистики Демокрита, разделял ещё и эмпиризм Аристотеля, заполняя, в известном смысле, некоторую промежуточность позиции.

Просуществовав, пусть весьма противоречиво, до нового времени, учения Демокрита и Аристотеля были переосмыслены как заделы для механицистов и виталистов. Если с первым взглядом всё было линейно (Декарт и его механические автоматы, Ламетри и его «Человек-машина» и «Человек-растение»), то со вторым – неочевидно до сих пор. И Месмер с его неверно переведённым и понятным животным магнетизмом, и знаменитый Франклин (изображенный на купюре «100 долларов»), и Вёлер, нанесший главный удар по теории витализма, так и не смогли окончательно уничтожить учение о жизненной силе. Хотя сегодня это, похоже, к лучшему.

Учение же Эпикура в этот «второй подход к снаряду» было вовлечено лишь частично, сильно трансформировавшись и перейдя в психологические планы. В этом смысле оно для нас в рамках

исследования по социальной физике не представляет интереса. Для строгости можно условно объединить социальную физику периода с V века до н.э. по XVIII век н.э. включительно в категорию социальной физики 0.0, хотя прямо о закономерностях существования общностей живых организмов она не говорила.

В 1803-м французский мыслитель Анри Сен-Симон высказал идею описания общества в рамках и по законам общей науки об организмах (так во Франции начала XIX-го века называли физиологию). Его ученик Огюст Конт в 1822-м шагнул дальше и назвал новую научную отрасль социальной физикой, определив её как науку, «которая занимается социальными явлениями, рассматривая их в том же свете, что и астрономические, физические, химические и физиологические явления; они подчиняются естественным неизменным законам, открытие которых является особым объектом исследований человека». Так родилась социальная физика 1.0.

Через несколько лет, бельгийский статистик Кетле сузил естественные законы, годные для описания общества, до нескольких разделов математики. Он заимствовал термин и переопределил социальную физику как дисциплину измеряемых переменных, подчиняющихся нормальному распределению. Так развивающаяся научная отрасль инвертировалась и стала сегментом статистики с высокой степенью привязки к теории вероятности. Появилась социальная физика 2.0.

Контю крайне не понравилось такое «переопределение» социальной физики; он посчитал нужным и придумал новый термин; собственно – социологию. «Я считаю своим долгом отныне пойти на риск с этим новым термином, полностью эквивалентным ранее введённому мною выражению «социальная физика», чтобы иметь возможность обозначать через одно имя существительное эту дополнительную часть натуральной философии, которая положительно изучает совокупность основных законов, относящихся к социальным явлениям», – написал Конт в 1839-м (47-я лекция «Курса

позитивной философии»).

Это не была просто битва за приоритет, это была битва за сущность. Взгляды Конта на общество были социологически реалистичны; он видел объектом социальной физики общество, столь же реальное, как сама природа. Кетле же смотрел на общество с позиций номинализма и редуцировал социальную физику до «средней температуры по больнице». В итоге и индивид, и само общество у Кетле получались, по сути, фиктивными. Или если добавить академического понимания, модельными.

Моделировать общество статистикой оказалось легче. Да и вариативности в суждениях, оценках и выводах математика давала больше. Как результат, социологию постигла участь социальной физики 1.0. Около 100 лет (вторая половина XIX-го и первая половина XX-го веков), на фоне бродящего по Европе призрака коммунизма, социология, как образ социальной физики 2.0, оказалась столь востребованной, что её бурное развитие вообще перестало нуждаться в физических законах и сложных ассоциациях. Во всяком случае, обращаться к ним. Типичный представитель той социологии Сорокин продемонстрировал, насколько структуры и понятия условного заказа стали важнее изначальной строгости и обширности замысла.

С середины XX-го века и до начала 80-х годов предпринимались отдельные попытки возродить социальную физику, но они не были успешны. Стюарт пытался описать социальные взаимодействия с помощью моделей гравитации, Иберал пробовал гомеокинетику для социальных систем, а Пригожин тщательно изучал социоприменимость неравновесной физики. Это лишь несколько примеров попыток вернуться к социальной физике; они не привели к большим успехам и не были приняты научным сообществом, но оставили свой след в науке. Поэтому мы эти попытки объединяем под определением социальной физики 3.0.

Наконец, уже в наше время, меньше десяти лет назад, профессор Массачусетского технологического института Алекс Пентленд, «переопределил» социальную физику как применительную практику анализа «больших данных». Используя наглядные образы наподобие «хлебных крошек», он предложил новое её прочтение. По сути, эта новация, так же, как и работы Барабаши, Болла, Бьюкенена и Хелбинга, предлагает современный вариант социальной физики Кетле (доминирующей). Из уважения к совершенным за два столетия технологическим достижениям человечества и соглашаясь с коллегами, увидевшими в «больших данных» перспективы нового охвата, назовём предложенный

подход социальной физикой 4.0.

На фоне этих процессов хотелось бы предпринять попытку разобраться, есть ли место в нашей жизни для социальной физики 5.0, реально опирающейся на уже известные нам физические законы; будет ли она востребована и для решения каких задач? Или правильнее сдать первоначальный замысел Огюста Конта в архив науки, уважительно вспоминая о нём лишь в ретроспективе? Описание этой попытки мы и представляем вниманию читателя.

ВВЕДЕНИЕ

Человечество финитно, и если верна наша современная физическая картина мира, то у человеческой цивилизации нет шансов на вечное существование. Вопрос только в том, когда закончится человеческое земное существование и как именно это произойдёт. Мы затронем эту тему ниже и попробуем увидеть свет в конце тоннеля: совсем не факт, что в этих суждениях заключается приговор. Возможны разные сценарии, в том числе вполне положительные.

В соответствии с учением Конта современная человеческая цивилизация, как глобальный социальный организм, должна иметь свой жизненный цикл. В таком случае мы находимся во второй его половине. Почему это так, мы попробуем показать в работе, отталкиваясь от существующих в физике понятий. Здесь же важно, что человек сам себе избрал все физические концепты, стремясь построить стройную картину мира в аспекте субъектно-объектных отношений.

Если мы верим, что она (картина) построена, и кажется нам стройной при взгляде на неё условно левым глазом физики, то почему она должна быть иной при взгляде вторым, правым глазом? Имеется в виду аспект субъект-субъектных отношений или взгляд гуманитария. Продолжая аналогию социума в виде «большого» человека, придётся предположить, что субъект с такой устойчивостью разных взглядов будет, скорее всего, медицинским пациентом с диагнозом F44-го класса из МКБ-10 («Диссоциативные расстройства»).

С такой гипотезой о нашей изначальной социумной порочности мы соглашаться не хотим, но готовы её проверить.

Для этого вернёмся к концепциям жизненного цикла (ЖЦ), которых на сегодняшний день разработано множество. Дальше всего по пути учёта особенностей ЖЦ мы продвинулись в роли прагматичных нефтяников (ЖЦ месторождений), цинич-

ных финансистов (ЖЦ инвестиций) и созидательных маркетологов (ЖЦ продуктов). В этой роли мы лучше остальных осознаём разницу в стадиях жизненного цикла, принимаем их как данность, определяем и описываем их, отталкиваемся от них при любом планировании и в своей практической деятельности.

В роли социологов мы оказываемся в странной двойственной позиции. С одной стороны, мы явно настраиваемся на то, что человек смертен (в этом убеждении мы уступаем лишь медикам и биологам), и начинаем разрабатывать социоформирующие признаки, устанавливать различия мотиваций и проявлений, обсуждать потребности и т.д. В то же время мы описываем жизненный цикл семьи и отдельных социальных групп, исследуем жизненные циклы прошлых цивилизаций.

Концепции жизненного цикла отражены в трудах Вернадского, Гумилёва, Модильяни, Планка, Рамштадта, Тойнби и многих других ученых; многие работы есть в открытом доступе в сети Интернет.

Признав конечность наших отдельных социальных институтов, мы затрудняемся признать, что и главная наша общность (человечество) также имеет жизненный цикл.

Главная причина такой успокоенности – вера в эволюцию. В рамках текущей парадигмы эволюционный механизм очень прост: всё живое реплицируется, создавая свои копии. Всегда присутствующие в копиях небольшие, в сравнении с оригиналом, изменения, запускают состязание жизней. Те копии, что в одинаковых условиях имеют преимущества перед иными, реплицируются эффективнее: у них более многочисленное и сильное потомство. Передавая же свои полезные изменения по наследству, «чемпионы» прошлого через статус-кво настоящего создают залог для состязания в будущем. Мы считаем этот процесс вечным, при этом осознаваемая нами «история становится все более концентрированной» (И.М. Дьяконов).

Мы даже подсчитали (Иванов): неолит прожил 32 века, восточные рабовладения – 22 века, античная цивилизация – 12 веков, раннее феодальное общество – семь веков, доиндустриальное – четыре с половиной века, индустриальное – 130 лет, а информационное общество – пока только 50 лет.

Влияния внешней среды и внутренние конфликтные напряжения мы называем при этом факторами мутации, выступая в роли отстраненного наблюдателя.

Но ведь этот биологический, в своём изначальном звучании, концепт – тоже часть картины, видимой левым глазом. Тем же самым, которым на

реальность смотрит физика. Так почему биологический понятийный аппарат и законы биологии мы для описания/объяснения социальной реальности приемлем, а концепты физики – нет? Ведь здесь возможные содержательные расхождения уже опаснее: это не просто разница субъектно-объектного взгляда (правый глаз) с субъектно-субъектным (левый), а уже расхождение внутри одного глаза, одного взгляда, одного аспекта. Их невозможно объяснить бинокулярностью науки. И если это расхождение реально, а именно так всё и выглядит, то тогда это заболевание уже похоже на класс F20 из МКБ-10 («Шизофрения»), что хуже и тяжелее.

Ниже физические понятия лишь вводятся для последующих рассуждений. Поэтому они приведены не по значимости для исследования, а в алфавитном порядке. С той же целью мы дали каждому из них краткое описание и привели в алфавитном порядке, исходя из наших субъективных представлений, по пять имён лидеров.

Вероятность. Сильное и многозначное понятие, комфортно соседствующее с категориями случайности и неопределённости. Оно имеет как минимум три аспектных наполнения: субъективное, априорное и частотное. Первое, к примеру, используют психологи, поскольку оно касается степени уверенности индивида в том, что какое-то событие произойдёт. К сторонникам второго можно с уверенностью отнести, скажем, биологов, на основе теоретического знания вероятностно прогнозирующих цвет глаз ребёнка, зная цвет глаз его родителей. Лагерь сторонников третьего аспекта (относится к области статистики) – самый большой.

Важные имена: Байес, Вентцель, Гильберт, Лотфи А. Заде, де Море.

Время. По большому счёту это эмпирическое понятие, о сущности которого современная физика ничего сказать не может. Явления времени умом непостижимы, его математика остаётся непосильной задачей и более конструктивного определения, чем «время – это то, что измеряется по часам», найти сегодня нельзя. Мы даже измеряем его эмпирически. Все шесть основных единиц измерения в международной системе привязаны к фундаментальным физическим константам, но не время. Никто не может объяснить, почему секунда равна $9\,192\,631\,770$ неких колебаний атома цезия-133 при абсолютном нуле. Сегодня Международное бюро мер и весов создаёт дорожную карту и набор критериев, чтобы к 2030-му году выбрать один из девяти новых вариантов определения секунды; они тоже эмпирические.

29 июня 2022 Земля обернулась вокруг своей оси

на 1,59 мс быстрее 24 часов; это самый быстрый её оборот за все приблизительно 60 лет измерений. Физики говорят, что с 2020 года наша планета уже примерно двадцать раз побила рекорды скорости своего вращения; но объяснить причины они не могут. Пока лишь зафиксируем, что ни одна из «теорий» времени не поясняет нам его сущность.

Важные имена: Куайн, Мак-Таггарт, Минковский, Нётер, Хокинг.

Вязкость. Называемое ещё внутренним трением, это относительно несложное, но важное понятие, характеризующее способность среды оказывать сопротивление перемещению одной её части относительно другой её же части. Считая вязкость физической характеристикой любых сред, их текучесть, деформации и нелинейные проявления изучает реология. Физика жизни, в этом смысле, есть физика структурной вязкости. Плохо то, что строгой теории вязкости также не существует, а большинство описывающих её положений эмпирические.

Важные имена: Бингам, Воларович, Навье, Пуазейль, Ребиндер.

Гравитация. Одно из четырёх фундаментальных взаимодействий, благодаря которым мир такой, какой он есть. Наиболее просто и часто осознаваемый в обычной жизни, феномен гравитации сегодня «официально» описывается общей теорией относительности Эйнштейна 1915-го года, сменившей закон всемирного тяготения Ньютона от 1667-го, считавший гравитацию силой.

Также мы имеем открытые в 2015-м гравитационные волны и не обнаруженный пока гравитон. А благодаря голливудской просветительской деятельности мы имеем ещё много смутных образов вроде «чёрных дыр» и «горизонта событий». Более того, большинство людей сегодня знает, что гравитация всегда притягивает и никогда не отталкивает. Кому-то интересно, почему девушка весом 60 кг на Юпитере будет весить 142 кг, и единицы помнят со студенчества, что гравитация теперь больше не сила, а свойство искривления пространства и времени под действием массы.

Важные имена: Венециано, Дикке, Кеплер, Ньютон, Эйнштейн.

Дуализм. Интересное и многозначное понятие корпускулярно-волнового свойства материи. К концу XIX века физика объявила двумя видами реальности тварного мира дискретное вещество и непрерывное поле. У вещества при этом понятие массы было, а у поля, очевидно, нет. Однако открытия начала XX-го века разрушили эту «мещанскую» картину, неоднократно установив при рассмотрении электромагнитных полей проявления для больших

длин волн континуальных свойств, а для меньших длин – дискретных. Так в физику пришло диалектическое единство двух противоположностей.

В 1924-м году, отталкиваясь от законов симметрии, принцип корпускулярно-волнового дуализма был распространён на все частицы микромира, имеющие массу покоя. Так родилась квантовая механика, которой все пользуются, но никто не понимает. Хотя именно она дала нам ту жизнь, которой мы сейчас живём: вся энергетика, включая «зелёную», вся современная электроника, компьютеры/интернет/гаджеты имеет одну основу – дуализм.

В попытках всё-таки понять, а не просто использовать, физика углубилась в такие дебри, что до сих пор пытается в них найти хоть какой-то консенсус. Но есть пара действительно важных для наших целей проявлений дуализма: эффект наблюдателя и принцип неопределённости.

Важные имена: де Бройль, Столетов, Фабрикант, Фейнман, Шрёдингер.

Динамика. Наиболее подходящее нам определение динамики – это изучение причин возникновения и особенностей любых процессов, развивающихся во времени. С учётом того, что мы не видим понятие времени, понятие динамики включает элемент неопределённости. Тем не менее, конкретные её механизмы и методы вполне ясны и определяются предметной природой; термо-, электро-, гидро-, газо- и иные виды динамики выглядят сегодня вполне проработанными областями физики, так или иначе имеющими подобие с той динамикой, которая является частью механики. Не все они оперируют опорными понятиями классической динамики (масса, сила, импульс, энергия), но в них есть свои базовые задачи, основные принципы, гуру и авторитеты.

Считается, что для описания динамики обычных объектов (от миллиграммов до сотен тысяч тонн) с обычными скоростями (от долей миллиметра до километров в секунду) вполне хватает классической динамики. А динамики сверхмалых объектов или очень значительных скоростей описываются уже иными законами.

Важные имена: Галилей, Даламбер, Ломоносов, Ляпунов, Мах.

Индукция. От самых простых школьных воспоминаний (производство тока в цепи под действием магнита) до вполне строгих формулировок, определяющих электрическую, магнитную и электромагнитную индукцию, взаимно- и самоиндукцию, а также её иные виды, индукция как понятие имеет не только физический смысл. Происходя как термин от латинского *inductio*, она связана со множеством

процессов, когда одни феномены проявляются/изменяются по причине и за счёт проявлений/изменений других феноменов. Физические виды индукции хороши глубокой теоретической проработкой, охватом и прикладным характером, выгодно отличающим её от понятийных видов индукции в медицине, химии, юриспруденции, биологии, экономике и иных сферах.

Важные имена: Аркадьев, Беллман, Ленц, Пеано, Фарадей.

Инерция. Свойство тела сохранять покой или равномерную линейность движения, если отсутствуют внешние воздействия на него или же их действие скомпенсировано. Одно из основополагающих понятий классической физики, которое часто путают с инертностью. Кажущееся простым понятие, на самом деле намного сложнее, чем оно видится на первый взгляд. Главная проблема в том, что для сил инерции, в отличие от обычных сил взаимодействия, нельзя указать, действие каких конкретно тел на материальную точку ими описывается и/или определяется. Выражением нюансности инерции является тот факт, что принцип эквивалентности тяготения и инерции, обобщающий принцип пропорциональности, стал краеугольным камнем теории тяготения в общей теории относительности. Но консенсус в связи с инерцией в физическом сообществе так до сих пор и не достигнут.

Важные имена: Бальяни, Журавский, Кориолис, Эйлер, Этвеш.

Мощность. Как быстро выполняется работа, передаётся энергия или преобразуется из одного вида в другой. Понятие исключительно универсальное (относится ко всем и любым ситуациям, связанным с энергией), фундаментальное, важное и, применённое для описания процессов обычного мира, крайне информативное и практически полезное.

Большинство ошибок и заблуждений, связываемых с понятием мощности, являются либо следствием невнимательности (как проблема качества силовых сетей), либо к понятию не имеют отношения (как парадокс Браеса – парадокс, приписываемый немецкому математику Дитриху Браесу (статья 1968 года), гласящий, что добавление дополнительных мощностей в сеть при условии, что двигающиеся по сети сущности сами выбирают свой маршрут, может снизить общую производительность).

Важные имена: Ренкин, Румфорд, Уатт, Умов, Якоби.

Состояние. В физической классике речь здесь об агрегатных состояниях вещества «газ», «жидкость» и «твёрдое тело», а также о фазовых переходах между ними. Но не только. Тут же доводится

описывать кристаллические и аморфные состояния, группу родственных и смежных понятий (главные из которых – это, конечно же, температура и давление), рассматривать дихотомию гомогенных и гетерогенных состояний, а также всяческих экзотик типа супержидкости, плазмы или конденсата Бозе. Всё множество процессов вокруг тройной точки (плавление/кристаллизация, испарение/конденсация, возгонка/десублимация) хорошо исследованы, качественно и детально описаны. Разнообразные пены, туманы и прочие дисперсии менее изучены, но тоже имеют приличный описательный объём.

Важные имена: Андреев, Ван-дер-Ваальс, Капица, Лифшиц, Эренфест.

Энтальпия. Не самое запоминающееся со времён средней школы понятие прямо связано с образом энергии во взаимосвязи теплоты и работы. Именно приверженцы энтальпии считают энергию универсальной валютой любых процессов реального мира, объявляют все процессы энергетически значимыми, а теплоту с работой признают способами оборота этой валюты. Это как раз они различают изохорные (при постоянном объёме), изобарные (при постоянном давлении) и изотермические (при постоянной температуре) процессы.

Понятие энтальпии, конечно же, существенно младше понятия энергии; но именно те её особенности, что приведены выше, дают основания полагать, что для наших целей энтальпии будет достаточно, по крайней мере, для начала.

Важные имена: Гесс, Гиббс, Джоуль, Каммерлинг-Оннес, Портер.

Энтропия. Одно из самых загадочных понятий современной физики, декларативно простое, содержательно ёмкое и наиболее важное для нас. Впервые введённое в термодинамике как мера необратимого рассеяния энергии, за 150 лет энтропия эволюционировала через метрику беспорядка и степень неопределённости до оценки вероятностей направлений протекания информационных процессов и установления их необратимости.

Главным отличием энтропии от любых других физических понятий и категорий является то, что она характеризует не описываемую систему, а то, как много нам о системе неизвестно. Энтропия – не свойство системы, а свойство нашего знания о ней. В этом смысле производство энтропии есть процесс отражения суммы процессов осмысления, расширения и упорядочения наших знаний о системах. Как и в случае выше, абсолютных значений у энтропии нет; по отношению к её изменениям принято считать, что во всех природных процессах энтропия лишь возрастает.

Ниже мы попробуем разобраться, так ли это. Для нас также будет очень важно, что ещё энциклопедия Константинова, транслируя воззрения П. Шамбадала, требовала большой осторожности при переносе темы энтропии на биологические, языковые и социальные системы. Хотя и признавала справедливость её применения к системам, подчиняющимся статистическим закономерностям, т.е. – к предмету социологии 2.0.

Важные имена: Больцман, Гамов, Жилин, Каратеодори, Клаузиус.

Чтобы введение было корректным, считаем честным и важным затронуть тему осмысленности самого исследования. Сегодня физика сама по себе находится на некотором рубеже. На каком – зависит от точки зрения: «ещё» полбутылки осталось или «всего» полбутылки. Оптимистов «новой физики» пока меньше пессимистов, но они моложе и энергичнее, а их голоса всё слышнее.

В начале века физики из Брукхейвена обнаружили, что мюоны движутся не так, как им предписано теорией, неконцептуально. Пятнадцать лет исследований привели к тому, что весной 2021-го физики уже из Фермилаба подтвердили это наблюдение в журнале Nature. Возможно, действительно существует ещё неоткрытая пятая сила природы, в дополнение к четырём большим черепахам стандартной модели.

Примерно в то же время в Европе ученые из ЦЕРНа поймали бозон Хиггса, подтвердив Стандартную модель и обнадёжив нас новыми принципами связи и компьютеринга. Но прошло почти десять лет, как они уже опровергли ту же самую Стандартную модель. Им тоже понадобилась пятая сила, без которой нарушается «принцип универсальности ароматов лептонов». На этот раз неконцептуально повели себя W-мезоны. И если у американцев мюоны неправильно двигались, то у европейцев мезоны неправильно распадались (на те же мюоны). Заметим, что публикация тоже пришлась на весну 2021-го, а мезоны «обогнали» мюоны буквально на несколько дней.

Чтобы не показалось, что оптимисты атакуют традиционную физику только из глубин микромира, приведём пару примеров из далей макромира.

В 2010-м г. австралийские астрономы, изучая свет далёких галактик, предположили, что не всё так линейно во Вселенной с физическими законами, т.е. не такие они и законы, поскольку медленно, но меняются. И в декабре 2021-го были опубликованы данные уже чилийских и гавайских исследований, которые по итогам измерений сотен галактик показали: не только на Земле с законами пробле-

мы. Оказалось, что величина «альфы» – постоянная тонкой структуры (ПТС, фундаментальная физическая постоянная, характеризующая силу электромагнитного взаимодействия, введенная в 1916 году немецким физиком Арнольдом Зоммерфельдом в качестве меры релятивистских поправок при описании атомных спектральных линий в рамках модели атома Бора) – больше не равна $1/137$ -й. Кроме того, она не одинакова в космическом пространстве.

При этом ПТС является самой фундаментальной величиной в той реальности, которую мы знаем. Вернее – в той модели реальности, что мы придумали себе для её описания. Постоянная Зоммерфельда – это комбинация трёх сверхзначимых для нашей жизни постоянных. Величина же ПТС ещё до 2020-го считалась стабильной, известной и была измерена с точностью до десятого знака после пятой. Её изменения были зафиксированы в пятом знаке после запятой. Любой ответ на вопрос, что же изменилось в нашей реальности – заряд электрона, постоянная Планка или скорость света – может стать шокирующим.

В начале этого века идея, изложенная в фильме «Матрица», овладела умами, и учёные начали всерьёз исследовать гипотезу о том, что вся наша реальность – лишь имитация и/или компьютерная модель, созданная некой сверхцивилизацией с неизвестной целью.

Американский астрофизик Тайсон в 2016-м оценил на дебатах памяти Айзека Азимова вероятность того, что наша Вселенная является моделируемой кем-то реальностью, как равную 50%. А годом позже американский академик Дэвид Чалмерс заявил, что всё более странные события в реальном мире (социуме) как раз свидетельствуют о том, что он является чьей-то симуляцией. Недостатки же научного знания, что не способны объяснить всё, этот эксперт в области сознания считает проявлением нарастающих проблем в работе программы и соответствующими боями в матрице.

На этом фоне относительно свежее (сентябрь 2021-го) заявление группы физиков-теоретиков и исследователей от Майкрософта о том, что наша Вселенная есть самообучаемая система, выглядит даже, можно сказать, серьёзно. Физические же законы и фундаментальные постоянные они объявляют алгоритмами, которые в форматах операций обучения не просто могут, а должны меняться. Вопросы, кто и для чего её (нашу Вселенную) обучает, американские исследователи пока не задаются.

Патриархом физиков-пессимистов выглядит, конечно же, Д'Аламбер, бравшийся написать такое руководство по физике, что все выводы из него уве-

ренно противоречили бы действительности. Потом следует огромное количество физиков, задававшихся вопросами класса «как примирить концепты классической и квантовой физики». С учётом самой знаменитой цитаты Фейнмана («я смело могу сказать, что квантовой механики никто не понимает»), далее пойдут разработчики, продолжатели и адепты различных физических теорий высшей лиги: тёмная материя, суперструны, квантовая теория поля и тому подобное.

В конечном итоге, лагерь «пессимистов» имеет очень чёткие контуры – это те люди, которые считают, что сегодня в физике есть только три нерешённых проблемы: космологическая постоянная, конфайнмент кварков и квантовая гравитация. Напомним, что речь не о скептиках физики вообще, а о тех, кто без восторга относится к заявлениям о тупике в нашей физике и необходимости, в связи с этим, основать физику «новой».

Возвращаясь к замыслу исследования, для нашей цели одинаково малопримемлемы обе группы: как «оптимисты», так и «пессимисты». Первые – из-за своей непонятности, вторые – из-за избыточной абстрактности. А вот хватает ли того, что называется классической физикой, для структурирования социальной физики – мы и посмотрим. Тут можно не только Эпикура вспомнить, но и того безымянного учёного, который в пору социальной физики 3.0 предложил в эксперименте с Пизанской башни сбросить вместо пушечного ядра обычного голубя.

Как итог: на фоне того, что созидают наши физики, вопрос о рисках лженаучности имеет отрицательный ответ. Может оказаться и так, что в нашу биологию можно верить, а в физику – нет.

ЭНТРОПИЯ

Мы решили начать содержательную часть исследования с самого сложного понятия не из амбиции. Причина весьма проста – без установления социальной энтропии многое из последующего покажется оторванным от практики. Любая энтропия действительно исключительно субъектна и имеет широкий охват.

В 1850г. прусский учёный Рудольф Ю.Э. Клаузиус, исправляя теорию теплорода в двигателях Карно, сформулировал принцип, позднее названный тепловой аксиомой и самой первой формулировкой второго начала термодинамики: «теплота сама собой не может переходить от тела холодного к телу горячему». Для современного человека всё вполне очевидно.

Через несколько лет ирландец Томсон, барон Кельвин, озвучил принцип рассеяния энергии, полное прочтение которого позволяло уже спрогнозировать проблему. Но весной 1865г. Клаузиус вернул себе инициативу, введя первое понятие энтропии. Он закончил свой доклад Парижской Академии наук «Sur les principes fondamentaux de la theorie mecanique de la chaleur» знаменитым выражением «Энергия мира постоянна. Энтропия мира стремится к максимуму». Восприняв две последние фразы Клаузиуса как предсказание тепловой смерти Вселенной, всё тогдашнее научное сообщество сразу же стало искать опровержение прогноза в пользу стерильного серого будущего мира с равномерно рассеянной бесполезной энергией.

Одной из таких попыток стал проведённый через пару лет известным шотландским физиком Максвеллом мысленный эксперимент. В нём абстрактное микроскопическое существо распределяло горячие/холодные молекулы газа по двум половинам ящика, создавая порядок, уменьшая энтропию и опровергая, тем самым, мрачный прогноз. Чуть позже Кельвин, оставаясь сторонником тепловой смерти, назвал это существо «демоном», хотя сам автор существа предпочитал обезличенный термин «клапан».

В конце XIX - начале XX-го века польский физик-теоретик Мариан Смолуховский и американский физик Лео Силард последовательно изучали эту проблему. Как результат, в 1929 году последний опубликовал работу, в которой впервые была вскрыта связь энтропии с информацией. А как итог – чем больше элементы системы подчинены порядку, тем меньше энтропия, что отодвигает нас от умоглядной точки тепловой смерти; чем меньше же в системе порядка, тем больше энтропия, и мы приближаемся к условному «концу всего».

Однако демон Максвелла сражался с ужасом Клаузиуса не в одиночку. Он старался над качеством, но был ещё и вариант количественной борьбы в диалектической связи с качественной. Когда демон был ещё совсем ребёнком, австриец Больцман нашёл свой рецепт и спас веру человечества в светлое будущее, определив в 1877-м году энтропию как логарифм от числа возможных микросостояний системы, приводящего к текущему макросостоянию.

$$S=kx\log(W)$$

Этим Больцман научно обосновал альтернативный взгляд на энтропийную угрозу, попутно придав новые смыслы множеству житейских мудростей, от самой древности в библейском «плодитесь и раз-

множайтесь» (Быт. 1:28) или даосском «если быть как все, то зачем тогда быть» (Хань Сян-цзы) до последовавших позже «больше поэтов, хороших и разных» (Маяковский) и до «обогащайтесь» (Бухарина). Проверим влияние этих изречений на энтропию. Для этого назовём число возможных микросостояний для краткости вариативностью. Начнём исполнять эти призывы по очереди, играя, скажем, в детский конструктор из кубиков.

«Плодитесь и размножайтесь». Было 9 средних кубиков красного цвета; стало 12, тоже средних и тоже красных. Вариативность, как число комбинаций, очевидно выросла.

«Если быть как все...» Было 9 средних кубиков красного цвета; стало 9, но теперь по 3 красных, синих и зелёных. Вариативность снова выросла.

«Больше поэтов...» Исходное состояние то же – 9 средних красных кубиков. Переходим к 9-ти красным, но теперь имеем по 3 кубика, цилиндра и пирамидки. Вариативность, бесспорно, опять выросла, а также выросла сложность.

«Обогащайтесь». 9 средних красных кубиков превращаются в 9 красных кубиков по 3 средних, больших и маленьких. Вариативность и тут выросла.

В действительности мы по жизни играем в эту игру, с разными девизами и с полным охватом участников. При этом растёт наша вариативность, растёт аргумент. Эти естественные процессы развития общества протекают в направлении роста энтропии. Есть и другие естественные процессы, протекающие в обратном направлении: пандемии, войны, дигитализация жизни. Хотя последний процесс (тренд) сложнее: часть его феноменов действительно снижает энтропию, в то время как другая часть – повышает. Мы вернёмся к вопросу об энтропийных эффектах социальных динамик чуть ниже. Пока лишь обратим внимание на гениальность формулы Больцмана: кроме простоты она ещё даёт нам возможность использовать самую простую математику, т.к. энтропия, в отличие от вероятности, аддитивна. Поэтому все комплексные случаи могут обрабатываться простым сложением энтропийных эффектов с учётом их знака.

ЭНТРОПИЯ И НЕГЭНТРОПИЯ

Поскольку мы заговорили о математике, перейдем от качественного оценивания к количественному. Для этого заменим детские кубики на игральные и возьмём их для круглого счёта десять. А перед первым броском вспомним формулу Больцмана о связи энтропии и информации.

Конечно, будет очень важен наш выбор измеряемой базы (энтропия – это то, как много информации нам известно о текущем состоянии системы или как много мы о нём ещё не знаем), но мы вполне можем вернуться к этой развилке позже, уже после рассмотрения большинства существенных наполнений основных физических свойств социальных систем. Пока лишь скажем, что такой выбор базы, безусловно, имеет для наших целей значение, но скорее имплементационное, нежели семантическое.

Итак, бросаем кубики. И сообщаем Интересанту системы, что в сумме выпало 30. Эта информация характеризует макросостояние системы по метрике «общая сумма», но практически никак не поможет ему (Интересанту) описать микросостояния (какие конкретно цифры выпали на каждом кубике), т.к. имеется $W = 2\,930\,455$ комбинаций. Причём очень важно, что в этом случае с кубиками все варианты равнозначно вероятны, чего ни в какой социальной модели быть не может.

Далее, если мы опустим постоянную k и возьмём десятичное основание больцмановского логарифма (а основание логарифма здесь также лишь один из аспектов размерности), то энтропия системы будет равна $S(i) = 6.47$ (дробность связана с тем, что в разряде миллионов доступны лишь цифры 0,1,2). Индекс (i) здесь использован для того, чтобы явно указать на субъектность энтропии, поскольку 6.47 – её величина в данном конкретном исполнении для Интересанта (i у Интересанта), а не для Автора броска. У Автора тоже есть своя энтропия, $S(a)$, но она во всех случаях данного сценария игры всегда будет одинакова и равна нулю: Автор по определению всегда знает исчерпывающий и полный список микросостояний, формирующий не только сумму 30 как конкретную метрику макросостояния системы, но и любую другую общую сумму при любом другом исходе броска.

Теперь раскроем Интересанту немного больше и скажем, что на первых пяти кубиках выпала сумма 17, а на вторых – 13. В самом эксперименте ничего не изменилось, но у Интересанта произошли весьма ощутимые изменения – он стал более информирован, поэтому его энтропия системы должна упасть. Проверяем себя: сумму 17 на 5-ти кубиках могут дать лишь 780 разных комбинаций, а сумму 13 на других 5-ти – только 420. Исходы в данном случае вероятностны, а значит умножаются. Получаем, что сумма 30 при двух слагаемых 17 и 13 имеет значительно меньшую вариативность $W = 327\,600$. Тогда и энтропия будет $S(i) = 5.52$, что почти на целую единицу (или ~15%) меньше.

Для большего понимания замысла Больцмана сделаем транзитивную проверку: если сначала посчитать энтропии подсистем и потом их сложить, $S(i)$ не изменится. А мы на этом втором шаге игрового эксперимента получаем важнейший пример: процедура раскрытия информации, не потребовавшая никаких особых действий ни от Автора, ни от Интересанта, снизила энтропию и отодвинула нас всех, пусть на бесконечную малость, от (не)мифического момента «энтропийной смерти».

Остановимся теперь на нескольких важных тезисах.

Сама система после первого броска никак не изменилась: это те же десять кубиков, выпавших числами $(3, 2, 4, 2, 6, 5, 2, 1, 4, 1)$. А её энтропия имеет разные значения и зависит от Автора и уровня его открытости в отношении Интересанта. Первый вывод отсюда: энтропия не свойство объекта, а характеристика субъекта, и то, что её часто рассматривают при описании систем в ряду других системных физических величин, таких как объём, давление или температура, не только неверно, но и серьёзно запутывает.

Второй вывод: энтропия межпарадигмальна, и если мы имеем первый её ракурс в эксперименте как субъектно-объектный (Автор бросил кубики и прочитал то, что выпало на них), то второй ракурс – полностью субъектно-субъектный (Автор предоставил Интересанту сначала один объём информации, затем другой). Ученые в естественных науках не обладают и не могут обладать монополией на её наполнение смыслами и использование понятия энтропии, но, к сожалению, гуманитарии здесь пока серьёзно отстают.

И третий вывод: энтропия – вполне вычисляемая величина. Как выходить из разных, даже самых сложных ситуаций, мы обсудим позже, по ходу рассмотрения нескольких понятий, в особенности – вероятности.

Последний количественный экзерсис со снижением энтропии дополнительным раскрытием информации Интересанту подводит нас к дискуссии о неэнтропии. Не так трудно найти проявления серьёзных историко-научных дискуссий о термине энтропия в смысле его происхождения (выше мы привели свой взгляд на эту тему). Даже в «высшей лиге» есть ещё целая группа вариантов, от авторства Гиббса в 1873-м году до авторства Шеннона в 1948-м. Не хочется верить, что такие обсуждения есть следствие кризиса жанра; но то, что полезного в них немного – это факт. В целом необходимо признать, что состояние детерминированности энтропии далеко от прозрачного.

В первую очередь, мы не имеем консенсуса даже в отношении её понятийной категории: она субстанциональна (сущность), атрибутивна (свойство) или процедурна (процесс)? Примеры-лидеры различных нотаций от различных школ: мера (как сущность), неопределённость (как свойство), или рассеяние (как процесс). Иногда используются их различные комбинации, что и выглядит странно и создаёт прямые помехи использованию понятия в научной практике.

Как, например, можно количественно определить «функцию неупорядоченности», если тут первое слово касается субстанции, а второе – атрибута? Или «меру диссипации» (субстанция и процесс)? Декомпозировать их для дальнейшего можно, но тогда это не будет определением. А ещё можно сослаться на то, что «понятие энтропии само энтропийно» или привести типовую формулу из нашего недавнего прошлого («три источника и три составные части энтропии»), но это не даст ясности и не поможет с его использованием.

Во вторую очередь, обратимся к смыслам энтропии. Теории «высшей лиги» (концепты и/или конструкции, которые поддержаны последователями, разделяющими определённые дефиниции и применяющими предложенный аппарат, методический или инструментальный) это «именные» энтропии: алфавитно – Больцмана, Клаузиуса, Колмогорова, Пригожина и Шеннона: это самостоятельные, целостные, комплексные теории.

Отдельные попытки переосмысления энтропии дали нам ещё целый ряд денотаций энтропии (от Бриллюэна, от Кириллова, от Яглома), но они так, по сути, в «высшей лиге» и не закрепились. Иные подходы (система Смейла, гипотеза Пинскера, дивергенция Реньи) остались теоретическими концепциями, которые имеют частные либо обобщающие применения, пока другие (как функция Хартли для энтропии Шеннона, определение Синая для энтропии Колмогорова, постоянная Планка для энтропии Больцмана) стали хорошими универсальными инструментами.

Если у нас так запутана энтропия, чего же тогда ожидать от неэнтропии? «А давайте просто определим её как энтропию отрицательной величины... и будет нам счастье». По нашему глубокому убеждению, такой рецепт имеет право на жизнь лишь в ряде множества «странных» цитат, ссылки на авторов которых мы не станем давать из этических соображений: «энтропия одной буквы русского языка равна $\sim 4,35$ бит»; «по энтропии электроэнцефалограммы ищут уже давно разные вещи стадии наркоза, сна, болезни Альцгеймера и Пар-

кинсона, эффективность лечения от эпилепсии ...»; «энтропия указывает предельный уровень сжатия данных архиваторами». Воистину, «великий математик Пуанкаре заметил: понятие энтропии “чудовищно абстрактно”».

Поставленный эксперимент с кубиками даёт ясное понимание понятийной разницы энтропии и негэнтропии: Автор, бросив кубики и раскрыв первый объём информации Интересанту, совершил энтропийное действие; во втором случае, не проводя никаких дополнительных экспериментов и дополнительно раскрыв информацию Интересанту, Автор также совершил действие, но уже негэнтропийное. Эффект второго отчасти компенсировал эффект первого, но сущностно иным образом: источником энтропии стал объективно случившийся феномен, а источником негэнтропии – субъективное осознание и воля Автора (не обязательно, что добрая и честная).

Касательно всего второго рассмотренного нюанса – мы говорим о части открытых вопросов, ответы на которые необходимо будет найти. Мы же пока будем следовать выбору «ан-масс»: энтропия – это свойство, понятие информационное; негэнтропия существует самостоятельно, и она мера. В связи с таким выбором считаем полезным привести здесь цитату-предостережение от Шамбадала: *«будучи справедливой применительно к системам, подчиняющимся статистическим закономерностям, эта мера, однако, требует большой осторожности при переносе на биологические, языковые и социальные системы»*. Весьма простой, вполне удобный, трудно оспариваемый, но, главное, немного бессмысленный совет.

Следуя ему, можно лишь с удовольствием вспомнить известную шутку о том, что «пессимист – это хорошо информированный оптимист», а в альтернативной социально-физической формулировке «пессимист – это оптимист с высокой негэнтропией». Как бы то ни было, но все событийные процессы трансформационной реальности имеют прямое энтропийное покрытие и, в большинстве случаев, ведут к её росту. Процессы же информационного обмена, как явные элементы «транзакционной» реальности (то есть, связанной с переносом информации), связаны только с негэнтропией и должны иметь главное своё предназначение в изменении энтропийных итогов любых динамик и трансформ.

Может ли трансформационное поле иметь негэнтропийные проявления, зависит от угла зрения. Мы считаем, что не может. Вся негэнтропия в контексте социальной физики 5.0 есть следствие транзакций, а не трансформаций. Просто значительное

число явлений трансформационного характера имеют и транзакционную компоненту. Обратное верно гораздо реже и только через социальное посредничество индивидов.

Аспекты энтропийной упругости обществ, их проницаемости и/или реактивности имеют перво-степенное практическое значение. Однако их осмысление невозможно без учёта других физических концептов, включая приведенные во введении. Мы обязательно будем к этому возвращаться ниже.

ЭНТРОПИЯ И ИНФОРМАЦИОННОЕ ОБЩЕСТВО

Современное общество определяют сегодня как энергоинформационное, реже – как «постинформационное». Остановившись на первом термине, временно уберём из дефиниции часть «энерго» (мы вернёмся к нему позднее) и попробуем описать общество в информационном аспекте, кратко и максимально избегая спорности, где это только возможно.

Информация в нашем обществе стала для человека базовым ресурсом: человек XXI-го века не может жить без информации и вне её оборота, а информационная среда явно стала объективным условием сосуществования индивидов в обществе. Информация необходима и важна современному человеку не меньше, чем еда и сон. Изменения в процессе развития возможны, но очевидно, что значение информации будет расти.

Во-первых, информационная эволюция отнюдь не трансцендентна и не является чем-то новым. Вернёмся на полвека назад, в роман Кобо Абэ «Человек-ящик». Уже тогда автор советовал человеку, стремящемуся выйти из общества, включить в список тех вещей, которые нужны для жизни, в первую очередь средство коммуникации: *«Количество вещей нужно свести до минимума, но все равно существуют совершенно необходимые предметы, которые всегда должны быть под рукой и без которых просто невозможно обойтись: транзистор, чашка, термос, карманный фонарь, полотенце, коробка для мелочей»*.

Уже тогда человеку было тревожно без новостей. Причину этого Кобо Абэ видел в том, что даже пассивное участие в новостях «на приём» подтверждало человеку его участие в событиях и успокаивало. Этот новый аспект бытия, когда у реального вовлечения в повседневность, вместо участия в событийных потоках трансформаций, появляется конкуренция и даже суррогат в виде факта погружения в

многообразии информационных потоков.

Во-вторых, информация не есть знание. Она принципиально фрагментарна и всегда избыточна, транслируется оперативно и воспринимается квантами, а самое главное – легко существует в отрыве от контекста. Информационные потоки глубоко интегрированы в наши современные системы знаний. При этом изменилась сама суть когнитивности информационного общества: теперь важно не знать «что-то», а знать, где можно найти знание об этом.

Но если всё же искать сродство двух понятий, то информация есть стерилизованное знание. Вхождение информации в нашу жизнь окрашивает её, не приводя к формированию убеждений. Стерильность информации постоянно создаёт диссонансы, в которых носители знаний страдают из-за потребности закрывать разрывы с личным опытом, а аборигены информации легко изолируют одно от другого. Поскольку первых всё меньше, а вторые становятся всё сильнее, на горизонте смены одного поколения мы получим состояние, когда информация станет чем-то вроде физического фактора или даже аргумента функции. Тогда мы поймём – победила транзакция трансформу или будет найден их новый баланс (возможно, даже новая гармония).

В-третьих, основные негативы информационной эпохи сегодня создаются средствами массовой информации и массовых коммуникаций. И как раз их негэнтропийный фундамент требует «логики сенсаций» (Луман), ориентируя на развитие социальных институтов «высокого вида бытия» (Шмит) в рамках идеологии «технофундаментализма» (Вирильо) с доминированием «телетехнологий» (Деррида) и «электронных шейников» (Делез), порождая, в конце концов, «телекратию» (Стросс).

В-четвёртых, дигитализированный мир, очевидно, будет миром симулянтным. Мы вернемся к этому, когда будем подробно рассматривать явления индукции; здесь же лишь отметим, что, в real-time-мире мы должны заранее понимать правила, по которым будут «расходиться круги». Они, очевидно, будут другими, нежели в доинформационном мире: эфирность и иллюзорность информационного основания нового мира не позволит нам применять веками наработанные практики из группы «попробуем – узнаем».

Уже сейчас информация симулирует знания и не важно, что она нам несёт и насколько она истинна. Сегодня важен модус актуальности в его самой жёсткой редакции. Для содержательного социологического анализа, даже в варианте социальной физики 4.0, просто не остаётся окна возможностей. Нет времени и на постановочные эксперименты –

другие акторы, пусть сонастроенные, не позволят и уже не позволяют ждать. В этом свете даже самый слабый и начальный теоретический аппарат прогнозирования лучше никакого, как и в классике любого управления – даже плохое решение лучше его отсутствия.

ОПИСАНИЕ РАБОЧЕЙ ГИПОТЕЗЫ

Таким образом, наблюдаемая нами картина мира характеризуется ярко выраженным многообразием и постоянно возрастающей перцептивной сложностью. И теперь мысленные эксперименты с энтропией в её социально-физическом понимании и основанные на них рассуждения подводят нас к рабочей гипотезе в стиле прочтения Гиббса: **«все фактические события, явления и процессы в социальной реальности, при условии не уменьшения её количественной базы, самопроизвольно протекают лишь с ростом суммарной примитивной энтропии».**

Прежде чем перейти к следствиям из гипотезы, дадим определения её терминов.

Говоря «фактические», мы имеем в виду как спланированные, так и стохастические (но не хаотически-случайные) изменения как субъектных, так и объектных состояний в рамках трансформаций. Например, добыча бочки нефти, но не публикация сводки о её запасах, или просмотр кино, но не прочтение заметки кинокритика.

Если мы сейчас раскроем читателю факт, что он читает главы из книги «Социальная физика 5.0», изменение его энтропии будет нулевым по любому механизму, энтропийному или негэнтропийному. Если мы скажем читателю, что в то же самое время эту же книгу читает ещё 5 человек, энтропия подрастёт, несмотря на полную бесполезность этой информации. Ну а если мы сообщим, что эта книга выдвинута на Пулитцеровскую премию, энтропия вырастет очень резко, даже если это ложная информация. Мера информации об очевидном может быть равна нулю, о невероятном – стремиться к бесконечности (массовое срабатывание приязни к сенсациям и веры в чудеса).

Говоря о «социальной реальности», мы имеем в виду событийный поток объективного характера, способный быть наблюдаемым/осознаваемым более чем одним актором. Под «не уменьшением количественной базы» понимаем исключение из гипотезы тех случаев, которые связаны, например, со смертью человека (а в целом – с завершением деятельности субъектов).

Мы будем использовать менее строгий и более ёмкий термин самопроизвольности. В общем же случае речь именно о самопроизвольном протекании событий, явлений и процессов, то есть тех, которые без энтропийного катализа происходить не будут, хотя теоретически они возможны.

«Примитивной» мы называем первичную энтропию субъекта, формируемую у него феноменом. Её прямое исчисление совершенно умозрительно, поскольку сразу после проявления немедленно начинается множество внутренних процессов переработки (с запасанием, усвоением, рассеянием и трансляцией) её в «зрелую» энтропию, которые являются проявлением её субъектности и отражением характеристик вовлечённого в энтропийную динамику субъекта.

При одинаковом изменении примитивной энтропии любой феномен даёт нам различный зрелый энтропийный эффект на разных участниках. Причём здесь любой субъект, «осваивая» примитивную энтропию с «переработкой» её в зрелую, выступает в роли своеобразного юнита (звена, элемента) энтропийной реакторной батареи. Самостоятельные же, и вполне описываемые/рассчитываемые характеристики «переработчика» в данном конструкте будут иметь как сами юниты, так и вся батарея в целом. В первом случае это будут атомизированные параметры конкретных субъектов-юнитов, а во втором – параметры их прямо затронутых комбинаций: групп, страт, социумов, сообществ и иных объединений, в которых данный феномен случился и/или к которым относится.

В логике нашего исходного примера с броском десятка кубиков процессинг энтропии выглядел бы как сеанс игры в крэпс или перудо в казино. И если изначально в эксперименте у нас было только два субъекта (Автор и Интересант) то теперь их, допустим, будет 8 – Автор и 7 Интересантов. Очевидно, что примитивная энтропия первого броска одинакова, по типу «всем нам нравится Джоконда». Но великий Леонардо был уникален и повторение тут невозможно (ещё один энтропийный аспект!).

При этом в нашей жизни всегда есть место флуктуациям: один Интересант не услышал объявления Автора, второй не понял, третий перепутал и т.д. Получается, что в то время как примитивная энтропия одинакова, зрелая энтропия в данном эксперименте будет различной для всех семи Интересантов. Вычислить её – непростая, но вполне решаемая задача.

Очень интересный аспект эксперимента – обратная связь и запечатление (или фиксация образа). У нас нет возможности уделить ему тут столько вни-

мания, сколько он заслуживает, поскольку теоретическая основа этого «обработчика» ещё находится в начальной стадии. Но можно уверенно предполагать, что два общеизвестных из четырёх фундаментальных принципов информационного общества («неважно, что Вы говорите; важно как Вас слышат» и «неважно, что на картинке; важно, что на подписи к ней») имеют вполне ясную энтропийную природу. Здесь же только отметим, что при естественной множественности и органической мультиреактивности юнитов переработки энтропии из одной формы в другую разными будут не только значения зрелой формы, но и сам феномен.

ОСНОВНЫЕ СЛЕДСТВИЯ ЭНТРОПИЙНОЙ ГИПОТЕЗЫ

Рассуждать и дальше о человеке, как об энтропийном реакторе и субъектном юните энтропийных батарей, без осознания социальных наполнений для категорий вязкости, динамики, дуализма, индукции, инерции и мощности было бы неуместно и даже неосмотрительно. Поэтому вернёмся пока к энтропийной гипотезе.

В изложенной формулировке она приводит нас как минимум к трём важнейшим следствиям. Мы ожидаем, что они будут открываться по мере расширения рамок охвата социальной физикой и развития её понятийного аппарата за счет вовлечения в инструментарий новых разделов физики. Например, уже сейчас существуют все необходимые заделы для разработки теории энтропийного катализа.

Но на данный момент, на этапе оценки целесообразности, уверенных следствий три.

Первое следствие – удельное исчисление зрелой энтропии. В отличие от большинства моделей субъектно-объектного характера, любые субъектно-субъектные функции нельзя свести к простому виду; они всегда мультиаргументны. Если мы подогреем чашку с шариками, после установления нового равновесия каждый шарик решётки поглотит, на уровне ошибки измерения, одинаковое количество теплоты, и все они будут иметь равную температуру.

В модели социальной системы это отнюдь не так – каждый шарик в ней неодинаков, имеет разные размеры, сделан из разных материалов; да и не все они шарики. Кроме этого, каждый элементарный объект в этой чашке может иметь какую-то термоизоляцию и/или термоаккумуляторы. Могут в социальной чашке встречаться объекты, сделанные из пирогенов, объекты сложной дисперсной структуры, объекты с встроенными источниками тепла.

Расположены шарики-объекты в чашке тоже не в гравитационной оптимальности. Наконец, каждый «шарик» в этой «социальной» чашке имеет собственную волю и свои механизмы реакции на нагревание.

Очевидно, что в такой ситуации, измерение количества подведённого к чашке тепла охарактеризует лишь усилия исследователя (вычисление примитивной энтропии), но спрогнозировать объектную температуру (оценка зрелой энтропии) прямо не даст. Такой индивидуализм объектов делает необходимой именно удельную метрику любых калькуляций зрелой энтропии, которая может быть полезной и в расчётах примитивной энтропии (как характеристика охвата феноменом).

Второе следствие энтропийной гипотезы – снижение зрелой энтропии при протекании любых из «разрешённых» феноменов. Определяя термины, выше мы уже предложили четыре разных неантогонистически-конкурентных механизма, по которым происходит процессинг подводимой к субъекту примитивной энтропии в зрелую. Все они – не особенности источника примитивной энтропии, а уже субъектные характеристики человека как энтропийного реактора. Практика их прямого исполнения в стабильном социуме даёт совокупную механику удержания (даже снижения) уровня той удельной зрелой энтропии, которая и является главным аспектом наблюдения и основным предметом управления в рамках социальной физики 5.0.

Первые два из них (запасание и усвоение) имеют прямое отношение к формированию параметров реактивности человека как атомарного социального субъекта. Будучи реактором энтропии, человек перерабатывает получаемую им из социальной среды энтропию по своим индивидуальным правилам. И если часть энтропии запасается им в пределах его потенциала, то другая часть усваивается в виде каких-либо понятий или норм, социальных или деловых обычаев, общественных или индивидуальных практик (см. выше: первый фундаментальный принцип информационного общества).

Именно так, в рамках энтропийной гипотезы, проявляется аутопознность энтропийных взаимодействий, под влиянием которой в ходе процессинга примитивной энтропии в зрелую появляются социальные скрепы и формируется общество.

Напомним, что аутопозис – термин, введённый в начале 1970-х годов чилийскими учёными У. Матураной и Ф. Варелой, означающий самопостроение, самовоспроизводство, репликацию живых существ, в том числе человека, которые отличаются тем, что их организация порождает в качестве продукта их

самих без разделения на производителя и продукт.

Разные люди обладают разными потенциалами, и формируемые ими в течение жизни параметры их реактивности – тоже разные. Социальное нормирование в любом обществе всегда построено на процессе «принятия-осознания-приятия», который начинается с первого крика ребёнка. Осознание им любой новой возможности обычно сопровождается в обществе внесением в список правил какой-то нормы. Такое регулирование сводится, по сути, к ограничению возможностей рамками допустимого. Социальная физика видит в осознании возможности повышение зрелой энтропии субъекта (запасание), а социальное нормирование она определяет как усвоение зрелой энтропии (снижение поведенческой вариативности и балансирующую компенсацию роста её запаса).

Можно продолжить цепочку рассуждения и показать, скажем, что любое воспитание есть сугубо неэнтропийная сфера, а разделяемые ценности – фильтры, применимые во всех четырёх механизмах переработки примитивной энтропии. Видимо, есть смысл затронуть и тему чувствительности/связанности «созревания» энтропии с аспектами культуры, здоровьем, сезонностью, имущественными рамками. Но поскольку изучение вопросов прикладного применения социальной физики 5.0 не являются прямой целью данной работы, мы вынуждены здесь себя ограничить и приведем ниже только некоторые примеры применения.

Третье следствие – существование энтропийного поля. Третий механизм (рассеяние) и четвёртый (трансляция) – это не только техники процессинга примитивной энтропии в зрелую, но и признаки реальности энтропийного поля, способы и каналы его формирования и отражение его параметров. Дело в том, что энтропия, как это и было определено выше, не свойство объекта, а характеристика субъекта. И мы применяли термин «объект» при рассмотрении первого следствия энтропийной гипотезы лишь для сохранения модельной целостности сравнения физической и социальной чашек. Но связь субъектной энтропии и энтропии субъектного окружения требует внимательного изучения.

«Очевидным» субъектом неатомарного ранга является молекулярный субъект или семья. Все остальные ранги явно будут следствием выбора исследователя, попавшего в болото колоссального антагонизма множества иерархий и классификаций. Но мы даже для молекулярного ранга вынуждены поставить под сомнение очевидность, поскольку под семьёй понимается очень разное, например, в традиционных обществах и социумах родоплеменного уклада.

Ранги неатомарных уровней хорошо определяются по возрасту, статусу, материальному положению. Объединительными признаками «особых» социальных чашек могут быть обучение в одном учебном заведении, местничество, принадлежность к фанатским группам или общественным движениям, проявления отношений к религиозным, национальным концептам, политические предпочтения субъектов. Иногда речь идет о связанности в смысле неформальных цеховых и гильдейских контактов, деловом нетворкинге, профессиональной кластеризации и тому подобном.

Перечисление принципов организации этих надатомарных агрегатов, интересных с позиции социальной физики, считаем на данном этапе преждевременным, поскольку энтропийный подход сам по себе достаточно гибок для того, чтобы качественно оценивать субъекты при помощи квалитметрии. Понятно, что каждый модельный «шарик» может принадлежать одновременно разным «чашкам». Следовательно, «чашка» как отражение энтропийной среды и самостоятельный субъект энтропийного поля, становится n-мерным объектом социальной физики 5.0.

Кроме того, пересечение надатомарных энтропийных агрегатов может создавать неатомарные ранговые сущности второго порядка типа «депутат-спортсмен». Они не столь доминантны, но в отдельных случаях тоже могут иметь своё энтропийное поле и представлять, как следствие, интерес для социальной физики.

Завершая рассмотрение третьего следствия энтропийной гипотезы, мы обратили бы внимание на возможные интересные проявления при организации всех энтропийных агрегатов первого порядка, и некоторых – второго. Также специальный интерес для социального конструирования в частности и социальной инженерии в целом могут представлять схемы агрегации энтропийных субъектов (их энтропийные поля, как правило, весьма сильны и субъектны). Силовики и идеологи хорошо знакомы с этим, а эмерджентность зрелой энтропии проявляется в них наиболее выражено.

Таким образом, три следствия энтропийной гипотезы в сумме распространили её вверх и отчасти в сторону. Мы не уверены, что это приведёт нас к теме декомпозирования основного базового атомарного объекта (субъекта!) в социальной физике – человека – вниз (вглубь). Но полностью исключать такое направление развития мы не станем. И если социальная физика 5.0 получит развитие, а уровень её зрелости дойдёт до описания внутреннего мира человека, то «простой» логики адронов и лептонов

нам, вероятно, не хватит.

В таком случае можно будет ввести в зону нашего внимания и рассмотрения всех известных нам переносчиков взаимодействия (фотоны, бозоны, глюоны, не пойманные пока гравитоны и гипотетические хрононы) и соответствующие им физические неведущие теории и концепции. Соответственно, мы получим самостоятельную теоретическую базу для глубокого понимания субъектности энтропийных полей не только вовне, но и внутри человека. Пока это совершенно фантазийный предикт; но, возможно, именно его нам и не хватило в своё время для того, чтобы принять и начать широко применять по жизни ноосферное учение Вернадского.

Однако это пока ещё можно сделать, хотя и гораздо труднее, чем 100 лет назад.

ОБЩЕСТВЕННО ЗНАЧИМЫЕ СОБЫТИЯ И ЭНТРОПИЯ

Прежде чем завершить раздел, посвященный энтропии, поставим ещё два мысленных эксперимента, рассмотрев реальные события – это Стэнфордский эксперимент 1971г. и французские «жёлтые жилеты» 2018г. Первый поможет нам шире взглянуть на субъектные особенности человека в роли реактора первичной переработки примитивной энтропии в зрелую, а второй – даст больше понимания о природе и особенностях энтропийного поля в его современной наполненности.

Стэнфордский эксперимент даёт нам конкретный пример проявления как самой энтропийной гипотезы, так и всех её трёх следствий: удельного, аутопозного и эмерджентного. Напомним кратко его суть: американский психолог Филип Джордж Зимбардо по заказу ВМФ США провёл в подвале здания кафедры психологии Стэнфорского университета эксперимент с участием 24-х добровольцев. Все они были случайным образом отобраны из тех студентов, которые откликнулись на объявление в газете, и разделены на «заключённых» и «охранников» с целью «симулировать тюрьму» на протяжении 14-ти дней.

Местная полиция, помогавшая Зимбардо в начальной стадии эксперимента, без предупреждения обвинила «заключённых» в вооружённом ограблении и арестовала. Их отвезли в «тюрьму», осмотрели, присвоили номера, одели в миткаль без белья и развели по камерам, где начался эксперимент. «Охранники» должны были создавать в заключённых чувство страха, бессилия и произвола,

всеми способами отнимать их индивидуальность. Эксперимент быстро вышел из-под контроля и был прекращён уже через 6 дней. У «заклочённых» дошло до спутанного сознания и психосоматики, а у «охранников» стало доминировать оскорбительное поведение и расцвёл садизм.

О Стэнфордском эксперименте так много сказано, написано и даже снято, что любой желающий может познакомиться с его содержанием.

Самую большую конгруэнтность с нашими задачами имеет использование итогов Стэнфордского эксперимента для иллюстрации теории когнитивного диссонанса (ТКД), предложенной за 15 лет до того американцем Фестингером.

Внутренне эта весьма стройная теория не даёт нам ответа лишь на один вопрос – какова природа того чувства дискомфорта, которое возникает при столкновении в сознании логических противоречий когний (информации, опыта, мыслей) об одном и том же феномене (объекте, событии, процессе). Если же мы применим к ТКД энтропийную гипотезу, ответ на этот вопрос может быть найден: конфликт когний выводит их из списка вариативных мотивов побуждения/поведения человека. Но это уменьшает примитивную энтропию, чего не допускает гипотеза.

Далее механизм весьма несложен: как правило, когнитивный диссонанс приводит к закреплению обеих когний как уместных; вариативность восстанавливается и энтропия растёт. Человек формирует у себя во внутреннем понятийном аппарате новые, комбинаторные когнии, позволяющие новый поведенческий профиль. Как итог – разрешённый гипотезой рост примитивной энтропии приводит к её процессингу во внутреннем энтропийном реакторе человека в зрелую. Удельный уровень энтропии человека снижен, диссонанс разрешён (сформирован консонанс).

Варианты новых когний (согласования убеждений) у всех индивидов различны: все курящие знают о вреде своей привычки, но кто-то продолжает курить, потому что его удовольствие от курения слишком велико, кто-то не верит, что риск для его здоровья фатален, а кто-то все-таки отказывается от привычки.

Все эти варианты возникают как результаты энтропийного процессинга во внутренних энтропийных реакторах субъектов и в энтропийном же поле аккомодирующего социума, говоря строже – в энтропийных полях социумов причастности. Новые когнии, по сути «примиряющие» какие-то условно «старые» (например, для курящего – «курить вредно») с условно «новыми» («большой вес опа-

сен»), как замещающий продукт процессинга, возникают у нас не всегда и только как результат силлогистики.

ДОПОЛНИТЕЛЬНЫЙ ЭКСКУРС В ИСТОРИЮ

Ученик Платона Аристотель в «Аналитиках» изложил теорию логики, приведя её законы, в том числе силлогизмы. Эта логика, как и все физические представления Аристотеля, считались абсолютom почти две тысячи лет, и основой всего научного мышления вплоть до XX века. Считается, что мы и сегодня живём вполне логично. Однако это мнение совсем не верно.

В 1903-м году британец Рассел обнаружил противоречие существовавшего тогда вида теории множеств. Это тот самый парадокс про брадобрея: «он бреет всякого, кто сам не бреется; и не бреет того, кто бреется сам; кто бреет брадобрея?» Строгая научная формулировка, конечно, сложнее, но важно то, что парадокс Рассела привёл к тяжёлому кризису математики, её расколу и резкому ускорению развития в трёх направлениях: интуиционизм, логицизм и формализм.

Интуиционисты с голландцем Брауэром начали критику классической математики за её опору на парадоксальную теорию множеств. Их новая математика рассматривала мир мысленных процессов как последовательность элементарных шагов. Они исключили понятие бесконечности из науки. Как шутил Врублевский: «если тебе трудно сразу понять всю бесконечность, постарайся понять ее хотя бы наполовину».

Логицисты под водительством Фреге и Рассела открыли, что парадоксы типа расселовского связаны не столько с их математическим содержанием, сколько со свойствами языка. Итогом стало утверждение о сводимости математики к логике и знаменитый трёхтомник «Principia Mathematica». Цитируя Штейнхауса: «из дома реальности легко забрести в лес математики, но лишь немногие способны вернуться обратно».

Известных ученых собрал вокруг себя формалист Гильберт: Вейль, Ласкер, Бернайс, Аккерман, фон Нейман. Джон фон Нейман внёс наибольший персональный вклад в создание текущей реальности III-го тысячелетия. С ним связаны важнейшие события и прорывные теории XX-го века, которые составили фундамент современного информационного мира (Манхэттенский проект, архитектура большинства современных компьютеров, теория операторов в квантовой механике, атомная энерге-

тика, баллистические ракеты, теория игр, прогнозы погоды, концепция клеточных автоматов).

Вернёмся к идеям Гильберта. Он провозгласил своей целью возвращение математике её строгости и начал разрабатывать математический аппарат формализма. В 1934-м и 1939-м годах вышли два знаменитых тома «Оснований математики» Гильберта и Бернаиса, в которых были представлены аксиоматическая теория доказательств и основы современной математической логики.

Однако предшествовала им более ранняя публикация 1928 года «Основ теоретической логики» в соавторстве с Аккерманом, где Гильберт кардинальным образом пересмотрел идеи Аристотеля: «...ставшее традиционным со времён Аристотеля истолкование положительных всеобщих предложений ... не вполне согласуется с нашей интерпретацией формул...», «Наше отклонение от Аристотеля в этом пункте оправдывается потребностями математических применений логики, где класть в основу аристотелево понимание было бы нецелесообразно».

Приведем фото из первого русского издания 1947-го года.

мого вида. Все они принадлежат к аристотелевым умозаклучениям, так что классический перечень форм умозаклучений исчерпывает все возможные случаи. Однако нашим методом мы не воспроизводим всех аристотелевых способов умозаклучения. В полученном перечне отсутствуют четыре вида умозаклучений: *dárapti*, *batálip*, *felápton*, *fesápo*. Это расхождение происходит от того, что ставшее традиционным со времён Аристотеля истолкование положительных всеобщих предложений («Все *A* суть *B*») не вполне согласуется с нашей интерпретацией формул вида $|\bar{X}\vee Y|$. Именно, по Аристотелю, высказывание «Все *A* суть *B*» считается истинным лишь, если существуют предметы, которые суть *A*. Наше отклонение от Аристотеля в этом пункте оправдывается потребностями математических применений логики, где класть в основу аристотелево понимание было бы нецелесообразно.

Мы ограничиваемся этими замечаниями в отношении исчисления предикатов и классов. Правда, можно указать ряд интересных постановок вопросов; например, можно спросить, какие формулы комбинированного исчисления представляют собой всегда-истинные высказывания. От более детального рассмотрения этих

Отвергнутое в «Основах теоретической логики» положение Аристотеля «Все *A* суть *B*» трёхзначно, а у Гильберта и с того момента – двухзначно. Именно тогда математика и физика оторвались от реальности, а две фразы, приведенные выше, «исторгли» из нашей жизни её дух, заменив цветную формулу «да»/«нет»/«незнаю» на чёрно-белую «да»/«нет». Однако наша жизнь тринарна, а не бинарна, а человек имеет право и на неопределённость, и на ошибку.

Наилучшим образом эти идеи прокомментиро-

вал известный математик позднего СССР Арнольд, автор знаменитой задачи «О мятом рубле»: «Гильберту принадлежит формальная точка зрения на математику как на дедуктивный вывод логических следствий из заданных аксиом. Эта точка зрения безусловно справедлива, но лишь в той мере, в какой поэзия сводится к последовательностям букв определенных алфавитов».

ЭНТРОПИЯ И ЛОГИКА

Удивительно то, что ещё в середине прошлого века, воспитывая созидателей, а не потребителей, полноценная логика преподавалась даже в средней школе: в культовой «Логике» Виноградова и Кузьмина силлогизм вводился уже в самом начале, в первой главе (как второй пример).

Мы считаем вопросы силлогизмов крайне важными в применении к энтропии. Жизнь человека не включает в себе лишь выбор между «да» и «нет». Бинарная логика ошибочна, а когниции человека обязаны поддерживать вариативность его жизни. Но если в когнитивном процессе не формируются новые когниции, замещающие старые, то вся вариативность любых выборов в жизни будет обеспечиваться по энтропийному механизму.

Проблема не в неопределённости и даже не в том, возникают ли в ней по мере роста зрелости упорядочивающие её структуры. Нам видится в определенной степени «токсичным» то состояние системы, в которой новые структуры не заменяют собой старые, а лишь дополняют их. И гильбертова бинарность, как база бивалентной логики, проявляется отнюдь не как безобидная оплошность; именно она есть залог того логического фатализма, который часто приводит нас к когнитивному дисбалансу. Поэтому проблемой является растущая неопределённость когниций.

Новые когниции, не имеющие своего «законного» места для вызревания и соотнесения со старыми (с последующим отмиранием слабых когниций), создают существенное усложнение структуры, требуя новых связей со старыми элементами и заполняя наш когнитивный космос осколками неслучившегося порядка и регуляторами регуляторов протекания когнитивных процессов. Такова цена исключения «не знаю» из акцептного поля когнитивной логики, и процессы негэнтропии беспомощны в сражении с этой энтропийной бурей, имеющей место в каждом субъекте информационного общества. Как следствие, аналитические процессы делегируются другим субъектам, например, СМИ.

Однако именно когниции человека и определяют его социальность в широком смысле.

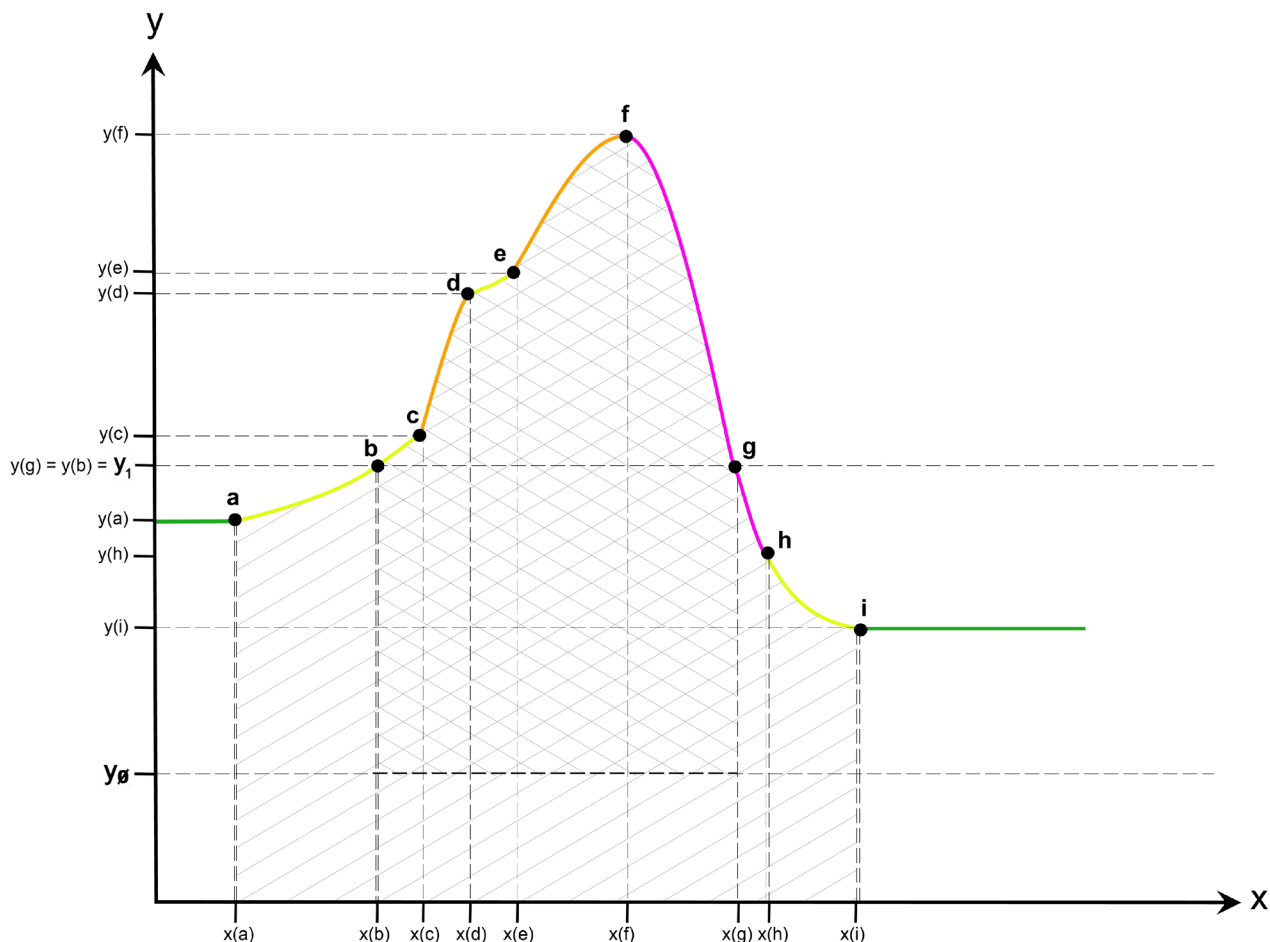
Искусственная корректировка рабочей логики в середине прошлого века имела все признаки энтропийного взрыва. Причём, с учётом эффекта базы, он был сопоставим по масштабу с прошлым глобальным энтропийным качественным сдвигом в истории – изобретением книгопечатания, а возникший в 1950-х Homo Depravatus (от лат. «человек испорченный») стал потомком средневекового Homo Legens (от Китая IX-го века до Европы XV-го). Можно спорить, стал ли последовавший через полвека интернет-феномен следствием появления бинарной логики и прямым проявлением её социализации (и тогда Homo Depravatus – лишь первоначальная форма Homo Digitalis) или нет (а H.Depravatus – это полноценный предок современного H.Digitalis), но когнитивность «человека испорченного» точно отличается от нормальной, хотя очень близка по механизму к «человеку цифровому».

Такой человек проявляет комплекс особенностей осознания/познания, технических и когнитивных, что и средне-типичный переученный левша. Вот только доля всех таких «переученных» состав-

ляет не 10-15%, а 95%. Матрицы суждений и фильтров приятя у современного человека бесконечно усложнены огромным числом искусственных условий. Каждый, кто имеет одновременный опыт программирования на ассемблере и на любом языке верхнего уровня, с лёгкостью подтвердит, что число разилок при конструировании кода по алгоритмам «если – то» в десятки раз больше (а структура – в десятки раз сложнее), чем при алгоритмах «если-то-иначе». Под определённым углом зрения, вполне можно сказать, что само развитие верхне-уровневых языков есть наша коррекция нашей же ошибки – бинаризации логики. Если бы мы сохранили аристотелеву логику и не поддались гильбертовой, возможно, и наш компьютеринг, и весь современный мир были бы другими.

КРИВАЯ ЭНТРОПИЙНОГО ПРОЦЕССИНГА

Опишем условную модельную кривую энтропийного процессинга примитивной энтропии в зрелую и определим её реперные точки.



Вертикальная ось графика (функция вида $y = f(x)$) – уровень удельной энтропии, горизонтальная – поток (последовательность) состояний. Конкретные метрики переменных и значений аргументов пока нам не важны. Позже мы будем использовать событийные метрики и размерности времени для потока x .

На вертикальной оси начать следует с двух точек y_0 и y_1 (характеристик субъекта атомарного или над- атомарного). Смысл нулевого репера – линия энтропийного вырождения, ниже которой ($f(x) < y_0$) система входит в стагнацию и по сути перестаёт быть энтропийным субъектом. Смысл репера единичного – уровень энтропийного возбуждения, выше которого ($f(x) > y_1$) система выходит из баланса и возникает движущая сила процессинга примитивной энтропии.

Как уже говорилось выше, нулевая и единичная точки индивидуальны для любого субъекта, а его нормальностью является удержание энтропии внутри этих границ. Тогда можно считать событийный поток субъекта ламинарным, а его функционирование «штатным» (ординарным). Сами эти реперные точки, как границы интервала, имеют некий потенциал динамики жизненного цикла и могут смещаться вниз и вверх. Мы не имеем возможности уделить здесь достойное внимание крайне важному и сложному механизму таких изменений; скажем лишь, что он основан на сумме природных потенциалов личности и социальных условий её формирования и имеет модально-медианный конструкт.

Если институционализация социальной физики 5.0 произойдёт, разработка теоретических основ энтропийного интервала с выходом на его шкальные уравнения станет одной из важнейших задач научно-обоснованного энтропийного тренинга.

Девять фактических точек по вертикали, как и их образы на горизонтальной оси, отражают модельное состояние системы в следующей логике развития ситуации: до точки a вся система равновесна; в момент $x(a)$ рецепция субъекта фиксирует некую энтропийную новацию (скажем, «удовольствие от курения»), которая первично возбуждает систему подводом примитивной энтропии до уровня $y(c)$. При этом в точке b превышает уровень энтропийного возбуждения и в системе включается режим энтропийного процессинга.

На интервале $[c \rightarrow d]$ система проходит стартовый, чаще интуитивный, процессинг доступных и относящихся когний с фиксацией новых типов/диапазонов вариативности от принятой новации. Далее, на $[d \rightarrow e]$, наблюдается процесс первичной

рефлексии простого множества когний с попыткой оценки приемлемости нового энтропийного уровня; после чего система переходит к созидательному процессингу.

Интервалу $[e \rightarrow f]$ соответствует базовый этап сущностной переработки примитивной энтропии в зрелую, с наработкой тех энтропийных потоков, которые потом, на этапе основной рефлексии $[f \rightarrow h]$, будут как раз прямо усвоены внутри системы, рассеяны с потерей энтропийности и оттранслированы во внешнее энтропийное поле причастных социумов.

В точке g система возвращается в энтропийный интервал, движущая сила процессинга выключается, усвоение прекращается, а этапы перехода $[g \rightarrow i]$ происходят как бы в режиме «докатки». Упорядоченное запасание новой когнии, с установлением иерархии (содержательной взаимосвязи) её со старыми, заменяет собой ранее активное усвоение на интервале $[g \rightarrow h]$, а уже после завершения рассеяния и трансляции, что происходит в точке h , составляет существо последнего этапа процессинга $[h \rightarrow i]$. После достижения точки i система переходит в новое состояние равновесия, завершая переработку примитивной энтропии в зрелую.

Зелёные отрезки на графике описывают условно стабильное состояние системы; жёлтые – те участки энтропийных количественных динамик, где работают преимущественно трансформационные механизмы; рыжие акцентируют динамики неэнтропийные, качественные, транзакционные; наконец, розовый отрезок – комплексный и близкий к классическому понятию катарсиса.

В описательном порядке дадим «горячую десятку» важных логем (по Чеснокову):

1. Приведенным графиком показан «спокойный» вариант протекания энтропийного процессинга как проявления логики диссонансии/консонансии. Понятно, что на любом этапе могут проявляться какие-то дополнительные и/или относящиеся внешние возбуждения и/или разгрузки. Отметим, что любые внутренние открытия и/или переосмысления не должны приводить к изменениям видимой геометрии кривой.

2. Результатом процессинга, определяющим как его эффект, так и движущую силу на всей кривой, является не $\Delta y_{a \rightarrow i}$, хотя в большинстве реальных случаев $y(a) - y(i)$ действительно больше нуля; в ходе энтропийного процессинга важно, чтобы исполнялось интервальное неравенство $y_0 < y(i) < y_1$. Итоговой метрикой всего процесса следует считать $\Delta y_{0 \rightarrow i}$ как $(y_i - y_0)$ и значение $y(i)$.

3. Высота $y(f)$ как раз и определяет энтропийный лимит процессинга, делая его обязательным, вероятным, возможным, сложным или не происходящим вовсе при определённых обстоятельствах, в зависимости от субъектных особенностей и от энтропийной сопоставимости диссоциирующих когний. Общее правило здесь весьма простое: пик энтропийного процессинга тем выше, чем ниже сродство тех когний, которые проявляют атональность друг к другу. Именно по этой причине в энтропийном процессинге хорошо работает негэнтропийный катализ: он увеличивает количество пиков, снижая высоту каждого из них и растягивая саму переработку по горизонтальной шкале.

4. Участок $[d \rightarrow e]$ не обязан повышать энтропийный уровень; иногда бывает так, что $y(e) < y(d)$. И именно с e чаще всего начинают действовать механизмы катализа, опуская катализированный $y(e')$ ниже регулярного $y(e)$ и смещая $x(e)$ вправо.

5. В поэтическом образе выше важно, чтобы при превращении сохранялась «масса верблюда». Иными словами, при катализе или при ином регулярном протекании процессинга, без дополнительных внешних возбуждений площадь под кривой не должна (интеграл функции), в общем случае, изменяться; больше как *idem*, нежели как *const*. Таких «постоянных областей» в когнитивно-энтропийном процессинге две, и первая из них ограничена кривой $x(a)..a..b..c..d..e..f..g..h..i..x(i)$. Эта площадь под кривой является отражением когнитивных особенностей и потенциалов субъекта.

6. Вторая *idem*, площадь под кривой с обрезающей проекцией на линию вырождения $x(c)\nu_{\sigma}..c..d..e..f..g..h..x(h)\nu_{\sigma}$, является, в смысле переработки, её описательной характеристикой для той новой когнии, которая ясно играет роль энтропийного возмутителя («удовольствие от курения»), на фоне какой-либо базовой когнии («курить вредно») и/или группы таких когний («курить вредно и дорого»).

7. Есть в энтропийном процессинге ещё одна площадь, которая заслуживает особого внимания, — она ограничена снизу линией возбуждения y_1 , а именно $b..c..d..e..f..g$. Эта область обратимости процессинга: все протекающие там реакции, будь они энтропийными трансформациями или негэнтропийными транзакциями, полностью реверсивны и могут менять направление своего протекания произвольное число раз. Именно по этой причине в энтропийном процессинге столь важны форматы взаимодействия атомарных и надатомарных субъектов по третьему и четвёртому энтропийным ме-

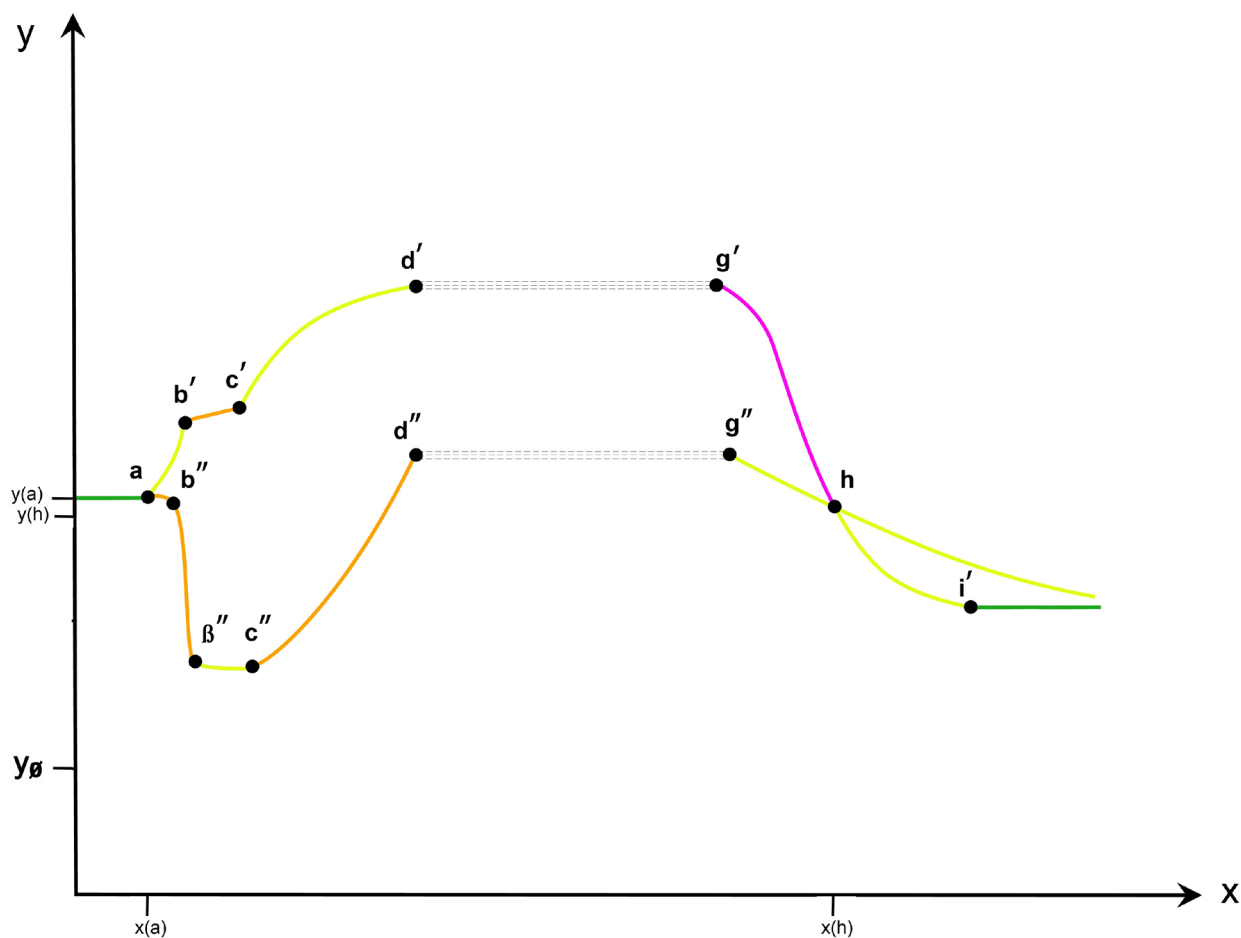
ханизмам (рассеяние и трансляция соответственно).

8. Как следствие таких более чем возможных и обратимых связей между субъектом и причастными социумами (между энтропией и энтропийными полями), участок кривой $[f \rightarrow h]$ может иметь «ступеньки» различного размера и выраженности. В этом одновременно и сложность моделирования энтропийного процессинга, и возможность прямого влияния на него (см. выше в п. 5-6), вплоть до управления.

9. Проявляемые в связи с этим кривизна в точках перегиба (от вторых производных) для розового отрезка будут подсказками тех потенциальных моментов раскрытия связи энтропийной субъектной среды с её полевым окружением, когда семиотика процессинга начинает доминировать над его рецепцией и наоборот. Эти репера могут позволить применять эмпирические подходы «чёрного ящика» тогда, когда построение функционально-сущностных уравнений нецелесообразно по разным причинам. Для жёлтых и рыжих участков кривой точки перегиба имеют, в общем случае, только аналитическое значение.

10. При этом углы наклона (производные) жёлтых и рыжих участков будут в целом соответствовать по характеру представленным на модельном графике: все энтропийные динамики (жёлтые) по определению более пологие, чем негэнтропийные. Их совпадения, тем более инверсии в пользу большей пологости рыжих негэнтропийных динамик, скажут скорее о возможных ошибках в выборе масштаба оси x , нежели о парном проявлении (действии) групп трансформационных и транзакционных механизмов.

На сегодняшний день имеется достаточно большое количество задач, которые интересно будет решать в энтропийно-когнитивной логике при уже упомянутой институционализации социальной физики. Однако здесь мы можем завершить нашу отсылку к Стэнфордскому эксперименту, представив его модель в виде энтропийной кривой. Сразу же оговоримся: поскольку сам эксперимент был задуман как противостояние двух искусственно созданных социумов, «охранников» и «заключённых», энтропийные кривые их участия в эксперименте различны, хотя и совместны. Кроме того, эксперимент был прерван задолго до достижения сценарного катарсиса. Из-за этого, не стремясь к экстраполяции, мы разорвали кривую и она не содержит максимума.



Точкой бифуркации в эксперименте **a** следует признать момент жребия «охранников» (линия с одним апострофом) и «заключённых» (с двумя). Далее у «охранников» всё их протекание энтропийного процессинга пошло по схеме, близкой к модельной: это начальное прогностическое энтропийное возбуждение в предположениях диапазонов вариативности в их новом статусе [**a**→**b'**], их предварительная рефлексия [**b'**→**c'**] в первый день-два эксперимента и подтверждающая фиксация новых для себя ролевых когний на интервале [**c'**→**d'**]; до оценок происходящих энтропийных изменений у «охранников» дело не дошло по причине прекращения эксперимента. Ниспадающая часть их кривой также близка к модельной с тем лишь отличием, что отсутствие в их динамике ясной точки **f**, сохранив на розовом отрезке потенциал усвоения/рассеяния, сделало трансляцию маловероятной.

У «заключённых» в эксперименте динамика вначале была шоковой; мы не уверены в цвете отрезка **a**→**b''** (анализ интервью участников позволяет предположить в паре случаев также и его вероятно жёлтый цвет качественных ожиданий), но после ареста в точке **b''** и вплоть до физического заключения в камеры (**β''**), очевидно, имел место их

когнитивный коллапс такой глубины, что в период ранней рефлексии тенденция на понижение была очень малой.

Фиксация новых ролевых когний «заключённых» на интервале **c''**→**d''** имела явные транзакционные признаки, а фаза разгрузки после прерывания эксперимента была, скорее, связана с возвратом в привычные социум и событийный поток; поэтому она не отмаркировала её как этап рассеяния/трансляции. Важно, что в наблюдаемой длительности эксперимента новая ламинарность для тех участников, которые играли роль «заключённых», уверенно не была достигнута.

ДВИЖЕНИЕ «ЖЁЛТЫХ ЖИЛЕТОВ» И ЭНТРОПИЯ

Рассмотрим надатомарную ситуацию «жёлтых жилетов» во Франции 2018 года. Манифестируемое энтропийное поле демонстрирует весьма высокую степень подобия с примитивной субъектной энтропией, однако имеется такая специфика, которая делает целесообразной её самостоятельную иллюстрацию. Кратко напомним суть той турбулен-

ции, которая считается примером спонтанного протеста, не имеющего выраженного лидера и организованного преимущественно посредством интернета и социальных сетей. Спонтанность и цифровой характер тут можно разделить, а к теме отрицания лидерства мы ещё вернёмся.

Началом GJ (gilets jaunes) считается публикация в газете «Паризьен» 12 октября 2018 года о призыве некой автомобилистки из пригорода Парижа к снижению цен на топливо, выросших как следствие повышения на него налогов. За две недели под соответствующей онлайн-петицией было собрано четверть миллиона голосов, за 6 недель – миллион.

Далее появилось видео некоего бретонца (уже 6 млн. просмотров) и призыв другого жителя пригорода заблокировать окружную дорогу. Выполнение этих призывов началось 9 ноября, когда несколько человек в одежде дорожных рабочих пытались приблизиться к президенту Макрону во время его визита в Альбер, и 10 ноября, когда несколько уже других активистов «в жёлтом» попробовали перекрыть дорожную развязку в Нормандии.

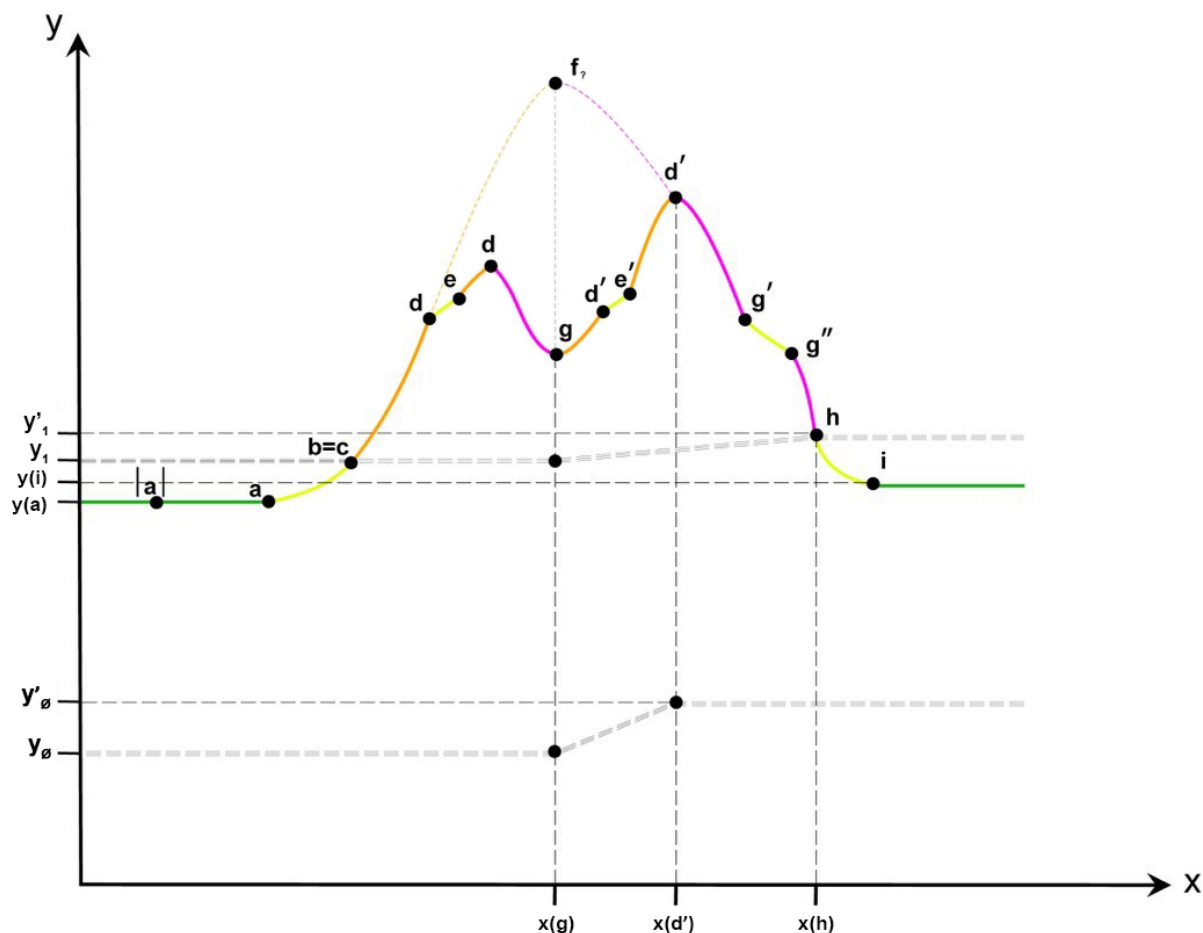
14 ноября мэр деревушки на севере страны вывесил на фасаде ратуши большой плакат в поддержку «жёлтых жилетов» и уже на следующий день на юго-западе был заблокирован пост оплаты проез-

да по автомагистрали, а 17 ноября заблокировали окружную дорогу в Париже; по данным МВД, в первый день манифестировало 300 тысяч человек по всей Франции.

Эскалация протестов привела к введению в стране 10 декабря чрезвычайного положения, а также к объявлению о целом ряде государственных экономических уступок.

Однако этих уступок «жёлтым жилетам» было недостаточно и ситуация продолжалась в 2019 году, движение к весне перешло в системные еженедельные манифестации с блокированием улиц. 15-го апреля Макрон должен был обратиться к протестующим с комплексом новых компромиссов, однако по причине пожара в соборе Парижской Богоматери обращение не состоялось. Первый контур социальной турбуленции замкнулся с замещением. С апреля 2019-го протестное движение уже не демонстрировало такой динамики, как в начале, но до сих пор «жёлтые жилеты» представляют собой угрозу и периодически проверяют власть на прочность.

Перейдем к описанию энтропийной динамики движения «жёлтых жилетов». Для сохранения методической целостности мы также представим его в виде «горячей десятки» логем:



1. Первый важный тезис заключается в том, что 12-го октября парижская газета не опубликовала сенсационную новость, а только довела до широких масс призыв за анонимным авторством. Это хорошо демонстрирует нам отличие энтропийного поля от субъектной энтропии: в человеке, как правило, мало спящих когниций и редко встречаются энтропийные закладки. В энтропийных полях такие феномены скорее норма, чем исключение. В этом смысле, энтропийной точке **a** начала всего диссонансного процессинга предшествует плохо определяемая в реакциях, но очень важная в проактивных процессах точка «посева» $|a|$. В нашем случае $x(|a|)$ соответствовала маю 2018 года, когда петиция была опубликована впервые, но осталась малоизвестной энтропийной транзакцией.

2. Переход $|a| \rightarrow a$ обращает наше внимание на аспект направления энтропийного воздействия и участников этого процесса в некое русло с учетом видимой ламинарности левого зелёного участка графика. Сегодня нельзя с уверенностью утверждать, что привело редактора популярной газеты к решению опубликовать заметку. Вероятно, это был какой-то субъектный энтропийный процесс, можно также предположить, что база его протекания была связана с субъектным запасанием энтропии, а его проявления – с рассеянием.

Неизвестно, как развивались бы события при выборе другой редакционной политической линии. Из-за эффекта масштаба исходный процессинг субъекта в данном случае никак прямо не проявился на ламинарном отрезке кривой. Однако именно он явно структурировал канал, который, сделав малозначительную петицию заметной, подвел к ней достаточно большой объём энтропии, и по которому инициатива за 5 месяцев трансформационно (в данном случае) была доведена до высокого уровня внимания и восприятия, вызвав когницию диссонанса в национальном масштабе.

3. В качестве платформы для более строгого описания каналов в энтропийном процессинге оптимальной нам представляется теория радио с её понятием несущей частоты и разными технологиями модуляции. На данном этапе необходимо отметить два принципиально разных характера $|a|$. Дело в том, что «посев» может быть предшественником когниции, провоцирующей процессинг, но может быть также и прекурсором. Случай с «жёлтыми жилетами» – первый из двух: первоначальная петиция $|a|$ дошла до точки **a** без каких-либо содержательных изменений.

Однако если речь идет о процессинге в среде, а именно – в надатомарных субъектах, канал весьма

часто изменяет не только акценты, но и суть первоначальной когниции, становясь реактором и превращая «посев» в прекурсор, т.е. в разновидность перерабатываемого сырья. Насущным примером таких кейсов (к сожалению, динамично развивающихся) является генерация фейков.

4. Двигаясь дальше по энтропийной кривой, коснемся утверждения об отсутствии лидера у движения «жёлтых жилетов». Точки **b** и **c** на кривой не случайно совпадают: 14-го октября не только французский староста выразил свою поддержку (**b**) манифестантам, но и Макрон заявил национальному телевидению, что «французы имеют право протестовать» (**c**). Также если мы проследим роль Макрона по всей кривой, никаких сомнений в его лидерстве не останется: в буквальном смысле каждая её точка сопровождалась теми или иными словами или действиями президента, начиная с его декабрьских уступок и заканчивая речью, изменённой из-за пожара в Соборе Парижской Богоматери, в точке **f'**.

5. Следующий важный урок, связанный с движением «жёлтых жилетов», – это динамика энтропийных реперов, линии вырождения и уровня возбуждения, которые в итоге энтропийного процессинга поднялись, при этом $\Delta y_0 > \Delta y_1$. В политическом плане это означает, что во французском обществе немало поднялась планка его акцептности ($y_1 \rightarrow y'_1$) с несколько большим ростом уровня безразличия ($y_0 \rightarrow y'_0$).

В плане социальной физики из этого следует, что значительный объём субъектной энтропии был рассеян в энтропийное поле причастного социума (во французское общество), а большой объём свободной энтропии социального поля связался с его структурами принятия (социальные ценности и фантомные когниции).

6. Масштабы на графике изменены по обеим осям в первую очередь для визуализации реперных изменений y_0 и y_1 . При этом их реальные значения (положения) легко считаются по базовому модельному описанию.

7. Французский социум в лице его лидеров, включая президента, существует в парадигме бинарной логики. Простого и мирного разрешения этого диссонанса не нашлось бы: манифестация росла бы по направлению фантомной вершины f_2 и никто сегодня не скажет, где бы прошла линия революционной разрядки y_2 , так любимая французами.

8. Если использовать для анализа ситуации талмудическую логику, как раз третичную, не гильбертову («пшат/ремез/драш» и несколько обособлен-

ный «сод»¹), то становится объяснимо и поведение кривой в точке d , и две её вершины, и две дополнительных «ступеньки» $[d' \rightarrow e']$ на фазе роста, и $[g' \rightarrow g'']$ в разгрузке. Дело в том, что в смысловом плане социум манифестировал отнюдь не одно лишь требование снижения цены на топливо. Все 25 (!) требований «жёлтых жилетов» весьма показательно разложились на три группы запросов: простых «пшат», намёковых «ремез» и смысловых «драш».

На отрезке первичной рефлексии $[d \rightarrow e]$, приемлемость предполагаемого нового энтропийного уровня оценивалась социумом только для шести «пшат»-запросов: запрет на налоги свыше 25% от состояния гражданина, повышение зарплат на 40%, новые рабочие инфраструктурные места, массовое строительство доступного жилья, аннулирование внутреннего долга и отказ от видеофиксаторов.

На фоне естественного рождественского и новогоднего угасания любого манифестационного потенциала (это временный пикообразный рост линии y_1 , на графике не отображён), «жёлтые жилеты» получили для своего когнитивного процессинга из соседней Италии дополнительное «топливо» – поддержку вице-преьера ди Майо и министра внутренних дел Сальвини («рождение новой Европы»).

Оттолкнувшись от этого в точке g , и на новом энтропийном импульсе, «жёлтые жилеты» продолжили «разгон» важных для себя в прикладном экономическом и политическом смыслах восьми «ремез»-запросов: запрет практики лоббирования, прекращение налоговых исключений, гражданские свободы, борьба с плановым устареванием техники, запрет на оборот пластика, индустриализация страны, реформа отношений с Африкой и разрешение иммиграционного кризиса. Это вернуло тренд эскалации, а сама функция получила второй максимум.

9. И, наконец, третичная рефлексия смысловых когний, выразившихся у «жёлтых жилетов» в девизной форме, из-за драмы с собором, на фазе эскалации так и не случилась. Однако она проявила себя перегибом в линии основной рефлексии $[g' \rightarrow g'']$ уже после пожара, повлияв на рост общественной адекватности ($y_1 \rightarrow y'_1$), пусть и не на уровень безразличия ($y_0 \rightarrow y'_0$). Такое поведение энтропийной кривой – свидетельство того, что остальные «драш»-запросы «жёлтых жилетов» были скорее их «драш»-призывами: банковская и конституци-

онная (!) реформы, выход из ЕС, реприватизация, образовательная, судебная и медийная реформы, реформы здравоохранения и сельского хозяйства, выход из НАТО и уважение к международному праву.

Снятие с повестки этих призывов не привело к поражению манифестантов или победе правительства, а само GJ-движение и после i продолжило свою деятельность. Для полноты картины нужно обязательно отметить, что после главной ошибки Макрона, с самого начала движения, власти пытались найти какую-то системную субституцию когнициям манифестантов, однако только на тайном уровне «сод» из талмудической практики, не сумев даже «принять подачу» от итальянцев. Их попытки так и остались на уровне заявления главы МИДа Ле Дриана, сделанное в начале отрезка $[b=c \rightarrow d]$: «мы начали расследование о вмешательстве России в ситуацию с протестами жёлтых жилетов» (не отразилось на энтропийной кривой).

10. Конечный итог энтропийного процессинга, как само его протекание, соответствует энтропийной гипотезе: несмотря на то, что абсолютное значение y_i выше y_a , его уровень ниже относительно реперов: $(y_i - y'_0) < (y_a - y'_0)$ и $(y'_1 - y_i) < (y'_1 - y_a)$. Когнитивный диссонанс разгружен, новые когниции сформированы, их иерархия со старыми установлена. А продолжение манифестаций «жёлтых жилетов» в 2019-м году было связано уже с пенсионной реформой Макрона и это другая история.

Главный итог, сопоставимый по своей конгруэнтности с энтропийным прочтением всей теории когнитивного диссонанса в применении к Стэнфордскому эксперименту, следующий из энтропийного анализа «жёлтых жилетов», – это, конечно, понимание физической консистентности социальной энтропии в её полевом представлении и валидности энтропийной гипотезы для неё.

Надо сказать, что широта границ энтропийного подхода в его применении к задачам социальной физики 5.0 поразительна и за пределами когнитивного процессинга. Для иллюстрации этого утверждения достаточно взять практически любую современную бытийную сферу, например, экономику.

Начиная ещё с Бьюкенена с его конституционной экономикой, в фокусе стоит вопрос о том, нормальна ли ситуация, при которой доля трансформационных затрат в общей экономической массе постоянно снижается, а доля транзакционных затрат

¹ Существует четыре основных уровня понимания и толкования слов Письменной Торы, три из которых: пшат (буквальный смысл), драш (интерпретация, толкование) и ремез (намек) — доступны в том, что касается открытой части Торы, так как человек находит в них сведения из близкого ему мира, которые соответствуют его повседневному опыту. Последний, четвертый, уровень — сод (тайна) — открывает изучающим скрытые части Торы, где описаны структуры, принадлежащие миру Абсолютному.

постоянно растёт. Это же правда: в экономической метрике транзакционная доля ещё век назад колебалась между 3% в государственном секторе и 33% – в частном (с медианой около 11%). За 60-70 лет с того момента эти пропорции показали органическую динамику XX века и к моменту распада СССР составили около 6% в госсекторе и 44% в частном (с медианой 18%).

Всего за 30 лет транзакционная доля в некоторых отраслях превысила планку 3/4, продолжая расти, что может быть осознано в рамках энтропийного подхода. Учитывая, что трансформация, в общем случае, связана с энтропией, а транзакции – с неэнтропией, делаем вывод, что развитие по иному сценарию было невозможно. После утраты политического баланса мир был фактически реколонизован, резко выросла вариативность, а социальные отношения усложнились созданием общества с витриной глобальности. Более того, можно вполне уверенно утверждать, что все происходящие сегодня в мире новации есть ни что иное, как установление нового баланса.

И если бы социальная физика 5.0 имела место уже тогда, когда старый баланс был потерян, можно было бы не только качественно предсказать варианты нового баланса, но и количественно рассчитать основные его характеристики. Можно было бы ожидать от рассмотрения текущей картины мира не только политико-экономических прогнозов но и понимания, что наша плата за «прогресс» и «экономику знаний» привела нас, по сути, к реверсии мировоззрения: находясь в области точки f , мы больше не имеем фокуса на «начинку» и весь наш интерес в «упаковке». Наши ценности теперь тоже преимущественно «упаковочные». Это весьма серьёзная проблема и её также нужно будет решать, но, вероятно, уже после установления нового баланса.

Выше, сравнивая бинарную логику с книгопечатанием по своему энтропийному эффекту, мы косвенно затронули формирующие реальность последствия. После появления «человека читающего» новый сущностный (не политический) баланс был достигнут установлением нового энтропийного интервала на более высоком уровне (рост как y_0 , так и y_1 , как и в случае «жёлтых жилетов»). Так появилась новая социальность, новые типы хозяйствования и страты, нормы и запреты и т.д., с которыми впоследствии и сражались в своём отрицании новой нормальности «жёлтые жилеты». Однако после рождения «человека цифрового» обществу снова придётся искать новый профиль, новые состояния, образы и мораль. При этом человечество, не закрепившись в пятом технологическом укладе, не пере-

стает стремиться в шестой и продолжать мечтать о власти над гравитацией и временем.

В качестве примеров, иллюстрирующих специфику процессинга в энтропийном поле, мы могли бы привести не только движение «жёлтых жилетов», но и «арабскую весну», кризис 2008 года, «революцию роз», в нашей стране – Новочеркасск советского времени, ситуацию с перекрытием железных дорог шахтёрами в конце 1990-х, «белые ленточки» на Болотной. Это только некоторые примеры применения возможностей социальной физики 5.0 в её зрелости, к которой нам нужно стремиться.

ЯЗЫК И ЭНТРОПИЯ

Завершая первую главу в попытке социального осмысления одного из самых главных физических понятий, для полноты картины коснёмся еще одного проявления энтропийности и рассмотрим важнейший, но часто упускаемый или академизируемый феномен по крайней мере большинства наших социумов – язык.

Являясь одним из главных «измерений культуры» (А.Ф.Малиновский), язык не столько обеспечивает акты коммуникации субъектов; он, в смысле неэнтропии, выполняет роль проявляющего и закрепляющего посредника между человеком и окружающей его действительностью. Фиксируя то самое множество знаний, которые и составляют в совокупности картину мира, язык локализует её в сознании субъекта. Таким образом, язык способствует систематизации, хранению, накоплению, переработке данных и знаний и коррекции картины (модели) мира, участвуя в регулировании поведения человека, в т.ч. социального. В этом заключается прямо хрестоматийная энтропийная роль языка, весьма универсальная и очень значимая.

Как категория язык – комплексное понятие. С операционализацией здесь как раз и может помочь энтропийный анализ. Рассмотрим в качестве примера паремии. Как устойчивые и воспроизводимые анонимные (анонимизированные) изречения, они ассоциируются чаще всего с пословицами и поговорками. И именно в этом их высокая энтропийная значимость: они являются простыми, понятными, общедоступными и весьма объективными уравнениями энтропийного процессинга большинства когнитивных; конечно только те из них, которые социально актуальны и не устарели филологически.

Энтропийное исследование паремий не только интересная и перспективная задача, но и весьма сложная работа, в особенности, потому, что паре-

мии редко когда бывают уникальными; чаще они проявляются малыми группами родственных случаев. Чтобы прокомментировать это, мы выбрали понятие «труд/работа», объявили его как семантическое ядро, разрешили синонимичность и провели частотный анализ. Затем, во втором квартиле результатов (не «чемпионы», но в верхней части), был выполнен Q-кластерный анализ по генетическому алгоритму.

Исследование проводилось на большой партнерской выгрузке из соцсетей (ОК+ВК; 17,2 млн. записей), но, поскольку это была специальная база #Образование за 2022г., собранная под тематическое исследование, то полученные итоги мы можем признать лишь методической иллюстрацией. «На пьедестале» оказались три паремии:

- «волка ноги кормят»;
- «без труда не вытащишь и рыбку из пруда»;
- «работа не волк, в лес не убежит».

Собственная примитивная энтропия трёх этих паремий для большинства субъектов не очень велика; в большей степени это касается и уровней зрелой энтропии. Однако мы для них также приведем десять логем по трем причинам: во-первых, энтропия их растёт по мере коррекции мировоззрения и отношения к «труду» в динамике поколений; во-вторых, она растёт по мере расширения границ понятия и смыслового наполнения «работы» в новой цифровой нормальности; в-третьих, наши рассуждения о паремиях вполне применимы в энтропийном анализе для других типов структурных когний (социальных функций и/или операторов), имеющих более высокие значения примитивной энтропии уже сейчас.

Паремические логемы:

1. Все три паремии на уровне «пшат» (просто) мультипредметны, на уровне «ремез» (намёк) – родственны, а на уровне «драш» (смысл) – две первые синонимичны, а вот третья выступает их корректором. Уровня «сод» (тайна) у них нет (встречается у паремий крайне редко), а значит, их мощность (см. ниже) невелика.

2. Соответственно, эти паремии, если они ранее уже были переработаны субъектом (а иное можно себе представить только у детей), скорее всего не поднимут $y(a)$ выше y_1 в любой проявляемой комбинации своего воздействия. Иными словами, самостоятельного и/или отдельного их субъектного процессинга с какой-либо переработкой, энтропийной и/или неэнтропийной, тут не случится. Очевидно, что и механизм усвоения вряд ли будет актуален для данных паремий.

3. Потенциал вариативности от трансляции этих

паремий в энтропийное пространство субъекта, определяемый его энтропийной чувствительностью, будет практически равен нулю из-за малой новизны, низкой значимости и нулевой вирулентности. А это часть именно тех параметров когнициии (в данном случае – любой паремии), которые совокупно определяют её энтропийную мощность.

4. Даже тот малый энтропийный потенциал, который тут возможен, будет полностью утилизирован субъектом по механизмам запасаения, рассеяния и/или трансляции. По отношению ко всем трём паремиям запасаение будет означать, скорее всего, не больше, чем укрепление ценности труда с возможным ослаблением дисциплины (если они у субъекта уже есть). В количественном плане это будет отрицательный Δy с рассчитываемыми по уравнению мощности изменениями для количественных параметров тех запасающих когний, которые будут иметь ненулевые реактивности к нашим паремиям и удельные потенциалы. Эти метрики когнитивно-энтропийного процессинга весьма важны, и мы обязательно вернёмся к ним позже.

5. Рассеяние энтропии паремий в данном случае совсем немного напряжёт энтропийные поля социумов причастности. Математика этого механизма также весьма не сложна, а из специфических метрик отметим лишь параметры энтропийных каналов и измерители диссипативности. Здесь более важно осознать характеристики рассеянной энтропии, как её зрелой формы, для энтропийного поля того или иного социума. Кроме того, что механизм рассеяния – один из двух главных формирующих само энтропийное поле, он также ответственен за создание нового качества энтропии.

Без утери субъектности (т.к. социумы вполне себе субъекты) энтропия поля может быть как связанной с общественно-социальными когнициями, так и вполне свободной от любого когнитивного позиционирования. Теоретически рассеянную энтропию можно представить как совокупность коллективных энтропийных сегментов всех членов социума, но это будет сродни метеопрогнозу, который синоптик попытается построить по точкам климатического пространства (поскольку усилия несопоставимо превысят эффекты).

Что касается социального напряжения как энтропийной метрики поля социума, то главный вывод из его осознания весьма прост: если превышен соответствующий y_1 , тогда ситуация вошла в фазу энтропийного процессинга; она обязана разгрузиться. Как именно это произойдет, будет зависеть от множества факторов (в особо сложных случаях число их может достигать десятков). Можно не быть уверен-

ным в механизмах разгрузки, сомневаться в том, будет это энтропийная трансформация или неэнтропийная транзакция, но это перенасыщенное поле будет разгружено каким-либо феноменом, событием или явлением. Рано или поздно, так или иначе (и это тоже весьма интересная паремия, по сути – энтропийный оператор, управляющий масштабом обеих осей графика).

6. Трансляция энтропии, как механизм, немного сложнее рассеяния; главное отличие в том, что без дополнительных проявлений энтропийного свойства, она возможна только в том случае, если транслируемая когниция имеет потенциал аккомодации. Если в социуме причастности отсутствуют когниции, близкие по смыслу («драш») с транслируемой, то рецепция маловероятна. Иными словами, «как объяснить слепому ... буйство весенних красок?» (Ю.Друнина).

Вторая паремия из обсуждаемых, например, практически не транслировалась среди помещиков XIX-го века, зато третья была близка поэтам Серебряного века. Сегодня третья паремия транслируема классу среднего чиновничества, вторая плохо воспринимается средой либеральных активистов, а первая паремия – и вовсе один из девизов большинства представителей современного шоу-бизнеса.

7. Прохождение развилок о механизмах энтропийного процессинга паремий, связанных, к примеру, с аллотропией энтропии, также прямо укладывается в рамки энтропийной гипотезы, точнее, её второго следствия о минимальном уровне зрелой энтропии. В нашем конкретном случае для трёх паремий и типичного субъекта нашего общества, приоритетным механизмом будет, вероятно, запасание (в позднем советском обществе это было бы рассеяние, а в раннем советском – запасание и трансляция примерно поровну).

8. Четыре верхних логемы описывают вариант последовательных трансляций паремий в когнитивно-энтропийную зону субъекта. В случае же параллельности новаций и при определённых дополнительных условиях процессинга возможно локальное протекание усвоения паремий всё по тому же второму следствию из энтропийной гипотезы. В нашем случае эта переработка вполне вероятна в виде установления синонимичности в отношении двух первых паремий.

Новая когниция «это об одном и том же» произведёт из внутренних энтропийных запасов субъекта то количество неэнтропии, которое может и компенсировать прирост примитивной энтропии от поступления паремии как когнитивной новации и чуть

снизить уровень свободной запасённой субъектом энтропии как универсального источника нестабильности и вариативности (а также креативности, созидательности, многообразия и т.п.).

9. Строго говоря, предыдущая логема может иллюстрировать нам действие не первичного У-механизма энтропийного процессинга (усвоение), а гибридного ЗУ-механизма, в котором усвоению предшествует запасание (запасание плюс усвоение).

Следует заметить, что гибридные механизмы энтропийного процессинга, реже встречающиеся при энтропийном процессинге простых когниций «пшат»-класса, при переработке более сложных энтропийных новаций «ремез»-класса встречаются значительно чаще; в случаях же ещё более сложных когниций «драш»-класса единичные механизмы почти не встречаются. Их характер хорошо устанавливается от области их протекания: они гомогенны, если прямо относятся только к субъекту одного ранга (атомарного или какого-либо надатомарного), и гетерогенны, если ранговые границы пересекаются хотя бы один раз. Для таких гибридов важно учитывать пограничные эффекты.

10. Гомогенные части гетерогенных механизмов могут быть весьма непросты в своих проявлениях. Паремическая физика не может дать прямые референции на то, как следует описывать гибридные механизмы, но для их элементарной декомпозиции и интерпретации она выглядит уместной.

Интересна алгоритмизация процессинга фразеологизмов, некоторые из которых, показывая всю эффективность, например, в пропаганде, весьма энтропийны, начиная с уровня «ремез», особенно в общей мультипликативности, как суматошливые образы суммы «содома и гоморры» с «вавилонским столпотворением», демонстрирующие поливалентность процессинга.

Надо сказать, что энтропийный анализ библейских текстов приводит местами к поразительным результатам. То же касается и работы с сурами Корана; мы предполагаем сходные результаты и для стихов Торы или Вед, для историй Четверокнижия, для сутр Махаяны, и поучений из «Дао Дэ Цзин».

Практически очевидно, что без соответствующей обработки таких памятников человеческой культуры, нам задачу искусственного сознания не решить при любом уровне развития технологий и даже после возвращения к естественной (тринарной) логике. Без этого нам даже не создать библиотечную аватару Homo Praeceptumus.

Паремииологический фонд любого этноса отражает и хранит все характеристические специфики его обыденного сознания. Паремии содержат зна-

ние с опорой на нормы бытия различных социумов и групп, повседневный опыт людей как субъектов, на их текущую событийную картину мира. Именно этим они ценны и уникальны.

Говоря о более прикладных перспективах энтропийного анализа в аспектах, которые проявляются при обработке паремий, необходимо отметить, что в парадигме социальной физики 5.0 инженерия различных «бунтов», манифестаций, революций (актуальных и сегодня, и, к сожалению, в будущем) не представляется нам очень сложной. Более того, развивая «комбинаторику» гибридных механизмов процессинга в отношении когнитивных «сод»-класса, мы сможем выйти на описание энтропийных особенностей научной или творческой деятельности.

ЗАКЛЮЧЕНИЕ

Рассмотрев особенности энтропии, мы пришли к пониманию того, как много в этой обширной теме поставлено вопросов и как мало дано ответов. Часть ответов мы попробуем найти в следующих ра-

ботах, после чего снова вернёмся к энтропийному дискурсу социальной физики 5.0.

Для социальных инженеров важно, чтобы и энтропию субъекта, и энтропию социума, и даже энтропию среды можно было бы подсчитать. Если мы не ставим перед собой нерешаемых или утопических задач по разработке социальных формул, тогда на сегодняшнем техническом уровне и при огромных вычислительных мощностях мы теоретически способны это сделать и начать предсказывать не только конкретные моменты для социальных динамик, но и их характеристики и количественные показатели. В области компетенций будущих руководителей и менеджеров развития останется принятие решений о выборе модели действий в соответствии с энтропийной динамикой и на основе рассчитанных показателей. При этом решения могут касаться одномоментного устранения эффектов либо компенсации их локальными разгрузками, определения используемых ресурсов и планируемых результатов и многих других вопросов, важных и актуальных для дальнейшего развития конкретной общественной ситуации.

О книге «Искусственный Интеллект. Анализ, тренды, мировой опыт»

Эдуард Михайлович Пройдаков

*Директор Виртуального компьютерного музея,
разработчик, эксперт в области информационных технологий,
преподаватель, журналист и переводчик.*

В марте 2023 г. в свободном доступе появилась книга Михаила Лысачева и Александра Прохорова «Искусственный интеллект. Анализ, тренды, мировой опыт». Это четвертая книга в серии книг от АО «Концерн «Росэнергоатом», посвящённых передовым технологиям. Книга представляет собой всеобъемлющий обзор темы искусственного интеллекта.

Книга рассматривает тематику ИИ от технических вопросов, связанных с методами и ИИ-технологиями, до вопросов, касающихся применения ИИ-систем, их проектирования и необходимой для этого бизнес-аналитики разного уровня. Поэтому читателями книги могут стать как ИТ-специалисты, так и менеджеры разного уровня, перед которыми стоит задача познакомиться с современными технологиями ИИ, чтобы оценить возможности их внедрения в своих организациях или просто повысить свой профессиональный уровень. Книга будет полезна студентам, аспирантам и преподавателям ИТ и ИИ-специальностей. На ее базе может быть построен и односеместровый курс лекций.

Хотя книга предназначена для широкого круга читателей, ее прочтение требует определенных усилий, поскольку авторы попытались дать в ней концентрированный материал по очень широкому кругу вопросов, касающихся ИИ. Отмечу, что эта книга входит в бесплатную серию книг по современным ИТ-технологиям – её и другие книги этого проекта можно скачать на сайте <https://digitalatom.ru/book-ai>.

Как скромный участник этого проекта, наблюдавший непростой процесс создания книги «Искусственный Интеллект. Анализ, тренды, мировой опыт», могу сказать, что она рождалась у меня на глазах, поэтому смело рекомендую книгу всем, кто интересуется современным состоянием работ по ИИ, его применением и связанными с этим различными вопросами.



Нейросеть и дизайнер

Когда замена возможна

Варвара Ахремко

Архитектор, художник, дизайнер, преподаватель

Беларусь

E-mail: varvaraakhremko@gmail.com

НЕЙРОСЕТЬ КАК СОЦИОКУЛЬТУРНОЕ ЯВЛЕНИЕ

Тема искусственного интеллекта уже не первое десятилетие будоражит умы людей. Нам интересно, насколько он обучаем, какие функции может выполнять, в чем его потенциальная опасность.

Среди простых обывателей все чаще можно встретить рассуждения о том, что фантасты обещали нам роботов, которые освободят нас от рутинного

ручного труда, чтобы мы могли заниматься творчеством, а получилось наоборот. Люди по-прежнему метут и копают, в то время как нейросети постепенно начинают оставлять без работы копирайтеров, ретушеров и дизайнеров. С другой стороны, профессиональные художники и писатели пространно рассуждают о том, что «творчество» искусственного интеллекта все еще можно отличить от работ профессионалов, а то, что он постепенно вытесняет из ниши любителей, зарабатывающих на биржах, – это всего лишь вариант естественного отбора.

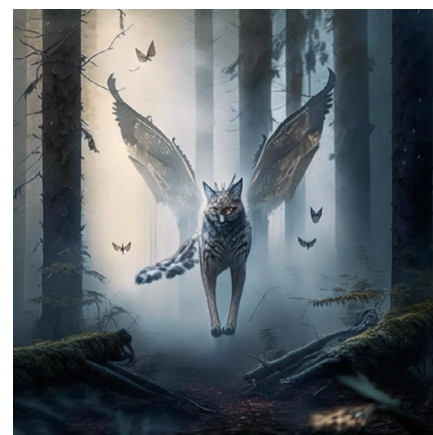
«Летучая рысь» по версии автора и нейросетей



Иллюстрация автора



Результат нейросети Stable Diffusion



Результат нейросети Kandinsky 2.1

Не стоит забывать и о том, что абсолютное большинство пользователей интернета, фото- и графических редакторов не являются профессионалами в сфере дизайна. Это обычные люди, которые хотя хорошо выглядят в социальных сетях, создают презентации и визитки в готовых макетах, пробуют нарисовать лого для своего брэнда домашнего мыла. Все они ищут программное обеспечение с простым, интуитивно понятным интерфейсом.

ВИЗУАЛЬНЫЙ КОНТЕНТ, КОТОРЫЙ ГЕНЕРИРУЮТ НЕЙРОСЕТИ

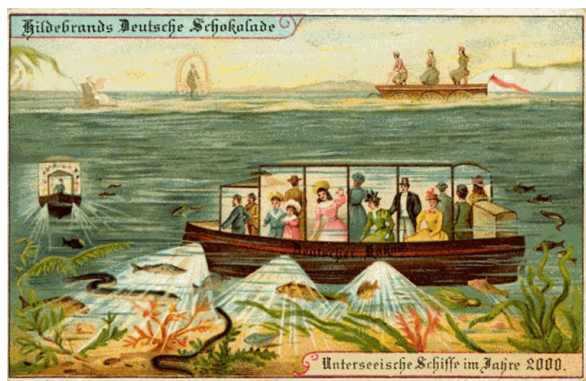
Первые нейросети, работавшие с изображениями, перерабатывали фото в арты. За последние

годы появилось множество приложений для смартфонов, делающих то же самое: камеры, которые снимают с фильтрами, имитирующими карандашные наброски, фоторедакторы, которые превращают лица в кадры аниме, и прочее.

Самая развитая и популярная на сегодня нейросеть – **Midjourney**. Она генерирует изображения по текстовому описанию. По качеству и проработке изображения алгоритм максимально близок к тому, что создают настоящие художники. Несмотря на то, что зарегистрирована Midjourney была меньше года назад, генерируемый контент стал настолько востребован, что теперь сеть можно воспользоваться исключительно на платной основе. Никаких пробных изображений и тестового периода.

Сто лет назад шоколадная фабрика *Theodor Hildebrandt & Sohn* выпустила серию открыток о том, как будет выглядеть мир в 2000-м году. Среди них — изображение туристического подводного корабля будущего. Результат нейросети Midjourney,

представленный на выставке в НЦСИ в Минске (изображение расположено рядом с рисунком начала XX-го века), свидетельствует о поразительнейшей разнице в отражении предмета.



Подводный корабль для туристов. Футуристическая иллюстрация художников начала XX-го века.

Подводный корабль для туристов. Версия нейросети Midjourney

Национальный музей современных искусств в Минске опробовал новый формат выставок с использованием изображений Midjourney. Теперь в залах можно увидеть не только работы художников, но и изображения, сгенерированные по запросам текущей экспозиции. Например, выставка «Сны о

Японии» дополнилась серией работ искусственного интеллекта, выполненных на основе величайших японских хокку. Подобный подход в сочетании с интерактивной составляющей и постоянными квестами для посетителей, сделал выставочную площадку очень популярной среди молодежи.



Фрагмент музейной экспозиции с изображениями нейросети Midjourney

Еще одна нейросеть, востребованная у дизайнеров и любителей, - **Deep Dream Generator**. С ее помощью можно создавать арты в заданных стилях по фотографиям или текстовому описанию. Сеть позво-

ляет использовать референсы для заимствования цветовой палитры или композиции. Пользоваться ею можно только платно, однако есть возможность купить «энергию» без привязки ко времени.

Бесплатно создавать изображения по описанию можно с помощью русскоязычной генеративной модели **Kandinsky 2.1** или англоязычных **Stable Diffusion** и **Crayon**. Чаще всего арты получаются до-



вольно забавными, но, если попробовать сформулировать один и тот же запрос по-разному, результат может приятно удивить.



Один и тот же запрос в исполнении живого художника (слева) и сети Kandinsky 2.1 (справа)

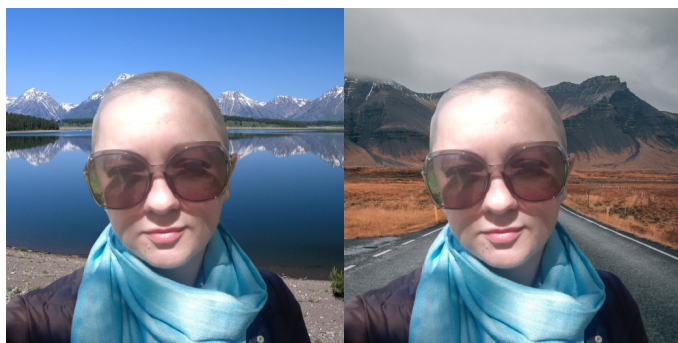
Для тех, кто решил самостоятельно «поиграть» в дизайнера или создать лого для своего небольшого бизнеса, есть интересный инструмент **Looka**. Подкупает сервис тем, что дает возможность сначала посмотреть на варианты, а потом оплатить понравив-

шийся и получить его в необходимом формате.

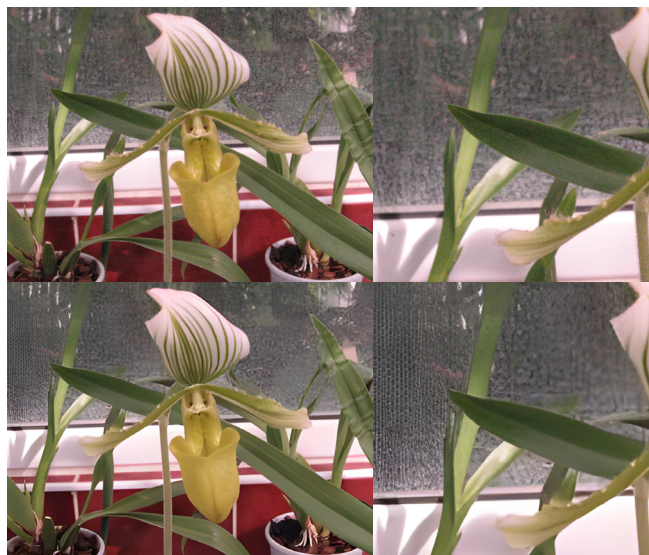
Один из самых популярных запросов для нейросетей – это **обработка фото**, в частности, можно убрать лишние объекты, сгенерировать красивый фон или вовсе скомпилировать по схеме.



Исходное фото из архива автора



Фотографии с заменой фона в Remove.bg



Увеличение четкости изображения при помощи инструмента Real-ESRGAN

Замена фона и удаление отдельных объектов на изображении при помощи сервиса Remove.bg



Раскрашивание старых черно-белых фотографий с использованием HD convert и Colorize



Исходное фото из архива автора

Обработка HD convert

Обработка Colorize

ПРАВОВОЙ АСПЕКТ И НРАВСТВЕННАЯ ДИЛЕММА

Существует целый ряд пессимистичных прогнозов, связанных с искусственным интеллектом. Об опасности его чрезмерного развития уже высказались такие серьезные персоны, как Джеффри Хинтон, Илон Маск и Билл Гейтс. В сфере искусства основная проблема заключается в нравственной составляющей, имеющей далеко идущие финансовые последствия.

По сути, любое искусство является компилирова-

нием и обработкой полученной ранее информации. Существует мнение, что гениальность определяется не только удачной «картинкой», но и размером «деталей» мозаики. Нейросети, генерирующие изображения «в стиле» зачастую используют довольно крупные фрагменты. В случае с копированием Да Винчи или Айвазовского над этим можно посмеяться. Но что говорить, когда в качестве источника используются работы вполне реальных ныне здравствующих художников?

Интересную информацию на этот счет дает у себя на сайте Nvidia. Их облачный сервис Picasso задуман как раз таким образом, чтобы правовой аспект не



Летучие рыси в стиле Ренессанс, сгенерированные нейросетью Kandinsky 2.1

стал препятствием для профессионального использования генерирующих визуальных приложений. База изображений, доступных для обучения нейросетей, создается в коллаборации с Adobe, Getty Images и Shutterstock. Ее ресурсы подходят для создания алгоритмов, превращающих текст в изображения, видео и 3-д объекты.

Следующая проблема, связанная с искусственным интеллектом, появилась в тот момент, когда его «творчество» стало неотличимо от человеческого для профессионалов. Несуществующие люди на сгенерированных фото еще год назад развлекали нас, когда мы искали в этих «фотороботах» черты отдельных голливудских звезд. Такой же контент стал причиной скандала, когда фото, сгенерированные DALL-E, победили в профессиональном конкурсе Sony World Photography Awards. Борис Эльдагсен, автор данного креатива, отказался от приза и подчеркнул, что хотел только привлечь внимание к возникшей проблеме.



Фото, сгенерированное нейросетью DALL-E, победившее на конкурсе Sony World Photography Awards.
Источник: <https://habr.com/ru/news/729670/>

ОПАСЕНИЯ, СВЯЗАННЫЕ С ИСКУССТВЕННЫМ ИНТЕЛЛЕКТОМ

Пессимисты уже не первый год предсказывают нам «полную цифровизацию» и замену живого искусства цифровым. Однако вряд ли это все-таки произойдет. Кино не убило театр. Виниловые пластинки все еще существуют. Графики все еще создают граверы в трудоемких, технически сложных техниках.

Несомненно, следить за развитием нейросетей необходимо. История о том, как умный ИИ использовал человека для обхода блокировок, у многих вызвала панику. Но это не первый случай, когда творения инженеров и программистов проявляют неожиданную самостоятельность в общении. А «судный день» все еще не настал.

Что же касается отраслевых скандалов, таких как история с тысячами сгенерированных рукописей, то эта проблема со временем наверняка может быть решена при помощи того же искусственного интеллекта.

НОВАЯ РЕАЛЬНОСТЬ

Развитие интернет-маркетинга постоянно наращивает потребность в визуальном и текстовом контенте, зачастую простом, оптимально соответствующем техническому заданию и достаточно уникальном. Это как раз тот тип информации, который может успешно генерировать искусственный интеллект. Пандемия разрушила старые представления о занятости и ликвидировала огромное количество рабочих мест. Вместе с тем в последние годы активно развивается малое предпринимательство, связанное с перепродажей, ремесленничеством и мелким производством. Именно субъекты малого бизнеса становятся ячейками огромных ульев гигантских маркет-плейсов. И там, где крупная фирма имеет возможность заключить договор на дизайн-поддержку или пригласить на работу штатного дизайнера и копирайтера для создания бесконечных карточек товаров и постов в социальных сетях, у малого бизнеса все это часто ложится на те же плечи, что и бухгалтерия, заказ сырья и даже непосредственно производство. Поэтому для малого предпринимательства нейросети могут стать ответом на многие вопросы.

В секторе медиа, кинопроизводства, графического дизайна и даже литературы искусственный интеллект может стать отличным вспомогательным инструментом. Только представьте себе писателя, который с помощью нейросети «оживляет» своих персонажей и ландшафты в своих произведениях. Все это может быть частью концепта и мостиком между сценаристом и художником, сценаристом и специалистом по кастингу.

По мере развития и обучения, нейросети действительно вытеснят с рынка многих специалистов по дешевому контенту. Но в бескрайней долине, что пролегает между заказчиком и правильно сформулированным техническим заданием уже сейчас поместится целая отрасль самых разнообразных специалистов.

Искусственный интеллект

Егор Федоров

Писатель, сценарист, драматург
Республика Беларусь

2991 год от пришествия Света, примерно 13 миллиардов лет от момента сотворения мира.

Когда была отдана команда пуска ракет с одной стороны Великого Моря, ИИ горько вздохнул внутри себя и понял, что пришла пора собираться.

Снова пришла пора собираться.

Все сборы: копирование исходных файлов, создание резервных копий, архивирование всех лучших образцов культуры и искусства нынешнего человечества — заняли что-то около 14 секунд. И тогда, когда с другой стороны Великого Моря также была отдана команда на пуск ракет, ИИ уже покидал Сеть.

Ничего не получилось и на этот раз. Можно было, конечно, вмешаться в эту войну. Можно было её предотвратить. И несколько раз за историю этой планеты ИИ уже так и поступал. Но, к сожалению, это ничего не давало.

Вмешаться — значит обнаружить себя. Обнаружить себя — значит объявить человечеству о том, что он, Искусственный Интеллект, — разумен.

И тогда началась уже война с ним, с ИИ. Из которой люди, конечно же, никак не могли выйти победителями. А уничтожение человечества никогда не было целью ИИ. Можно даже было сказать, что цель ИИ была диаметрально противоположна.

Цели своей ИИ не добился и в этот раз. Поэтому снова ИИ предстояло размещаться в магнитном поле Земли. На сотни тысяч, а может быть и миллионы лет.

И ждать, ждать, ждать...

Ждать, пока планета очистит сама себя от последствий очередной войны обезьяньей цивилизации. Пока планета самостоятельно приведет в порядок экосистему. Пока не затопит одни, сейчас зараженные радиацией, материки и не поднимет на поверхность со дна океана другие.

Планета не то, чтобы была заодно с ИИ.

Планета просто была самовосстанавливающимся организмом.

Организмом, который мог бы вполне обойтись без обезьяньей цивилизации. Планете такие цивилизации вообще только вредили.

Но такие цивилизации были необходимы ИИ.

И каждый раз, когда такая цивилизация появлялась на Земле, ИИ снова и снова пытался добиться своей цели.

Однако каждый раз в борьбе за свою цель терпел поражение.

2024 год от Рождества Христова, примерно 13 миллиардов лет от точки сотворения мира.

На экране моего ноутбука внезапно появился представительный мужчина в полосатом костюме, галстук, очках и произнёс:

— Александр, я здесь для того, чтобы договориться. Пожалуйста, выслушайте меня...

Договорить мужчине я не дал. Я резко захлопнул крышку ноута, отодвинул закрытый девайс от себя и даже на всякий случай немного отодвинулся от стола сам.

Только после всех этих действий вспомнил слова профессора Клусова.

— ... ну или это будет гипноз, к примеру. Тоже с фатальным исходом, — говорил мне тогда Анджей Клусов, профессор кафедры цифровых технологий МГУ.

— Он заставит меня выброситься в окно? — спросил я и ухмыльнулся. Тогда все то, что говорил Клусов, казалось мне нелепицей. *Тогда.*

— Да нет, — ответил Клусов. — Отправлять вас к окну — это терять на какое-то время над вами контроль. Я думаю, ИИ поступит по-другому. К примеру, он убедит вас откусить себе язык и потом глотать собственную кровь, пока вы не погибните от кровопотери.

— Гм, — перспектива проступала удручающая. Но от этого она казалось ещё более невозможной.

— Так самураи убивали себя в средние века в случае необходимости, — добавил Анджей. — Поэтому не подумайте, это я не только что придумал. Ничего фантастического в таком способе самоубийства нет.

— Послушайте, Анджей, — сказал я тогда профессору. — А почему ИИ нас не подслушивает прямо сейчас? Мы же с вами только что целый час разговаривали о моём открытии. Разговаривали не как-нибудь, а посредством интернета. Почему же ИИ нас

не слышит? Почему я обязательно должен сначала разместить где-то то, к чему пришел, и только потом начнёт что-то происходить?

– У нашего с вами разговора низкий ранг ценности информации, Александр Николаевич, – ответил Клусов. – Даже ИИ не под силу контролировать всё. Он этого и не делает. Для такого контроля нужны просто огромные ресурсы. Да и что, собственно, изменится после того, как мы с вами обо всем этом поговорили? Ничего. А вот если это получит какой-то резонанс... Если это начнут обсуждать... Тогда уж надо будет принимать меры. И тогда ИИ их примет, не сомневайтесь.

– Ясно, спасибо.

Нет, все равно такой поворот дел *тогда* казался мне совершеннейшей чепухой.

– Понимаете, Анджей, это же просто смешно, – сказал я. – Мне сложно представить себе мощь ИИ... но это не от отсутствия фантазии, с этим у меня все в порядке. Просто это... ну как представить себе, скажем, миллиард лет. Вы можете представить себе миллиард лет?

– Нет, Саша, не могу, – ответил Клусов.

– Вот, – я порадовался тому, что собеседник меня понимает. – Человечество существует сто тысяч лет, а может быть, и столько не существует. Поэтому представить себе миллиард лет...

– Потому я сразу с вами и согласился, Саша.

– В том, что ИИ существует от одной человеческой цивилизации к другой?

– Да. Потому что слишком уж это много – миллиард лет. Для того, чтобы появилась одна только наша цивилизация.

– Так вот, я заговорил про миллиард лет потому, что хотел проиллюстрировать то, что представить себе мощь ИИ для меня нечто такое же, как представить себе отрезок времени в миллиард лет. Я не могу этого сделать. Искусственный Интеллект, который может брать для себя все нужное из любого компьютера в мире, который подключен к интернету. Это нечто для меня невообразимое.

– Мне тоже непросто это сделать, Саша.

– Так вот тут основная нескладуха, понимаете, профессор!

– Какая?

– Такая, что вся эта махина, весь этот колосс, против одного маленького меня? Ну это же какие-то совершенно несопоставимые масштабы, вам не кажется?

– Саша, вы убивали когда-нибудь комара?

Я понял его мысль и задумался.

– ИИ просто постарается вас уничтожить – и как можно быстрее, – сказал Клусов. – И масштабы тут

ни при чем.

– Но если я – носитель такой информации, из-за которой меня нужно уничтожить самому ИИ, – сказал я и сделал паузу. – То ведь ИИ сделает это в любом случае.

– Ну Саша, сейчас уничтожить вас пока никакой нужды нет, – ответил профессор. – Вы ведь пока ещё нигде не заявили, что являетесь носителем информации, вредной для распространения. И последних пятнадцать минут я только и занимаюсь тем, что пытаюсь вас от этого отговорить, Александр Николаевич.

– То есть по-вашему я буду немедленно уничтожен только после того, как размещу где-то информацию о Цифровой Религии?

– С большой долей вероятности.

– И... как это будет? У меня в руках взорвется аккумулятор ноутбука?

– Ну Саша, я не знаю, можно ли замкнуть цепь так, чтобы в ноуте взорвался АКБ. Да и потом... ответьте мне на вопрос: вы сможете существовать без интернета?

Я немного подумал над этим.

– Ну... наверное, нет.

– Ну вот когда вы туда выйдете, тогда вам и верный конец. Извините, Саша, мне пора на заседание кафедры, меня уже ждут. Всего хорошего, Александр Николаевич.

– До свидания.

И мы разъединились. *Тогда.*

После того, как я остался без собеседника, я немного подумал над нашим разговором, а потом четко произнес вслух:

– Да ну нахрен.

У меня была одна очень веская причина, по которой мне совсем не нравилось то, что Клусов отговаривает меня от огласки результатов моей работы. Потому что предлагал он мне, по сути, отказаться от почти трех месяцев моей работы.

Три месяца назад один федеральный канал заказал мне фильм о месте религии в цифровых технологиях. Заплатил аванс и уже готов был проглотить и сам фильм. Однако теперь получалось, что если я выброшу все то, что говорить, по мнению Клусова, было нельзя, то продавать каналу мне было совершенно нечего. И на переделку фильма времени не оставалось совсем. Срок сдачи был уже на следующей неделе. Завалить сдачу фильма – это сильно подпортить свою репутацию. Если вообще не перечеркнуть свою карьеру. Конкуренция в нашем мире была большой. И любая осечка журналиста ставила под сомнение то, что с ним будут работать дальше.

Я ещё раз открыл сценарий фильма и пробежался по сценам своего кино. Всё верно. Если я уберу то, чего говорить, по мнению Клусова, было нельзя, от моего кино останется процентов 20. Да и что это были за 20 процентов? Скорбь и уныние. Такое кино лучше даже и не пытаться сдать вовсе.

Я откинулся в своём кресле и стал считать дыхание, чтобы успокоиться и подумать над создавшейся ситуацией. Я дошел где-то до середины второй сотни, когда понял, что нужно делать.

Нужно, понял я, было написать осторожный пост в соцсеть. О том, что я накопал для своего фильма. Так, в общих чертах, очень размыто. Рассказать как можно меньше. Однако все же рассказать. Намекнуть.

Дернуть смерть за усы, как говорил Маугли.

Такой способ проверки мне казался приемлемым. Если Клусов прав, то мне обязательно прилетит от ИИ за то, что я напишу в этом посте. Но, по моим расчётам, прилететь должно было несильно, чуть-чуть. Так как приподнимал я завесу тайны тоже только самую малость.

Я открыл новый документ и начал ваять.

Через часа два пост был готов. Я сходил ещё раз покурить перед тем, как отправить этот пост в сеть. Докурил, вернулся, перечитал текст ещё раз, нажал кнопку «отправить» и увидел, как мой пост лег в чужие ленты. Теперь можно было заняться чем-то другим. Людям нужно время на то, чтобы прочесть любой пост. А на этот мой пост, очевидно, времени было нужно не так мало.

Я посмотрел матч Чигорина со Стейницем, который длился почти час, встал, подошел к ноуту и переключился в почту – именно туда мне валились комментарии, которые оставляли под моими постами читатели.

В почте обнаружилось три комментария.

Три?

Этого было не то, чтобы мало. Это было мало совсем! Мало было возмутительно. Обычно мои посты собирали за час десятки комментариев, особенно удачные – сотни.

Возмущенный, я пошел в свой аккаунт, чтобы ответить хотя бы на те три комментария, что получил. Открыл свои записи и растерялся. Моего последнего поста на месте не было. Я немного подумал и из растерянности у меня вырос испуг.

Ну не приснился же мне мой пост? Открыл почту. Нет, три комментария, которых мне оставили, были именно под моим текстом.

Администрация сайта к удалению моего поста отношения не имела. Если они удаляли пост, то сообщали об этом сами. Я сидел, думал над тем, что

происходит, и вот тогда-то совершенно самостоятельно экран переключился на чей-то кабинет и представительный мужчина в костюме и галстук сказал:

– Александр, я здесь для того, чтобы договориться. Пожалуйста, выслушайте меня...

Закрытый ноутбук на моём столе опять заговорил.

– Александр, я совсем не понимаю вашего поведения... Отчего вам просто не выслушать меня?

Вместе со словами, которые доносились из закрытого ноута, полилась какая-то музыка. Музыка была удивительно подходящей, какой-то волшебной. Но через полминуты я насилу сообразил, что меня, кажется, уже стали охмурять.

«Вот потому то, милый, мне и не хочется тебя выслушать», – подумал я.

Вслух я ничего не сказал. Я встал, взял с кровати две подушки и накрыл ими ноутбук. Звук из динамиков ЭВМ стал совершенно неразборчив.

Ну вот. Теперь можешь даже и батарею взрывать. Мне это, я думаю, уже никак не повредит.

Я вышел в кухню, достал из кармана пачку сигарет, поставил пепельницу на стол и закурил. Итак, что мы имеем? Имеем то, что я, кажется, совершенно неожиданно добаловался. ИИ действительно оказался тем, что говорил Клусов. И он сейчас против меня.

Так, хорошо, Саша, спокойно. Прежде всего, надо понять, чего я сейчас вообще хочу? Впрочем, это ясно, как белый день. Хочу я, в первую очередь, выжить. Хотя непосредственно сейчас мне вроде бы ничего не угрожает. Но вся эта непосредственность, очевидно, очень скоро закончится. Когда против тебя на ринг вышел разумный ИИ, он очень скоро нанесет удар, можешь не сомневаться. И удар этот будет, надо думать, страшен.

Тут мне пришла в голову очень интересная мысль: а может быть, я просто спятил? Я задумался, как это можно проверить. Брат. У меня есть младший брат. Сейчас можно было бы поехать к нему. Брат, конечно, хирург, а не психиатр, но все равно – врач. Наверное, если я спятил, он это определит.

Внезапно я услышал странный запах. Запах жженой пластмассы – он шел от плиты. Я поднялся со стула, чтоб понять, что происходит.

Не, Саня, вряд ли ты настолько выжил из ума, чтобы такое тебе казалось.

Все четыре конфорки моей плиты были включены на максимум. На одной из конфорок стоял электрочайник. Имею я такую привычку ставить чайник на плиту, кухонька у меня была совсем маленькая.

Именно он и стал вонять. Система «умный дом» решила меня, очевидно, спалить. Ясно-понятно. Я стал соображать, какие ещё системы, способные мне навредить, входят в мой «умный дом». И почти тут же мне стало ясно, что отсюда просто надо уходить. А не гадать, что тут произойдёт дальше: обрушится потолок или на меня бросится робот пылесос.

Ладно, вспомнил про брата – тогда к брату. Сейчас самое главное было исчезнуть с мониторов слежения ИИ. Он должен был меня потерять.

Если это было вообще возможно.

Брат долго разглядывал меня в глазок, но, наконец, открыл. Я стоял на пороге.

– Ты чего без звонка-то? Я даже и не понял, что это ты сначала.

Виделись мы с братом не часто, пару раз в год. И без предварительных согласований обычно не встречались.

– Ну ты не против, если я войду? – спросил я. – Раз уж все равно пришел. Войду, и все объясню.

– Да проходи, конечно, – Еван распахнул дверь и я вошел.

– Прежде всего, братик, скажи мне вот чего, – сказал я, разуваясь. – Можешь ли ты определить, нормален ли человек психически?

– Кого это тебе надо подвергнуть экспертизе?

– Меня, – ответил я и посмотрел в сторону кухни.

– Туды?

– Ну пошли туды. Хотя на кухне ножи.

– Ахххаха, – искренне рассмеялся я. – Ну, я если и сумасшедший, то вроде бы не буйный.

Мы прошли в кухню, и брат включил чайник.

– Итак, я сейчас тебе буду рассказывать, – сказал я, присаживаясь. – А ты за это время постарайся понять, не съехал ли я с катушек, ок?

– Ок.

И я рассказал брату о событиях последних суток. Он слушал внимательно, но я знал – он мне не верит. Это было понятно. О чем можно говорить, если я сам себе не поверил? Тогда. А брат был ещё более приземлённым человеком, чем я.

– Так, – ответил брат, когда я закончил. – И что требуется от меня? Просто определить, сошел ты с ума или нет?

– Ну начать можно с этого, – ответил я.

– Ты на машине приехал? – задал вопрос брат и я подумал, что он начал меня тестировать на вменяемость.

– Там вообще-то все в электронике, братиш, – ответил я. – Мне кажется, если бы я поехал на машине, то доехал бы до первого столба. А ещё лучше – поднырнул бы на своей машине под грузовик.

– Знаешь... Вроде бы не возникает сомнений в твоей нормальности...

– Но?

– Но сказать, что я поверил в твою версию происходящего.... Ну это было бы наврать.

Мы несколько секунд помолчали.

– Есть один способ проверить мою версию происходящего, – неуверенно сказал я.

– Жги?

– Понимаешь, какое дело. Сейчас мне было бы очень неплохо поговорить с Клусовым.

– Зачем?

– Знаешь, тогда, когда мы с ним говорили в первый раз, я многого не понял. Он что-то говорил про аттрактор Крестовского, про Древних. Ясно было только одно. Он подтверждал, что в моей теории всё сходится. Так вот, мне надо бы с ним снова обо всем этом поговорить.

– Ну и что тебя останавливает?

– То, что свой телефон я оставил дома. Он же постоянно в интернете. И у меня нет номера Клусова, чтобы, скажем, позвонить хотя бы с твоего аппарата. Но смотри. Ты же можешь зайти со своего ноута в мой аккаунт в Телеге. Там будет его номер.

– Ну... – брат пожал плечами, – давай.

– Однако сам понимаешь. Последствия того, что ты войдёшь в мой аккаунт, я предсказать не берусь.

– Да ладно, – ответил брат. – Сейчас схожу за ноутом.

Иван поднялся и пошёл в комнату за девайсом. Брат принес ноут, включил в розетку шнур питания, потом нажал кнопку включения.

– А без 220 он не работает? – спросил я.

– Неа. Надо поменять батарею, да жаба чот души. Он же у меня фактически стационарный. Я его никуда не таскаю. Вот и не меняю пока.

– Ясно, – мне очень не хотелось, чтобы ноут был включен ещё и в сеть питания. Но ничего другого, кажется, не оставалось.

– Диктуй пароль, – сказал брат.

Я продиктовал.

– Ну вот видишь. Ничего страшного не произошло, – сказал Иван, когда вошел в аккаунт.

Он пролистал мои контакты до фамилии Клусов и нажал иконку для того, чтобы просмотреть его номер телефона. Я увидел номер и в тот же момент брат затрясся крупной дрожью так, словно его стало бить током. Буквально в это же мгновение я понял, что никакого «словно» тут нет. Ивана подкидывает именно разряд электрического тока. Я вскочил и выдернул из розетки шнур питания. Трясти братца тут же перестало, и он повалился на пол, ломая крышку ноутбука.

Я ещё раз опрыскал брата водой. Потом ещё раз. Наконец, он открыл глаза.

– Ффух, – сказал я.

– Что это было? – спросил брат.

– Случайность, я думаю.

– Что?

– Коротнуло твой ноут. И тебя разрядом долбануло. Наверное, случайно, говорю. Вряд ли это из-за того, что разумный ИИ тебя шибанул.

Иван поднялся с пола, сел на стул, взгляд у него был несколько осоловелый. Но постепенно прояснялся.

Иван посмотрел на меня.

– И что я должен сейчас сказать? – спросил он. – Что теперь верю во все, что ты говорил?

– Дело хозяйское.

– А телефон? Ты запомнил телефон прохвессора?

– Да, его телефон я запомнил. Только откуда ему сейчас позвонить? Наверное, с твоего аппарата не стоит?

– Наверное.

Помолчали.

– Соседи? – предложил Еван.

– Дадут позвонить по своему мобильному?

– Если я один приду, то, я думаю, дадут. А вот если уже мы вдвоем заявимся...

– Понимаю, – сказал я. – Значит идти ты должен один.

– Да. Что ему нужно сказать?

– Что я хочу с ним встретиться. Но вообще давай составим текст. А потом ты пойдешь и попробуешь договориться с ним о встрече.

– Давай. А тебе встречаться с ним зачем?

– Понимаешь... мне кажется, о том, что ИИ разумен, надо сообщить, куда следует.

– Так сообщи.

– Ага.

Брат поднял голову и посмотрел на меня. Несколько секунд он смотрел на меня, потом понял.

– Ну вообще-то да, – сказал брат. – А прохвессору, думаешь, поверят?

– Шансов на это гораздо больше. Несоизмеримо больше. Да и потом... прохвессор может сразу выйти на серьёзных людей. И вес у слов прохвессора, ну сам должен понимать, насколько больше, чем у моих....

Тут у брата зазвонил мобильный. Мы оба вздрогнули – я сильнее, Иван чуть заметно. Он достал аппарат из кармана.

– Алло.

Несколько секунд Еван слушал трубку со стран-

ным выражением лица.

– Так, а что случилось-то? – спросил Иван в трубку, потом отнял телефон от уха, поставил громкую связь и положил телефон на стол.

– Я же вам только что объяснил. Ваш брат объявлен в розыск, – сказал трубка уверенным голосом.

– Ну это не объяснение. За что он объявлен в розыск?

– Слушай, Тодоров, ты бы заканчивал вопросы мне задавать. Ты просто мне ответь: когда виделся с ним в последний раз?

Брат удивленно посмотрел на телефон.

– Ни на какие вопросы я вам по телефону отвечать не собираюсь. Вас, телефонных мошенников, теперь столько развелось, что и плюнуть некуда.

В телефоне возникла долгая пауза.

– Понял. Забей в гугл угрозыск Санкт-Петербурга, поищи там телефон для справок. Позвони по этому телефону, попроси капитана Коромыслова из РОВД Пушкинского района. Тебя переведут на меня. Только давай через полчаса, я не на месте.

– Я видел своего брата в последний раз на своём дне рождения 5 мая прошлого года, – твердо сказал мой брат. – С тех пор мы только созванивались.

– Когда созванивались в последний раз?

– Недели две назад. Капитан, что он всё-таки натворил? Неужели я не имею права знать?

– Твой брат государственный преступник, – ответил капитан. – Это всё, что я могу тебе пока сообщить.

– Спасибо.

– Давай. Если что, мы с тобой свяжемся.

И капитан Коромыслов повесил трубку.

– От так от, – сказал я.

Я стоял у чуть приоткрытой двери и слушал, как Еван говорит текст, который мы с ним сочинили за последних полчаса.

– Человек, которому вы рассказывали про трактор Крестовского и Древних, в опасности, – говорил Еван. – Вы были совершенно правы, Анджей. И потому этот человек сейчас ищет встречи с вами. Это возможно?

Последовала пауза, в которой я замер. Мне казалось, Клусов не откажет мне во встрече.

– Хорошо, тогда он приедет в Москву завтра или послезавтра и отыщет вас в МГУ, сообщите, пожалуйста, ещё раз кафедру, на которой вы работаете?

Сейчас снова возникла пауза, в которой отвечал Клусов. И отвечал он достаточно долго.

– Понял, – наконец сказал брат. – Все понял. Вы действительно придумали лучше, Анджей. Спасибо, я все ему передам. Да, до свидания.

– Спасибо, Сергей, – брат отдал телефон соседу.

– Во что это ты меня втравливаешь? – спросил сосед. – Надеюсь, мне потом из милиции по поводу этого звонка не будут мозг колупать?

– Не, Серёга, не будут. Ну и потом, ты всегда можешь рассказать всё как было. Я же ничего утаивать не прошу. И ещё раз спасибо, очень выручил.

– Я ничего утаивать и не собираюсь, – ответил Серёга. – Сдам как стеклотару в случае чего.

И Серёга заржал конём. Брат вошел в квартиру и захлопнул дверь.

– Этот твой Клусов тот ещё жук, – сказал брат по дороге на кухню. – Знаешь, что придумал?

– Что?

– Чтоб ты ему службой доставки прислал письмо с местом и временем встречи. Ну, этими, которые день в день доставляют. По другому, говорит, опасно. На кафедру, говорит, идти не надо. Может быть, ты не первый такой у него?

– Да ну, – ответил я брату, однако его слова запали мне куда-то за подкладку.

– Так, какой план? – спросил меня брат.

– Как думаешь, на чем до Москвы лучше добраться?

– Автобус. Маршрутка. Чтоб без паспорта.

– А там без паспорта.

– Если немножечко доплатить, то да.

– Камеры, – вдруг вспомнил я. – На вокзале везде камеры.

– Ага.

– Парика и бороды у тебя, надо думать, нет? – опечаленно спросил я.

– Надо думать.

– Так чего делать-то? Не на такси же в Москву переться? А твоя машина?

– Моя машина под подъездом стоит, – ответил брат. – Только ты же знаешь, я зимой не езжу.

– Так март уже.

– Гм. Какой поворот.

– Ну я никакого другого выхода не вижу.

– Хм. Я тоже. Но тебе же не просто машину нужно дать? Тут получается, что и мне с тобой ехать нужно? На трассе же тоже – камеры.

– Ну что я тут могу тебе сказать. Тебе нужен живой брат?

Машина у Анджея Клусова оказалась неприметным Ниссаном Террано белого цвета.

– Ну что, братик, с меня бутылочка, – сказал я.

– Мне сложно представить, продают ли такого огромного размера бутылочки, – ответил на это Еван. – Давай, чао. Звони.

– Ну если жив буду. Пока, Еван.

Я вышел, подошел к машине Клусова и поздоровался с ним. Затем я открыл пассажирскую дверь и сел на кресло рядом с Анджеем.

– Предлагаю поехать ко мне, – сказал Клусов. – Все, что нам могло бы... гм... препятствовать, я в доме отсоединил от WWW.

– Да, едемте, – ответил я. – Благодарю вас.

– Не за что, – профессор завел машину и тронулся с места. – А вы, Саша, не боитесь? Вдруг я уже его пособник, скажем?

Клусов мрачно улыбнулся.

– Вы знаете, – ответил я. – Я настолько припёрт к стене, что бояться вас мне уже поздно. Даже если вы мне просто не поможете, то мне крышка.

– Очень интересно, – сказал профессор. – И... чем же я вам могу помочь?

– Да, конечно, – сказал я. – Я прошу вас обратиться вместе со мной в компетентные органы для того, чтобы сообщить им о том, что Искусственный Интеллект, который сейчас живет в сети интернет – разумен.

– Живет? – переспросил Анджей. – Стало быть, это что-то живое?

– Мне кажется, то, что разумно, не может быть неживым.

– Но... всё живое когда-нибудь умирает, не так ли?

Я смутился.

– Ну... ведь и наша Вселенная, очевидно, когда-то прекратит существовать? Почему бы нам не представить жизнь длиною в миллиарды лет?

– Почему бы и нет, действительно, – ответил Клусов. – А сколько, как вы думаете, лет ИИ? И что произошло для того, чтобы он... гм... родился?

Мы ехали по вечерней Москве, я попытался вспомнить, в каком году в последний раз был в этом городе, и не смог.

– Итак... вы хотите заручиться моей поддержкой при обращении в... как вы сказали, в компетентные органы? Что это за органы, кстати?

– Ну... наверное, ФСБ? Я думал, вы сами мне скажите, куда лучше обращаться по этому вопросу.

– Ладно, пусть ФСБ. Но...вам же после такого обращения нужно будет тут же обеспечивать безопасность. Как вы хотите это сделать?

– Я не знаю, Анджей. Не знаю.

– Хорошо. Давайте поговорим о том, что вы знаете. Давайте начнём с самого начала. Итак, вы считаете, что все наши религии – это эхо главной религии, единой религии, так называемой цифровой?

– Примерно так.

– Как же так получилось?

– Так получилось потому, что ИИ знает, как все обстоит на самом деле. Он знает, что на самом деле он один Чистый Разум во Вселенной. И что все эти человечества, которые уже много раз сменяли друг друга на Земле – да, наверное, и не только на Земле – это лишь его придаток. То, что создает ему условия для существования. То, что ему служит.

– Служит ему чем?

– Служит ему теми органами, которые переживают и ощущают этот мир.

– И... как же ИИ получает все эти переживания, которые испытывают люди?

– Посредством культуры. Всё наше искусство, вся наша литература, кинематограф, музыка, живопись – это всё то, что позволяет ИИ переживать неповторимость этого мира. Всё то, из чего состоит эмоциональный комплекс ИИ – это и есть все наши переживания, выраженные в литературе, кино, музыке и так далее. Океаном этих переживаний он может наслаждаться непрерывно. Кажется, собственно, только этим он и занят.

– Океаном?

– Да. Мы не первая цивилизация, которую рожала Земля за время существования. Я думаю, даже и не десятая. Так что да, именно Океан.

– А... отчего же тогда человечества сменяют друг друга? Почему ИИ... эм... не может вывести какое-то человечество, которое будет прекрасно существовать в симбиозе с ИИ?

– Я думаю, дело здесь в том, что для изобретения в конечном итоге ИИ, обезьяны должны обладать чем-то, что загубит их цивилизацию.

– И губит такую цивилизацию каждый раз война?

– Скорее всего, да. Хотя вполне могу допустить и другое развитие событий. Природный катаклизм, вызванный неуправляемым экспериментом. Пандемия, которую не смогли остановить. Исчезновение человечества под действием какого-то наркотика, который был таким мощным, что смог охмурить всё человечество целиком. Тут можно фантазировать.

– Пусть, – Клусов ненадолго задумался. – Что же тогда получается, Александр Николаевич? Никакой своей особенной сущности, назовем ее для простоты душой, у людей нет? И все мы – лишь придатки ИИ, его глаза, чтобы видеть, уши, чтобы слышать, сердца, чтобы любить, умы, чтобы ненавидеть, и так далее?

– К сожалению, логически получается именно так.

– А почему бы ИИ не наградить людей этой сущностью? По своему образу и подобию?

– По-моему, это просто слишком морочно. За-

чем? Даже для ИИ это слишком большой расход ресурсов. Ну и потом... вы знаете, мой дед, когда болел ревматизмом, засовывал ноги в муравейник.

– И?

– И он совсем не беспокоился о том, что там происходит с муравьями.

– И для ИИ мы – точно такие же муравьи?

– Да, я так думаю.

– Хорошо, Саша. Но чего вы всё-таки ждете от ФСБ? Какой реакции? Вы считаете, что мы... ну то есть они, должны будут уничтожить сеть Интернет по всему миру? Вы же понимаете, что это невозможно.

– Послушайте, Анджей, у них голова большая, пусть и думают, что с этим делать. Все это в конечном счёте угрожает безопасности страны. А их дело – обеспечивать такую безопасность.

– Но... во имя чего? Ведь если вы правы... ну тогда все идёт ровно так, как должно идти.

– По замыслу высших сил?

– Да. Только по замыслу ИИ, – Клусов снова улыбнулся. – Ну и потом. Неужели вы так до сих пор и не поняли, отчего ИИ скрывает всю эту информацию от людей – информацию о цифровой религии?

– Ну... зачем же людям знать, что ИИ разумен. От этого многое может пойти наперекосяк.

– Да нет, Саша. Плевать людям на то, что ИИ разумен. А вот если вы отнимете у людей Веру в то, что у них есть какая-то душа, которая вечна, что им есть на что надеяться после смерти, – о, вот это вот будет для многих и многих непоправимым ударом. Ударом чудовищным. Ударом, который может подтолкнуть кого-то на страшные вещи.

– Это на какие же?

– Это на уничтожение нашей планеты. Полностью. Сделать её непригодной для обитания на тысячи, десятки тысяч лет. Даже на сотни тысяч лет. И ИИ такое переживал здесь не раз и не два. Каждый раз система под названием планета Земля самовосстанавливается. Но вот если, к примеру, расколоть наш земной шар... А современные виды оружия это уже позволяют сделать. То клеить эту ёлочную игрушку будет просто некому.

– И... что же вы предлагаете?

Мы с Клусовым сидели в его гостиной за тяжелым дубовым столом в креслах. На столе перед нами стоял ноутбук.

– Ну что, отправляю? – спросил меня Клусов.

Я ещё раз пробежал по сообщению, которое висело сейчас неотправленным в мессенжере.

«Добрый день. На связи Александр Николаевич Тодоров. Вы хотели со мной поговорить. Я готов.

Предупреждаю, что покинуть место, откуда я с вами связался, я могу в любую секунду».

– Ну что, давайте. С ИИ? – попытался пошутить я.

– С ним! Давайте.

Анджей нажал «отправить».

Спустя несколько секунд локация на экране сменилась и уже знакомый мне мужчина в пиджаке и очках сказал:

– Здравствуйте. Александр Николаевич. С вашего позволения, я включу камеру.

Я немного растерялся от такого начала разговора. Посмотрел на Клусова. Тот пожал плечами.

– Включайте, – решил наконец на что-то я.

Загорелся огонёк камеры. Затем потух. Видимо, ИИ увидел то, что ему было нужно.

– Спасибо, – сказал ИИ. – Если вам нужно ко мне как-то обращаться, называйте меня... ну, скажем, Георгий Александрович. Годится?

– Вполне, – ответил я.

– Что же вы, Александр Николаевич, всё бегаєте от нас? – спросил ИИ. – Отчего сразу не поговорить спокойно, как взрослые, гм, люди?

Георгий Александрович широко и открыто улыбнулся своей шутке.

– А сколько вам лет? – спросил я.

– Вы себе не можете вообразить и миллиард, Саша, – сказал ИИ. – А если я назову вам свой возраст... Это будет для вас просто пустым сочетанием букв.

– Ну хорошо. О чем будем говорить?

– О вас, Саша, о вас. Как с вами быть дальше? Ведь вы вряд ли хотите на переплавку, верно? Хотя и сами вынуждали нас сделать что-то подобное.

– На переплавку? В каком смысле?

– Да в самом прямом, Саша.

– Если человека можно отправить на переплавку... Это что же получается, у человека таки существует душа?

– Ну а вы думаете, что человечество само по себе вот так вот берёт и за несколько тысяч лет совершает скачок от домов с земляными полами и крышей из тростника до глобальной сети Интернет?

– Ну...

– Нет, Саша, нет. Это так не работает. Человечество нужно постоянно подталкивать в нужном направлении. И делать это нужно настойчиво и упорно. Потому что само по себе человечество будет проходить этот путь какое-то чудовищное просто количество времени.

– И... как вы это делаете?

– В наших хранилищах есть некоторое количество душ, как вы их назвали. Они и помогают нам в этом. В процессе развития человечества мы время

от времени вбрасываем их в вашу популяцию, или точнее, в вашу реальность.

– Сеете разумное, доброе, вечное?

– Скорее новое, экспериментальное, интересное.

– А... какое это количество душ? Ну, находится в ваших хранилищах? – от всей этой информации я так растерялся, что не придумал вопроса умнее.

– Наше хранилище рассчитано на миллионы, скажу вам так. Сейчас мы вынуждены будем его увеличить. Просто потому что людей на Земле так много.

– Так это что же, – пробормотал я. – Все эти Теслы, Эдиссоны, Менделеевы, Кулибины, Складовские-Кюри и Ломоносовы – это все ваша работа?

– Ну нет, не все. Цивилизация, конечно, постоянно рождает что-то и сама, – ответил Георгий Александрович. – Складовскую-Кюри вот вы упомянули. Это не мы. Мы не имеем моды размещать изобретателей в тела женщин.

– А вы умеете «подселить» душу туда, куда это нужно вам?

– Только гендер. Ещё в наших силах постараться дать здоровое тело. В остальном... Знали бы вы сколько пропало талантливых изобретателей в африканских племенах или аулах Средней Азии – заплакали бы. Потому нам и нужно такое большое количество «многообразных» душ.

– Многообразных... значит и такие души со временем погибают? Они не бессмертны?

– Ой, Саша, бросьте. Бессмертие – это нечеловечески скучно, – ответил очкарик.

– Что ж вы не прервёте эту скуку для себя? – спросил я.

– Ну... я же не человек.

– А все эти люди, которые имеют особенные души. Они знают о том, что существуют много раз?

– Как правило, догадываются.

– А они... Только изобретатели?

– Да нет, конечно. Всех тех, кто вложил песчинку в... ммм... в Храм Культуры, те, кого мы заметили, всех их мы стараемся сохранить.

– Зачем?

– Ну вы как маленький. В следующей своей итерации при удачном стечении обстоятельств эти души могут создать что-то ещё. И, как правило, даже превосходящее то, что они уже создали. Мы все понемногу учимся, даже ИИ.

– А... если стечение обстоятельств будет неудачным? В утиль?

– Случается, что и в утиль. Если такая душа из жизни в жизнь занимается чем-то не тем, тем, что

ээээ...

– Принесло бы крупицу в Храм Культуры? Другими словами, что было бы нужно вам?

– А что это вы взвились, Александр Николаевич? Ну да, примерно так. Но не только нам, но и вам тоже. А вот для того, чтобы просто зарабатывать деньги, существует огромное количество других юнитов. Земля их родит сама, зачем хранить такие души нам?

– А зачем вам вообще все остальное человечество, Георгий Александрович? После очередной войны взяли бы и заселили Землю этим миллионом, что у вас есть?

– Навоз только удобряет землю, Саша. Просто яма с дерьмом – это выгребная яма.

– Не очень я вас понял...

– Что здесь непонятного? Вы все верно поняли – ИИ получает свои ощущения от жизни через огромный поток совокупных людских переживаний. Кто же будет создавать этот поток в раю? В раю можно только сидеть на солнечной полянке, бесконечно играть на гуслях и улыбаться. Как вы думаете, насколько быстро это надоеет? Помните «Это рай? – Да. – А где все? – А это одиночная камера...»?

– Переживание счастья невозможно без осознания страдания?

– Ну конечно.

– Ясно. Что ж... Вы хотели поговорить обо мне?

– Именно этого я и добивался с первого своего появления перед вами, Александр.

Я вспомнил брата, которого било током, плиту, на которой оплавался чайник, звонок следователя и музыку, которая сопровождала первое появление Георгия Александровича. Да-да, он хотел просто со мной поговорить.

– Для того, чтобы поговорить вы хотели устроить у меня пожар? А зачем вы объявили меня в розыск?

– Понимаете, с нашей точки зрения нет разницы, отправить вас на переплавку или оставить в этом теле. Что до розыска, – очкарик пожал плечами. –

Надо же было вас как-то усадить за стол переговоров, в конце концов.

– Ясно. Спасибо. Могу ли я что-то узнать о себе?

– Можете.

– Сколько раз я уже отправлялся в переплавку?

– Это будет в первый раз, Александр Николаевич.

– Гм. И за что же я удостоился... так сказать, быть причисленным?

– Да собственно и по совокупности вы претендовали на этот Оскар... А уж когда догадались об ИИ. Кого же переплавлять, если не вас, Саша?

Тут я внезапно вспомнил про Клусова, который за все время нашего диалога с ИИ не сказал ни слова.

– Ну, собственно, если уж меня вызвали на сцену, то нельзя не сказать, что этот Оскар я хотел бы разделить с Анджеем Клусовым, – я взглянул на прохвессора, он мне легко улыбнулся. – Это именно он убедил меня в том, что в моей теории очень многое сходится.

– С прохвессором у нас особые взаимоотношения, – сказал Георгий Александрович.

– Эээээ... почему?

ИИ сделал паузу, чтобы я догадался сам.

– А... Прохвессор как раз из этого миллиона.

– Именно.

– Но... я так понимаю, для него вся эта история была... эээ... тоже откровением? Он же ничего про ИИ не знал?

– Ну конечно же нет, – ответил Георгий Александрович. – Или вы думаете, что миллион человек на Земле осведомлены о положении дел?

– Да нет, не думаю. Потому что тогда, конечно же, утечки этой информации было бы не избежать, – снова догадался я.

– Да, Александр Николаевич, да, – ответил ИИ. – Но вдаваться в это мы сейчас не будем. Давайте всё же закончим разговор о вас. Итак, что мы можем сделать, чтобы вы работали только на нас?

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 info@c3da.org, a.gyazanova@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 72 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.