ISSN 2686-9373

ВЕСТНИК СОВРЕМЕННЫХ ЦИФРОВЫХ ТЕХНОЛОГИЙ

13. 2022 (ДЕКАБРЬ)

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

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.

№13

ДЕКАБРЬ 2022

ISSN 2686-9373

www.c3da.org

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

РГСУ

Подписано в печать 28.12.2022 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

© Журнал Вестник современных цифровых технологий

РЕДАКЦИОННЫЙ СОВЕТ

Главный редактор – Щербаков Андрей Юрьевич, доктор технических наук, профессор, главный научный сотрудник РАН (ИТМиВТ им. С.А. Лебедева), 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, кандидат исторических наук, 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.

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.

СОДЕРЖАНИЕ

Редакционное примечание 3

1. ПРАКТИЧЕСКИЕ АСПЕКТЫ ЦИФРОВЫХ ТЕХНОЛОГИЙ

Д.Ф.Алиев, А.Ю.Щербаков – О практических подходах к созданию доверенных защищенных цифровых платформ
D.F. Aliev, A.Yu. Shcherbakov – On practical approaches to creating trusted secure digital platforms 4

2. ЦИФРОВЫЕ ТЕХНОЛОГИИ В ОБРАЗОВАНИИ

С.В. Запечников – Учебно-методическое обеспечение дисциплины «Прикладная криптография»
S.V. Zapechnikov – A curriculum of applied cryptography course 13

3. ЦИФРОВЫЕ ТЕХНОЛОГИИ В БИОЛОГИИ И МЕДИЦИНЕ

П.А.Кожевин – Природоведческая микробиология в эпоху цифровизации
P.A. Kozhevin – Microbial ecology in the digital age 20

4. ЦИФРОВЫЕ ТЕХНОЛОГИИ В ПРОМЫШЛЕННОСТИ

В.Ю. Шевцов, Д.И. Правиков – Применение сетей Петри при моделировании атак на системы АСУ ТП
V.Yu. Shevtsov, D.I. Pravikov – The application of Petri nets for modeling attacks on ICS 32

5. ВОПРОСЫ МЕТОДОЛОГИИ И ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

А.А. Рязанова – Исследования и разработки в области искусственного интеллекта: достижения, выводы, перспективы
A.A. Ryazanova – Research and development in the field of artificial intelligence: achievements, conclusions, prospects 38

6. ЛИТЕРАТУРА О ЦИФРОВЫХ ТЕХНОЛОГИЯХ

Егор Федоров – Homo digital 47

РЕДАКЦИОННОЕ ПРИМЕЧАНИЕ

Редакционный Совет поздравляет читателей и авторов журнала с наступающим Новым годом и желает всем крепкого здоровья, душевной гармонии и творческих успехов!

Прошедший год был непростым для науки и образования, и, тем не менее, мы достигли в нем больших успехов – наш журнал получил статус ВАКовского и стал выходить под эгидой Российского государственного социального университета. Несмотря на трудности, мы выпустили все намеченные номера журнала и опубликовали все запланированные материалы. Уверены, что наступающий год принесет успех нам и нашим читателям!

Новогодний номер включает весьма интересные материалы, в первую очередь отметим статью **«О практических подходах к созданию доверенных защищенных цифровых платформ»** Джомарта Алиева и Андрея Щербакова, опубликованную в разделе «Практические аспекты цифровых технологий». Эта работа посвящена рассмотрению вопросов реализации защищенной доверенной платформы достоверного обмена документами и хранения их в распределенном реестре на основе отечественных стандартов и с использованием отечественных криптографических алгоритмов. Авторы приводят практический пример реализации распределенного реестра и смарт-контрактов на основе зеро-кодинга – использования встроенных механизмов платформы.

Раздел «Цифровые технологии в образовании» включает статью Сергея Запечникова **«Учебно-методическое обеспечение дисциплины «Прикладная криптография»**. В статье представлен новый курс «Прикладная криптография», разработанный автором для обучающихся по магистерской программе «Безопасность данных и криптография» в соответствии с актуальным мировым уровнем знаний в области криптографии. Курс может служить базой для дальнейшей разработки спецкурсов по отдельным областям современной криптографии. Полагаем, что данный материал будет весьма полезен в педагогической практике преподавателей ВУЗов.

В разделе «Цифровые технологии в биологии и медицине» вниманию читателей предлагается статья **«Природоведческая микробиология в эпоху цифровизации»** Петра Александровича Кожевина – доктора биологических наук, профессора, академика Российской Экологической Академии, профессора кафедры биологии почв МГУ. Эта работа дает нам уникальную возможность ознакомиться с новой парадигмой современной микробиологии, формирующейся под влиянием молекулярно-генетических методов и цифровизации. Научная деятельность Петра Александровича посвящена изучению «микроорганизма и его естественной среды обитания», телеономичности микробных систем с механизмами “тонкой настройки“, он является автором более 250 статей, монографий, учебников для университетов и патентов.

В статье **«Применение сетей Петри при моделировании атак на системы АСУ ТП»** Вадима Шевцова и Дмитрия Правикова, публикуемой в разделе «Цифровые технологии в промышленности», рассмотрен метод моделирования атак на системы АСУ ТП на базе расширенного аппарата сетей Петри, позволяющий подробно описать процесс объекта автоматизации – нефтеперекачивающей станции (НПС). Описана типовая схема управления НПС, сценарии ее работы в случае различных атак злоумышленника.

Раздел «Вопросы методологии и технологий искусственного интеллекта» включает статью Алины Рязановой **«Исследования и разработки в области искусственного интеллекта: достижения, выводы, перспективы»**, посвященную изучению вопросов развития, достигнутых результатов, актуальных тенденций в области искусственного интеллекта (ИИ). В работе представлена динамика показателей эффективности новых технологий ИИ в области распознавания изображений, обработки естественного языка, обучения с подкреплением, глубинных нейронных сетей. Рассмотрены этические аспекты развития и применения технологий искусственного интеллекта, вопросы финансирования проектов в области ИИ.

Наш тринадцатый, новогодний выпуск завершает рассказ Егора Федорова **«Homo digital»** о возможности появления нового вида человека и философском осознании его предназначения. В преддверии наступающего 2023 года автор делится своими мыслями об изменении смыслов существования человека с течением истории и в будущем времени.

УДК: 004.03, 004.72, 004.4'2

О практических подходах к созданию доверенных защищенных цифровых платформ

D.F. Aliev, A.Yu. Shcherbakov

On Practical Approaches to Creating Trusted Secure Digital Platforms

Abstract. *This article is devoted to the consideration of a secure trusted platform for reliable exchange of documents and their storage in a distributed registry with minimal borrowing of third-party software products, based on domestic standards and indicators of programming and information security quality, using domestic cryptographic algorithms. It is shown that within the framework of the platform it is possible and reasonable to implement smart contracts and chain code. The advantages of zero-coding as a way to create a minimum viable version of a platform product, understandable and verifiable for the purpose of further development of platform solutions, are considered.*

Keywords: *platform, trust, cryptographic information protection facility (CIPF), electronic signature (ES), zero-coding, distributed ledger (blockchain), script.*

Д.Ф.Алиев[1]
А.Ю.Щербаков[2]
[1]Доктор философии в области бизнес-права (PhD), доктор делового администрирования в области финансов (DBA), кандидат экономических наук, первый проректор Федерального государственного бюджетного образовательного учреждения высшего образования «Российский государственный социальный университет».
E-mail: kharchenkoDD@rgsu.net
[2]Доктор технических наук, профессор кафедры комплексной безопасности критически важных объектов РГУ нефти и газа (НИУ) имени И.М. Губкина, заведующий кафедрой когнитивно-аналитических и нейро-прикладных технологий РГСУ, ведущий научный сотрудник Государственного университета управления, главный научный сотрудник РАН (ИТМиВТ им.С.А.Лебедева).
E-mail: x509@ras.ru

Аннотация. *Статья посвящена рассмотрению вопросов реализации защищенной доверенной платформы достоверного обмена документами и хранения их в распределенном реестре при минимальном заимствовании программной продукции третьих фирм, на основе отечественных стандартов и показателей качества программирования и информационной безопасности, с использованием отечественных криптографических алгоритмов. Показано, что в рамках платформы возможна и целесообразна реализация смарт-контрактов и чейн-кода. Рассмотрены преимущества зерокодинга как способа создания минимально жизнеспособной версии платформенного продукта, понимаемого и верифицируемого в целях дальнейшей разработки платформенных решений.*

Ключевые слова: *платформа, доверенность, средство криптографической защиты (СКЗИ), электронная подпись (ЭП), нулевое программирование (зеро-кодинг), распределенный реестр (блокчейн), скрипт.*

ВВЕДЕНИЕ

В текущей геополитической ситуации крайне важным является курс на создание унифицированных программно-аппаратных платформ для обмена документами и их хранения, основанных на следующих принципах:

- полное владение исходным кодом платформы, минимальное использование продуктов третьих фирм,
- компактность кода, возможность его доработки и технической поддержки,
- опора на отечественные криптографические алгоритмы, проектирование и реализация СКЗИ сразу по требованиям регуляторов,
- минимальное использование внешних инфраструктурных решений (удостоверяющих центров) в целях повышения надежности и доступности платформ.

При этом весьма существенным требованием является доверенность [1], т.е. возможность верификации свойств платформы как программно-аппаратного проекта на всех этапах его жизненного цикла.

Доверенность включает минимальное заимствование программной продукции третьих фирм и опору на отечественные стандарты и показатели качества программирования и информационной безопасности, в первую очередь на отечественные криптографические алгоритмы.

С другой стороны, для повышения уровня доверия к разработке необходимо использование средств разработки и расширения функционала платформы таким образом, чтобы не нарушить базовые свойства платформ, такие как локальная

замкнутость на уровне субъектов [2]. Для этого целесообразно использовать механизмы вызова сценариев (скриптов), а также в случае использования архитектуры распределенного хранения или распределенного реестра – извлечение исполняемых модулей и скриптов, их содержащих, из доверенных хранилищ с проверкой их целостности.

Предлагаемая читателю статья посвящена практике создания программной части доверенных и защищенных цифровых платформ в соответствии с указанными принципами.

В качестве примера рассмотрим квалиметрическую платформу Сешат [3].

Напомним основные бизнес-процессы платформы.

ОСНОВНЫЕ ИНФОРМАЦИОННЫЕ ПРОЦЕССЫ (БИЗНЕС-ПРОЦЕССЫ) ПЛАТФОРМЫ

При установке и разворачивании платформы регистрируется как минимум один администратор системы. Один из администраторов (в случае присутствия нескольких) производит верификацию регистрирующихся пользователей и экспертов (администратор верификации).

1. Регистрация пользователей

Пользователь вводит свое имя, получает анонимное имя UserX, вырабатывает свой ключ в ключевом контейнере, защищенном паролем. Далее пользователь загружает в систему свои квалификационные документы (диплом об образовании, ученом звании и степени, список трудов, некоторые труды, которые он считает важными), после чего заполняет анкету, где указывает тематики, по которым он дает рецензии или проводит экспертизы (если он претендует на роль эксперта).

Администратор верификации производит верификацию загруженных документов и личных/профессиональных данных самого пользователя и завершает его регистрацию. Пользователь получает статус – одну или несколько ролей и перечень тематик, в которых он компетентен. Параметры пользователя отражены в его профиле.

2. Загрузка статей (документов)

Статьи загружаются в систему для рецензирования или депонирования (во втором случае рецензирование не требуется, фиксируется приоритет; объектами депонирования также являются статьи или работы с требованиями сохранения конфиденциальности).

При загрузке производится индексирование статьи и установление ее принадлежности к тематике.

Также предпринимаются меры по предотвращению загрузки статей которые уже есть в системе (например, путем сравнения с загруженными ранее статьями).

После успешной загрузки администратор рецензий направляет ее на рецензирование или депонирование.

Направление на рецензирование происходит тремя возможными способами: всем экспертам тематики, избранным экспертам тематики, желающим экспертам тематики. Этот выбор делается автором при загрузке и оплачивается внутренними токенами платформы. Соответственно, эксперт тематик выставляет в своем профиле параметр, желает ли он в текущее время участвовать в рецензировании.

При загрузке и поиске работает ядро семантического сервиса – процессы индексирования и сравнения текстов.

3. Рецензирование статей

Рецензент по публичной методике выставляет оценки статье и обосновывает их в виде рецензии, которую подписывает своей электронной подписью (ЭП).

Рецензии и оценки модерируются администратором рецензий (например, в целях дополнительной анонимизации эксперта для исключения выяснения его личности и вероятного давления на него).

Возможен режим без модерации, когда собираются оценки и рецензии не менее трех экспертов и автору направляется только усредненное мнение (оценка).

Весь документооборот на платформе выполняется в виде файловых операций между соответствующими директориями пользователей и статей.

4. Начисление токенов за рецензии и статистика

После формирования рецензии и оценки эксперты получают токены в соответствии с их рейтингом.

В случае если реальных токенов (начисленных авторами или спонсорами) не хватает для оплаты работы экспертов, начисленные токены маркируются как кредитные (вексель) и учитываются по мере появления реальных токенов в хронологической очередности оплаты услуг экспертов.

Все действия в системе регистрируются в журналах.

5. Работа внешних заказчиков

Внешний заказчик регистрируется отдельно и также проходит процедуру верификации как физическое или юридическое лицо. Он также является донором (поставщиком) токенов в систему.

Он имеет возможность знакомиться со статисти-

кой поступления статей, оценками за них, а также отдельно оплачивать процедуры развернутого поиска – когда его текстовый запрос сравнивается со статьями тематики с учетом заданного порога их рейтинга (средней экспертной оценки). Поиск может происходить и только по рейтингу статей.

К внешним заказчикам также относятся эксперты государственных учреждений и сервисов, которые обращаются за фактами приоритета или плагиата, различными характеристиками научных достижений авторов или экспертов.

РЕАЛИЗАЦИЯ БИЗНЕС-ПРОЦЕССОВ В МОДУЛЯХ ПЛАТФОРМЫ

Рассмотрим реализацию описанных бизнес-процессов в модулях платформы.

Регистрация пользователя, генерация сетевого имени и создание личного ключа для подписи

Модуль gk0 – генерация личного ключа.

Результатом работы является появление в системе пользователя с уникальным анонимным именем и его ключа. Ключ размещен в ключевом контейнере с именем, совпадающим с анонимным именем пользователя, и защищен паролем пользователя.

Модуль gks – отвечает за генерацию сетевого ключа.

Данный модуль обеспечивает связь пользователя с системой. В качестве корреспондента для информационного обмена должен быть указан пользователь, зарегистрированный как администратор, который обозначает систему приема статей или подключает рецензента, или внешнюю организацию.

В модуле формируется длинное сетевое имя, которое описывает связь между пользователем и системой и состоит из анонимного имени отправителя и получателя статей. Имя также помещается в файл Netname, который может быть использован модулем динамической генерации смарт-контрактов, который описан ниже.

Формируется ключ для передачи данных и их верификации для записи в блокчейн.

Модуль chpin

Меняет ключ доступа к контейнеру.

Модуль rsen

Выполняет подписание статьи и отправку ее в систему.

Модуль rrec

Производит прием статьи и проверку подписи под ней, при необходимости – экстракцию статьи из подписанного файла. Необходимость экстракции зависит от политики – статья помещается в реестр с подписью автора или только с подписью администратора системы.

Модуль areestr

Размещает статью в распределенном реестре.

При размещении статьи формируется квитанция, которая направляется автору и рецензентам.

В системе также реализованы модули извлечения из реестра с проверкой цепочки и модуль динамической генерации смарт-контракта.

Семантическая часть системы опирается на вызов модулей индексации и сравнения текстов, которые описаны в статье [4].

Работа платформы демонстрируется динамическим смарт-контрактом 1first.bat, который создает двух пользователей andrey и boss, затем все необходимые имена и ключи. Смарт-контракт также передает ключ в защищенном виде пользователю, меняет пароли контейнеров, подписывает статью и передает ее в систему, проверяет подпись под статьей, размещает ее в реестре и выдает пользователю квитанцию с приоритетом размещения.

Далее статья должна быть проиндексирована семантическим модулем, отнесена к некоторой тематике (сравнением индексированной статьи с шаблоном тематики), после чего автоматизированно или вручную (администратором) обработана для рецензирования (с экстракцией автора и списка литературы, по которой также можно опознать автора).

Приведем процесс разворачивания платформы в виде последовательного вызова модулей (скрипта).

```
rem First Demo SmartContract for creation one user Andrey and operator (Boss)
rem Create Main key
gk0 boss BossPas
rem Create Dir for Boss
md boss
rem Create Call for copy key to psv extanton file
mks a.bat [copy netname [*.psv
call a.bat
mks a.bat [copy [*.psv [boss\boss
call a.bat
pause
del *.psv
rem Create Andrey key
gk0 Andrey 1234
rem Create Dir for Andrey
md andrey
rem Create Call for copy key to psv extanton
mks a.bat [copy netname [*.psv
call a.bat
```

```
pause
mks a.bat [copy [*.psv [andrey\andrey
call a.bat
del *.psv
rem Create Call for Andrey Network key generation use passw1 method
mks a.bat [gks [Andrey [boss passw1
call a.bat
rem Create Call for copy key to psw extanton
mks a.bat [copy netnames [*.psw
call a.bat
rem Send psw to Boss and to Andrey dir
mks a.bat [copy [*.psw [andrey\*.*
call a.bat
mks a.bat [copy [*.psw [boss\*.*
call a.bat
del *.psw
rem Distribute ChangePin prog
copy chpin.exe andrey\*.*
copy chpin.exe boss\*.*
rem Distribute MakeSmart prog
copy mks.exe andrey\*.*
copy mks.exe boss\*.*
rem Distribute SendReestr prog
copy rsen.exe andrey\*.*
rem Distribute RecordReestr prog
copy rrec.exe boss\*.*
rem Distribute AddReestr prog
copy areestr.exe boss\*.*
rem Normalize psw files names
cd andrey
copy *.psw a2boss
mks a.bat [chpin [a2boss ..\passw1 [1234
call a.bat
pause
cd ..
cd boss
copy *.psw frandrey
mks a.bat [chpin [frandrey ..\passw1 [boss
call a.bat
pause
cd ..
rem Send Article file (c2.txt) to boss
copy c2.txt andrey\*.*
cd andrey
rem Sign Article file
rsen a2boss 1234 c2.txt c2.sen
rem Send Signed File to boss
copy c2.sen ..\boss\*.*
cd ..
cd boss
rem Check Article signature and extract it
rrec frandrey boss c2.sen-x
rem Add Article in Reestr and create notify file
areestr.exe boss BossPas c2.txt
rem Send notify file to andrey
copy *.kvt ..\andrey\*.*
pause
```

Интересно рассмотреть программу mks, которая динамически формирует строку в описанном выше файле.

```
int main(int argc, char *argv[])
  {
   int td[6];
   int i,j;
   char ss[16][130],itog[2048];

//  Current Time and Date
   GetTimeDate(td);
   AppLogT(LOGNAME,"Start Gks");
  if((argc<3)||(argc>12))
    {
        printf("Use format: mks file part1 part2 ... part10\n");
     AppLogT(LOGNAME,"Bad format");
     return(-2);
    }
  strcpy(ss[0],argv[1]);
   for(i=2;i<argc;i++)
     {
      if(argv[i][0]=='[')
        {
//  printf("%d %s\n",strlen(argv[i]),argv[i]));
  for(j=0;j<strlen(argv[i]);j++) ss[i-1][j]=argv[i][j+1];
        }
      else          ReadS(argv[i],ss[i-1]);
     }
//    for(i=0;i<argc-1;i++)
//      printf("%s\n",ss[i]);
   itog[0]=0;
   for(i=1;i<argc-1;i++)
     {
      strcat(itog,ss[i]);
      strcat(itog," "  );
     }
  AppS(ss[0],itog,strlen(itog));
   return(0);
  }
```

В данном примере достаточно компактного кода мы выделяем из командной строки аргументы, начинающиеся с символа квадратной скобки и интерпретируем их как текстовые строки (имена), а остальные строки понимаем как имена файлов и переносим в итоговую строку их содержание.

Например

```
mks a.bat [gks [Andrey [boss passw1
```

Трансформируется в вызов

call a.bat

gks Andrey boss VeryLongPassForExchangKeys

В результате мы получаем возможность динамического изменения интерпретируемого файла (скрипта) и его реального исполнения в рамках модулей платформы с заданными параметрами и аргументами. При этом, как приведено в примере, мы можем вызывать сам модуль генерации строк чейн-кода с необходимыми аргументами, то есть реализовать рекурсию.

Покажем, что таким образом в рамках платформы можно реализовывать смарт-контракт или чейн-код.

Данный подход также демонстрирует процесс «нулевого» программирования, когда для реализации гибкой логики платформы используются уже встроенные в нее возможности.

ПОНЯТИЕ СМАРТ-КОНТРАКТА И ЧЕЙН-КОДА

Будем говорить, что платформа [5] поддерживает смарт-контракты, в терминах Hyper Ladger Fabric (HLF) — чейнкоды (chaincode), создаваемые на языках общего назначения, таких как Golang, JavaScript, Java, в отличие, от, например, Ethereum, в котором используется контрактно-ориентированный, ограниченный по функциональности язык Solidity (LLL, Viper и др).

С точки зрения разработчика блокчейн-приложение состоит из двух основных частей, представленных ниже.

On-chain модули — смарт-контракты (программы), работающие в изолированном окружении блокчейн-сети, определяющие правила создания и состав атрибутов транзакций. В смарт-контракте основные действия — это чтение, обновление и удаление данных из состояния блокчейн-сети. Следует подчеркнуть, что удаление данных оставляет информацию о том, что эти данные присутствовали.

Off-chain модули — приложение, взаимодействующее с блокчейн-средой через SDK (software development kit, набор средств для разработки ПО). Под взаимодействием понимается вызов функций смарт-контрактов и наблюдение за событиями смарт-контракта — внешние события могут порождать изменение данных в смарт-контракте, в то же время события в смарт-контракте могут инициировать действия во внешних системах.

Чтение данных производится обычно через “домашний” узел блокчейн сети. Для записи данных приложение отправляет запросы на узлы организаций, участвующих в “политике одобрения” определенного смарт-контракта.

Итак, разницу между чейн-кодом (цепным кодом) и смарт-контрактом можно описать следующим образом.

Чейн-код - это программа, написанная, как правило, на Go или на других языках программирования, таких как Java, которая реализует предписанный интерфейс.

Смарт-контракт - это набор кода (его функций) и данных (его состояния), который находится по определенному адресу в блокчейне Ethereum.

В некотором смысле цепной код также можно считать смарт-контрактом, потому что он обрабатывает бизнес-логику, согласованную участниками, так же, как смарт-контракт.

В нашем случае приводимый фрагмент более корректно отнести к чейн-коду.

Приведем результат выполнения описанного выше чейн-кода в составе скрипта. Он демонстрирует вызов скрипта, содержащего как фиксированные приложения, описанные выше, так и динамически созданные строки скрипта. Кроме того, в данном случае мы используем также модули записи в распределенный реестр и формирование квитанции для пользователя, что его информация помещена в распределенный реестр с указанием номера звена (цепочки). Приведенный пример также относится к наукометрической платформе Сешат (Семантически-Естественная Шкала Анализа Текстов) [3].

C:\DEV\SESHAT>rem First Demo SmartContract for creation one user Andrey and operator (Boss)

C:\DEV\SESHAT>rem Create Main key

Процедура создания основного ключевого контейнера оператора системы и распределенного реестра.

C:\DEV\SESHAT>gk0 boss BossPas

Ok Test Random

UserName: boss

UserPIN: BossPas

UserX: 429398babb45cb58

Ok Test Random

Successful UserFile create!

Creation UserKey Time-> 14:07:31 21.10.2022

Обратим внимание на то, что сформировано анонимное имя для оператора платформы 429398babb45cb58.

C:\DEV\SESHAT>rem Create Dir for Boss

C:\DEV\SESHAT>md boss

C:\DEV\SESHAT>rem Create Call for copy key to psv extanton file

C:\DEV\SESHAT>mks a.bat [copy netname [*.psv

Программа (модуль) динамического формирования скрипта (чейн-кода) формирует процедуру копирования полученного контейнера в файл с расширением psw.

C:\DEV\SESHAT>call a.bat

Вот реальный результат вызова

C:\DEV\SESHAT>copy 429398babb45cb58 *.psv

Скопировано файлов: 1.

C:\DEV\SESHAT>mks a.bat [copy [*.psv [boss\boss

C:\DEV\SESHAT>call a.bat

C:\DEV\SESHAT>copy *.psv boss\boss 429398babb45cb58.psv

Скопировано файлов: 1.

C:\DEV\SESHAT>rem Create Andrey key

Аналогичная процедура для пользователя Andrey

C:\DEV\SESHAT>gk0 Andrey 1234

Ok Test Random

UserName: Andrey

UserPIN: 1234

UserX:1b4acb08dc2df32f

Ok Test Random

Successful UserFile create!

Creation UserKey Time-> 14:07:33 21.10.2022

C:\DEV\SESHAT>rem Create Dir for Andrey

C:\DEV\SESHAT>md andrey

C:\DEV\SESHAT>rem Create Call for copy key to psv extanton

C:\DEV\SESHAT>mks a.bat [copy netname [*.psv

C:\DEV\SESHAT>call a.bat

C:\DEV\SESHAT>copy 1b4acb08dc2df32f *.psv

Скопировано файлов: 1.

C:\DEV\SESHAT>mks a.bat [copy [*.psv [andrey\andrey

C:\DEV\SESHAT>call a.bat

C:\DEV\SESHAT>copy *.psv andrey\andrey 1b4acb08dc2df32f.psv

Скопировано файлов: 1.

C:\DEV\SESHAT>del *.psv

Следующий фрагмент создает на стороне системы ключевой контейнер для подписания передаваемых от пользователя к системе документов (статей).

C:\DEV\SESHAT>rem Create Call for Andrey Network key generation use passw1 method

C:\DEV\SESHAT>mks a.bat [gks [Andrey [boss passw1

C:\DEV\SESHAT>call a.bat

C:\DEV\SESHAT>gks Andrey boss VeryLongPassForExchangKeys

Ok Test Random

MyName: Andrey

FriendName: boss

UserPIN: VeryLongPassForExchangKeys

MyUserX:1b4acb08dc2df32f

FriendUserX:429398babb45cb58

1b4acb08dc2df32f429398babb45cb58

Ok Test Random

User NetName: 1b4acb08dc2df32f429398babb45cb58

Successful NetFile create!

Creation NetKey Time-> 14:07:36 21.10.2022

C:\DEV\SESHAT>rem Create Call for copy key to psw extanton

C:\DEV\SESHAT>mks a.bat [copy netnames [*.psw

C:\DEV\SESHAT>call a.bat

C:\DEV\SESHAT>copy 1b4acb08dc2df32f429398babb45cb58 *.psw

Скопировано файлов: 1.

C:\DEV\SESHAT>rem Send psw to Boss and to Andrey dir

C:\DEV\SESHAT>mks a.bat [copy [*.psw [andrey*.*

C:\DEV\SESHAT>call a.bat

C:\DEV\SESHAT>copy *.psw andrey*.* 1b4acb08dc2df32f429398babb45cb58.psw

Скопировано файлов: 1.

C:\DEV\SESHAT>mks a.bat [copy [*.psw [boss*.*

C:\DEV\SESHAT>call a.bat

C:\DEV\SESHAT>copy *.psw boss*.* 1b4acb08dc2df32f429398babb45cb58.psw

Скопировано файлов: 1.

C:\DEV\SESHAT>del *.psw

C:\DEV\SESHAT>rem Distribute ChangePin prog

Следующий фрагмент распределяет исполняемые модули для вызова на стороне системы и на стороне клиента.

В первую очередь это модуль смены пароля контейнера с «длинного пароля» на разные пароли на стороне системы и клиента.

C:\DEV\SESHAT>copy chpin.exe andrey*.*

Скопировано файлов: 1.

C:\DEV\SESHAT>copy chpin.exe boss*.*

Скопировано файлов: 1.

C:\DEV\SESHAT>rem Distribute MakeSmart prog

C:\DEV\SESHAT>copy mks.exe andrey*.*

Скопировано файлов: 1.

C:\DEV\SESHAT>copy mks.exe boss*.*

Скопировано файлов: 1.

C:\DEV\SESHAT>rem Distribute SendReestr prog

C:\DEV\SESHAT>copy rsen.exe andrey*.*

Скопировано файлов: 1.

C:\DEV\SESHAT>rem Distribute RecordReestr prog

C:\DEV\SESHAT>copy rrec.exe boss*.*

Скопировано файлов: 1.

C:\DEV\SESHAT>rem Distribute AddReestr prog

C:\DEV\SESHAT>copy areestr.exe boss*.*

Скопировано файлов: 1.
C:\DEV\SESHAT>rem Normalize psw files names
C:\DEV\SESHAT>cd andrey
C:\DEV\SESHAT\ANDREY>copy *.psw a2boss
1b4acb08dc2df32f429398babb45cb58.psw
Скопировано файлов: 1.
C:\DEV\SESHAT\ANDREY>mks a.bat [chpin [a2boss ..\passw1 [1234
C:\DEV\SESHAT\ANDREY>call a.bat
C:\DEV\SESHAT\ANDREY>chpin a2boss VeryLongPassForExchangKeys 1234
Ok Test Random
UserKey: a2boss
NetName:1b4acb08dc2df32f429398babb45cb58
UserFile create at-> 14:07:36 21.10.2022
Ok Test Random
NetName:1b4acb08dc2df32f429398babb45cb58
NetName:1b4acb08dc2df32f429398babb45cb58
Successful Change PIN!
C:\DEV\SESHAT\ANDREY>cd ..
C:\DEV\SESHAT>cd boss
C:\DEV\SESHAT\BOSS>copy *.psw frandrey
1b4acb08dc2df32f429398babb45cb58.psw
Скопировано файлов: 1.
C:\DEV\SESHAT\BOSS>mks a.bat [chpin [frandrey ..\passw1 [boss
C:\DEV\SESHAT\BOSS>call a.bat
C:\DEV\SESHAT\BOSS>chpin frandrey VeryLongPassForExchangKeys boss
Ok Test Random
UserKey: frandrey
NetName:1b4acb08dc2df32f429398babb45cb58
UserFile create at-> 14:07:36 21.10.2022
Ok Test Random
NetName:1b4acb08dc2df32f429398babb45cb58
NetName:1b4acb08dc2df32f429398babb45cb58
Successful Change PIN!
C:\DEV\SESHAT\BOSS>cd ..
C:\DEV\SESHAT>rem Send Article file (c2.txt) to boss
C:\DEV\SESHAT>copy c2.txt andrey*.*
Скопировано файлов: 1.
C:\DEV\SESHAT>cd andrey
C:\DEV\SESHAT\ANDREY>rem Sign Article file
C:\DEV\SESHAT\ANDREY>rsen a2boss 1234 c2.txt c2.sen
Ok Test Random
Len= 285633
UserFile: a2boss
Successful UserConainer read!
Creation UserConainer Time: 14:07:36 21.10.2022
Network name: 1b4acb08dc2df32f429398babb45cb58
Length: 285680
Ok OutFile write
Ok OutFile read
Ok OutFile check
Registration User File in: 14:07:44 21.10.2022
User File Name: c2.txt
C:\DEV\SESHAT\ANDREY>rem Send Signed File to boss
C:\DEV\SESHAT\ANDREY>copy c2.sen ..\boss*.*
Скопировано файлов: 1.
C:\DEV\SESHAT\ANDREY>cd ..
C:\DEV\SESHAT>cd boss
C:\DEV\SESHAT\BOSS>rem Check Article signature and extract it
C:\DEV\SESHAT\BOSS>rrec frandrey boss c2.sen-x
Ok Test Random
Extract...
UserFile: frandrey
Successful UserConainer read!
Creation UserConainer Time: 14:07:36 21.10.2022
Network name: 1b4acb08dc2df32f429398babb45cb58
Ok OutFile read
Length: 285680
File Signature: 6af3181d4119a443
Calc Signature: 6af3181d4119a443
RecFile valid!
Registration User File in: 14:07:44 21.10.2022
User File Name: c2.txt
Extract name: 1b4acb08dc2df32f429398babb45cb58
Full validation!
Extracting to c2.txt
C:\DEV\SESHAT\BOSS>rem Add Article in Reestr and create notify file

Следующий фрагмент производит помещение экстрагированной статьи в распределенный реестр и выдачу квитанции пользователю при успешной записи в реестр.

C:\DEV\SESHAT\BOSS>areestr.exe boss BossPas c2.txt
Ok Test Random
UserContainer: boss
c2.txt
User File len = 285649
Successful UserConainer read!
Creation UserConainer Time: 14:07:31 21.10.2022
Ok OutFile write
Ok OutFileIndex write
Read Len = 285649
TNum ok Info ok Imi ok Ok transnum Ok imit
DNum :0000000000000000000000000000000
TNum :3de4ffa56c77bffa60dd49a415e6100d

Sign :845f8d751efc3207
File :c2.txt
NetName: 429398babb45cb58
AddTime: 14:07:45 21.10.0022
C:\DEV\SESHAT\BOSS>rem Send notify file to andrey
Квитанция посылается пользователю
C:\DEV\SESHAT\BOSS>copy *.kvt ..\andrey*.*
00000000.kvt
Скопировано файлов: 1.

В предлагаемом подходе к работе доверенной платформы мы можем объединить смарт-контракты и чейн-код в том случае, если исполняемые инструкции будут размещены в блокчейне и будут исполняться только после их верификации (проверки подписи или кода аутентификации) и экстракции из звена блокчейна.

ПОНЯТИЕ ЗЕРОКОДИНГА

Приведя пример интерпретируемого файла для разворачивания платформы, мы попадаем в новую парадигму разработки платформ с применением зерокодинга.

Зерокодинг [6] или no-code — это способ создавать работающие ИТ-продукты без использования или с минимальным использованием инструментов программирования, за счет визуального интерфейса программирования и/или готовых платформенных решений.

Большинство задач по реализации платформы, как мы видим, не отличаются большой уникальностью. Шаблоны no-code позволяют не писать код для таких задач с нуля, а пользоваться готовыми блоками, отталкиваясь от задачи — например, если нужно отправить запрос в базу данных или создать пользователя.

Разработчики, принявшие решение взяться за какой-либо IT-проект, оказываются перед следующей проблемой: у нас есть оформленная идея или гипотеза, при этом мы четко представляем себе нужный результат, но между идеей и результатом существует ощутимый разрыв. Чтобы запустить проект, необходимо получить инвестиции, привлечь аудиторию, продемонстрировать первый результат, что требует в первую очередь написания программного кода.

Поэтому складывается такое положение дел, при котором для достижения первых результатов нужно собрать команду программистов, создав для них идейные или материальные стимулы. Разумеется, это не только может быть сложно и рискованно, но и для первой реализации не является необходимым условием. Более того, первая реализация может показать, что идея была обречена изначально, а время, силы и деньги потрачены напрасно.

Зерокодинг быстро и без особых затрат помогает пройти путь от идеи до технического результата за счет встроенных решений, а также позволяет упрощать и решение более сложных задач в части создания мобильных приложений. К примеру, конструктор мобильных приложений Glide создает не полноценные мобильные приложения, а лишь веб-страницы, которые воспроизводят стиль взаимодействия с мобильным приложением, но этого будет вполне достаточно для демонстрации идеи на практике.

Под зерокодингом понимается и способ создания новых решений и продуктов, проверки бизнес-гипотез и автоматизации работы с помощью готовых инструментов, предназначенных для определенных элементов продукта. Готовое решение можно найти практически для любой идеи, например, маркетплейса, клуба по подписке. Такое решение всегда будет быстрее и дешевле разработки.

Для начала работы с этими инструментами, как мы видим, достаточно применить концепцию платформы. Архитектуру любого продукта можно разделить на ряд взаимосвязанных блоков или слоев.

Чаще всего их три:

- база данных;
- бизнес-логика (процессы работы с данными, принятие решений);
- клиентский слой (различные способы взаимодействия с пользователем, включая защищенные, регистрация пользователей и т.д.).

Для каждого из этих блоков появляются свои инструменты зерокодинга, решающие поставленные перед ними конкретные задачи. При этом нужно понимать, что когда мы говорим о создании продукта с помощью зерокодинга — мы говорим об MVP (Minimum Viable Product), то есть о минимально жизнеспособной версии продукта.

Итак, в результате использования зерокодинга создается понятный платформенный продукт в виде легко понимаемой, обсуждаемой и верифицированной блок-схемы, что позволяет получить как можно больше информации как о работе того или иного нововведения, так и о работе продукта в целом. Таким образом, появляется возможность «вырастить» ценность продукта эволюционным методом и в минимально возможные сроки, проходя этап проверки, внедрения и отбраковки неудачных обновлений, а также тестирования логики блоков платформы и продукта в целом.

ЗАКЛЮЧЕНИЕ

Реализация защищенной доверенной платформы обмена документами и их хранения с учетом применения зерокодинга, а также доверенного хранения скриптов и участвующих в них исполняемых модулей в распределенном реестре (блокчейне) позволяет достичь соответствия важнейшим принципам построения платформ, к которым относятся прежде всего максимальное владение исходным кодом платформы, минимальное использование продуктов третьих фирм, компактность кода, возможность его доработки и технической поддержки.

Для блокчейн-платформ выполнение этих свойств наряду с использованием симметричных криптографическх алгоритмов национальной (отечественной) реализации означает также постепенный переход к пятому поколению блокчейна [7], устойчивому к квантовому компьютингу.

СПИСОК ЛИТЕРАТУРЫ

1. Биктимиров М.Р., Щербаков А.Ю. Проблемы синтеза доверенных систем // Труды ИСА РАН. 2012. Т.53. С. 264-271.

2. Рязанова А.А. Цифровые платформы: интегративный потенциал, основные понятия и свойства // Вестник современных цифровых технолоий, № 4, с. 28-39.

3. Алиев Д.Ф., Бородулина С.А., Щербаков А.Ю. Актуальные подходы к наукометрии и квалиметрии // Вестник современных цифровых технолоий, 2022. № 12. С. 11-20.

4. Щербаков А.Ю. Методологические основы и прототип системы семантического искусственного интеллекта // Научно-технический сборник "Научно-техническая информация", сер. 2 Информационные процессы и системы, 2022. № 9. С. 1-6.

5. Разработка и тестирование смарт-контрактов Hyperledger Fabric. URL: https://habr.com/ru/post/426705/ (дата обращения: 12.11.2022)

6. Принципы зерокодинга: разработчики без опыта и приложения за несколько часов. URL: https://hightech.fm/2021/07/21/zerocode (дата обращения: 12.11.2022)

7. Пятое поколение технологии блокчейна. URL: https://cryptor-net.turbopages.org/cryptor.net/s/budushchee-nastupilo/pyatoe-pokolenie-tehnologii-blokcheyna (дата обращения: 12.11.2022)

УДК: 003.26, 004.04

Учебно-методическое обеспечение дисциплины «Прикладная криптография»

S.V. Zapechnikov

A Curriculum of Applied Cryptography Course

Abstract. *A new course of Applied Cryptography developed for students studying under the Master's program "Data Security and Cryptography" is presented in the paper. The general characteristics of the discipline are given. A summary of lectures, a list and a brief description of programming assignments and homeworks are considered. It is noted that the course materials fully correspond to the current world level of knowledge in the field of cryptography, and the created course can serve as a basis for further development of special courses in certain, the most popular and rapidly developing areas of modern cryptography.*

Keywords: *information security, applied cryptography, authentication protocols, key exchange protocols, secure connections, elliptic curves cryptography, blockchain technologies, zero-knowledge proofs, secure multi-party computations, post-quantum cryptography.*

С.В. Запечников
Доктор технических наук, профессор Института интеллектуальных кибернетических систем, Национальный исследовательский ядерный университет «МИФИ»,
Вице-президент по научной работе Ассоциации специалистов в области криптовалют и цифровых финансовых активов
E-mail: SVZapechnikov@mephi.ru

Аннотация. *В статье представлен новый курс «Прикладная криптография», разработанный для студентов, обучающихся по магистерской программе «Безопасность данных и криптография». Даётся общая характеристика учебной дисциплины, приводится краткое содержание курсов лекций двух семестров, перечень и краткое описание лабораторных работ и сборника задач по курсу. Отмечается, что материалы курса полностью соответствуют актуальному мировому уровню знаний в области криптографии, а созданный курс может служить базой для дальнейшей разработки спецкурсов по отдельным, наиболее востребованным и быстро развивающимся областям современной криптографии.*

Ключевые слова: *информационная безопасность, прикладная криптография, аутентификация, протоколы распределения ключей, защищенные соединения, эллиптические кривые, блокчейн-технологии, доказательства с нулевым разглашением, безопасные многосторонние вычисления, постквантовая криптография.*

ВВЕДЕНИЕ

Криптография была и остаётся основополагающей дисциплиной при обучении студентов всех уровней подготовки по направлению «Информационная безопасность». В быстро меняющемся мире очень важно поддерживать содержание этой учебной дисциплины в актуальном состоянии. С этой целью автором статьи разработан современный 2-семестровый курс «Прикладная криптография» для студентов, обучающихся по направлению подготовки «Информационная безопасность», магистерской программе «Безопасность данных и криптография» в Национальном исследовательском ядерном университете МИФИ.

В качестве ориентиров при разработке курса были взяты современные зарубежные курсы криптографии [1 – 4], дополнительно привлекались материалы курсов [5, 6], фрагменты множества других университетских курсов, учебников и научных статей. Таким образом, не будет преувеличением утверждать, что материалы вновь разработанного курса полностью соответствуют актуальному мировому уровню. Более того, созданный курс может служить базой для дальнейшей разработки спецкурсов по отдельным, наиболее востребованным и быстро развивающимся областям современной криптографии, таким как доказательства с нулевым разглашением или безопасные многосторонние вычисления.

В качестве основной учебной литературы по курсу рекомендуются учебники [7 – 9]. В перспективе предполагается создание собственного русскоязычного учебника прикладной криптографии, соответствующего актуальному мировому уровню знаний в этой области, однако для осуществления этого плана требуется значительное время.

К настоящему времени имеется опыт как полностью дистанционной, так и гибридной реализации курса. Гибридная реализация предполагает очные лекции и дистанционные лабораторные работы. Практика показала, что лекционные занятия с равной степенью успеха могут проходить как в очном,

так и в дистанционном формате, а оптимальная форма реализации лабораторных работ – это дистанционные занятия, так как они позволяют избежать лишних практических трудностей, связанных с переносом программного обеспечения с компьютеров студентов в вузовскую лабораторию либо необходимостью носить с собой ноутбуки на очные занятия. Защита лабораторных работ в этом случае проходит с использованием сервиса видеоконференцсвязи, что нисколько не снижает функциональные возможности и не ухудшает контакта между преподавателем и студентами.

1. ОБЩАЯ ХАРАКТЕРИСТИКА УЧЕБНОЙ ДИСЦИПЛИНЫ

Дисциплина «Прикладная криптография» является одной из центральных при подготовке студентов по магистерской программе «Безопасность данных и криптография». Она позволяет дать студентам представление об алгоритмических возможностях и способах реализации современных средств криптографической защиты информации, продемонстрировать принципы анализа и доказательства стойкости современных криптосистем, научить основам разработки многих важных функциональных и инфраструктурных элементов средств криптографической защиты информации.

Курс двухсеместровый, читается во 2-м и 3-м семестрах магистратуры. Ему предшествуют курсы «Симметричные криптосистемы» и «Асимметричные криптосистемы», читаемые в 1-м семестре магистратуры.

Первая часть курса включает в себя лекционный материал объёмом 30 академических часов и лабораторные работы объёмом 60 академических часов (два лабораторных практикума), завершается зачётом. Вторая его часть состоит из лекций объёмом 32 академических часа и лабораторных работ объёмом 32 академических часа (также два лабораторных практикума, один из которых продолжается с первой части), завершается экзаменом по материалам двух семестров.

Лекции охватывают широкий круг теоретических и методических вопросов, связанных с синтезом и анализом стойкости криптографических протоколов и схем для решения множества современных проблем обеспечения безопасности информации. Выполнение домашних заданий, связанных с решением задач по материалам лекционного курса, позволяет студентам закрепить полученные знания. Лабораторные практикумы позволяют приобрести навыки программирования криптографических алгоритмов и схем, получить опыт исследования атак на криптографические алгоритмы и протоколы, а также изучить основы блокчейн-технологий.

2. КУРС ЛЕКЦИЙ 1-ГО СЕМЕСТРА

Курс лекций 1-го семестра объёмом 30 часов посвящён фундаментальным принципам конструирования криптографических протоколов и схем, формулированию и доказательству их свойств безопасности, знакомству с наиболее употребительным математическим аппаратом, возможностями применения отечественных и международных стандартов по криптографическим методам защиты информации для решения сложных прикладных задач.

Далее приводится примерный план лекционного курса.

Введение. Организационная информация. Краткая история развития криптография в конце XX – начале XXI вв.

Основы конструирования и анализа криптографических протоколов. Основные понятия и определения. Доказательный подход к конструированию криптографических протоколов.

Элементарные протоколы. Протокол (1,2)-забывающей передачи. Схема открытого шифрования Эль-Гамаля. Гибридная схема шифрования. Протокол коммитмента, или обязательства. Дерево Меркле. Модель случайного оракула.

Управление ключами. Основные понятия и определения. Жизненный цикл ключей. Управление ключами симметричных криптосистем. Инфраструктура открытых ключей.

Протоколы аутентификации. Определение протокола аутентификации. Модели противника и атаки. Аутентификация по фиксированным паролям. Словарные атаки. Искусственное замедление вычисления хэш-функции. Многофакторная аутентификация. Аутентификация по одноразовым паролям: протоколы HOTP, POTP, S/key. Протоколы аутентификации «запрос-ответ» с использованием симметричного шифрования и цифровой подписи. Стандарты.

Криптография на эллиптических кривых. Эллиптические кривые над конечными полями. Группы точек эллиптических кривых. Кривые Монтгомери и Эдвардса. Стандарты эллиптических кривых.

Протоколы распределения ключей (ПРК). Основные понятия и определения. Классификация ПРК. Свойства ПРК.

Анонимный обмен ключами. Определение. Протоколы анонимного обмена ключами на основе классических задач криптографии: RSA и Диффи – Хеллмана. Шарады Меркле.

Протоколы аутентифицированного обмена ключами на основе симметричных и асимметричных криптосхем. ПРК конференцсвязи. ПРК с динамическим составом участников. Парольные протоколы аутентифицированного обмена ключами.

Защищенные соединения. Постановка задачи. Краткая история вопроса. Стандарты. Аутентифицированное шифрование. Функция выработки производных ключей HKDF. Спецификации TLS 1.3, IPSec, WireGuard, WEP.

Защищенные асинхронные соединения. Постановка задачи. Мессенджеры. Спецификация Signal: протокол X3DH, механизм «двойного храповика». Многосторонние защищенные асинхронные соединения. Спецификация ART/MLS.

Спаривания. Криптография на основе спариваний. Определение и основные свойства спариваний. Свойство билинейности. Вычислительно сложные задачи, порождаемые спариваниями. Спаривания Тейта и Вейля. Алгоритм Монтгомери. Протокол трёхстороннего обмена ключами Жу (Joux). Схема цифровой подписи BLS. Агрегированная цифровая подпись. Хэширование в точку эллиптической кривой. Функциональное шифрование. Идентификационное шифрование. Полиномиальный коммитмент.

3. КУРС ЛЕКЦИЙ 2-ГО СЕМЕСТРА

Курс лекций 2-го семестра объёмом 32 часа посвящён самым значительным прикладным задачам криптографии. Материал курса разбивается на несколько больших блоков: системы распределенного реестра и блокчейн-технологии, безопасные многосторонние вычисления, постквантовая криптография. Основные криптографические конструкции, изученные в 1-м семестре, служат строительными блоками, или примитивами, в значительно более сложных конструкциях, рассматриваемых в этой части курса.

Ниже приводится примерный план курса лекций.

Введение. Организационная информация.

Распределенные реестры. Системы распределенного реестра (СРР). Блокчейн-технологии. Архитектура СРР. Классификация и применения СРР. Криптоэкономика.

Протоколы консенсуса. Консенсус на блокчейн-платформах открытого типа. Proof-of-work. Proof-of-stake. Задача о византийских генералах. Протоколы византийского соглашения. Масштабирование протоколов консенсуса.

Криптографические доказательства. Интерактивные доказательства. Доказательства с нулевым разглашением. Простые примеры протоколов доказательства. Протоколы аутентификации с нулевым разглашением. Протокол Шнорра. Сигма-протоколы и их свойства. Неинтерактивные системы доказательства с нулевым разглашением. Эвристика Фиата – Шамира. Компактные неинтерактивные доказательства (succinct non-interactive arguments – SNARGs). Булевы и арифметические схемы. Система ограничений R1CS. Компактные неинтерактивные доказательства знания с нулевым разглашением (zero-knowledge succinct non-interactive arguments of knowledge – zk-SNARKs).

Применения криптографических доказательств. Анонимные удостоверения. Анонимная криптовалюта Zcash. Система конфиденциального исполнения смарт-контрактов Zexe.

Основы безопасных многосторонних вычислений (БМВ). Основные факты теории БМВ. Искаженные схемы Яо.

Схемы разделения секрета (СРС). Основные понятия и определения. СРС Шамира. Схемы проверяемого разделения секрета. Пороговая криптография. Линейные СРС. Схема Брикелла. Схемы атрибутного шифрования. БМВ на основе СРС.

Гомоморфное шифрование. Задача обучения с ошибками (learning with errors – LWE). Схема шифрования Регев (Regev). Пример: гомоморфная схема шифрования на основе задачи LWE. Аутсорсинговые и проверяемые вычисления.

Частные случаи БМВ. Конфиденциальная выборка информации из базы данных (private information retrieval – PIR). Пример схемы PIR на основе схемы шифрования Регев. Конфиденциальное вычисление пересечения подмножеств (private set intersection – PSI). Концепция статистической неразличимости (differential privacy).

Постквантовая криптография. Прогресс в создании квантовых компьютеров. Алгоритмы Шора и Гровера. Теорема Моска. Варианты задачи обучения с ошибками над кольцом и над модулем (R-LWE, m-LWE). Примеры: постквантовые криптосистемы Kyber и SABER на основе m-LWE. Криптосистема Мак-Элиса (McEliece) на основе задачи декодирования полных линейных кодов.

Заключительная лекция. Обзор и систематизация материалов курса.

4. ЛАБОРАТОРНЫЙ ПРАКТИКУМ «ПРОГРАММНАЯ РЕАЛИЗАЦИЯ КРИПТОГРАФИЧЕСКИХ ПРОТОКОЛОВ И СХЕМ»

Лабораторный практикум по программной реализации криптографических протоколов и схем продолжительностью два семестра ставит основной целью развить у студентов способности к самостоятельной реализации криптографических протоколов и схем с использованием библиотек широко употребительных криптографических алгоритмов (симметричных шифров, схем открытого шифрования, схем цифровой подписи, криптографических хэш-функций). Студенты не ограничены в выборе языков программирования и библиотек, однако практика показывает, что до 80-90% студентов выбирают язык программирования Python и библиотеки pycryptodome, pygost и др. При реализации программ к студентам предъявляется требование везде, где это возможно, использовать библиотечные реализации отечественных стандартов по криптографическим методам защиты информации (ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012, ГОСТ Р 34.12-2015, ГОСТ Р 34.13-2015 и рекомендации по стандартизации). Только в тех случаях, когда для какого-либо примитива нет стандартизованного отечественного алгоритма либо рекомендации, используются иностранные (международные) стандарты.

Лабораторный практикум начинается с относительно простых заданий, в которых требуется выполнить корректную программную реализацию протоколов по предложенному в задании описанию (спецификации). Для подтверждения работоспособности необходимо предъявить как минимум по одному образцу успешной и неуспешной работы протокола (криптосхемы). В лабораторных работах повышенной сложности предлагается учебное техническое задание, по которому нужно реализовать приведенные в нём функциональные требования и (или) требования стойкости, самостоятельно выбрав для этого необходимые криптографические алгоритмы, протоколы и элементы криптографической инфраструктуры.

В 1-м семестре выполняется 8 лабораторных работ из предложенного списка, из которых последние три отличаются повышенной сложностью (можно, выбрать, например, две из них). Выполнения первых пяти работ достаточно для получения минимальной оценки, последние две предлагаются студентам, претендующим на более высокую оценку. На выполнение лабораторного практикума отводится 30 академических часов.

1. Протоколы аутентификации (парольные, «запрос – ответ»). Лабораторная работа посвящена изучению и реализации базовых протоколов аутентификации по фиксированным и одноразовым паролям: PAP, CHAP, S/key, а также протоколам односторонней и взаимной аутентификации типа «запрос – ответ» на базе цифровой подписи.

2. Симметричные протоколы аутентифицированного обмена ключами. Работа посвящена изучению и применению протокола аутентифицированного распределения ключей с центром доверия на основе симметричных криптосхем 3PKD и его вариантов, а также исследованию атак на него и возможной нестойкости при некорректной реализации.

3. Асимметричные протоколы аутентифицированного обмена ключами. Работа посвящена изучению и реализации протоколов аутентифицированного распределения ключей на основе асимметричных механизмов: AKE1, AKE1-eg, AKE2, AKE2-eg. В учебных реализациях протоколов AKE1-eg и AKE2-eg в качестве алгебраической группы может выбираться либо мультипликативная подгруппа конечного поля, либо группа точек эллиптической кривой.

4. Парольные протоколы аутентифицированного обмена ключами. Работа посвящена реализации серии парольных протоколов аутентифицированного распределения ключей: PAKE0, PAKE1, PAKE2, PAKE2+. В учебных реализациях этих протоколов паролем должна быть произвольная относительно короткая строка символов, в качестве алгебраической группы может выбираться либо мультипликативная подгруппа конечного поля, либо группа точек эллиптической кривой.

5. Схемы гибридного и аутентифицированного шифрования. В работе предлагается реализовать схемы гибридного шифрования на основе библиотечных реализаций симметричного шифра и схемы открытого шифрования, а также сравнить четыре подхода к одновременному обеспечению свойств конфиденциальности и аутентичности сообщений в канале связи: аутентификация после шифрования (encrypt-then-MAC); аутентификация параллельно с шифрованием (encrypt-and-MAC), шифрование после аутентификации (MAC-then-encrypt и режимы аутентифицированного шифрования блочных шифров (GCM, CCM, OCB), сравнить скорости зашифрования и расшифрования файлов при использовании разных механизмов.

6. Реализация модели менеджера паролей.* Задание на лабораторную работу сформулировано в виде учебного технического задания. В нём тре-

буется реализовать программное средство хранения паролей, стойкое к атакам при заданной модели противника. Перечислены требования и ограничения, которым должна отвечать реализация. Конкретные способы защиты от атак студенты должны предложить и реализовать самостоятельно, обосновав состоятельность предложенных решений.

7. Реализация модели защищенного канала передачи данных по спецификации TLS 1.3.* Требуется в соответствии с выданным учебным техническим заданием реализовать модели четырёх участников криптосистемы: Удостоверяющего центра, сервера и двух клиентов. После этого необходимо реализовать протоколы выдачи Удостоверяющим центром сертификатов открытых ключей, протокол аннулирования Удостоверяющим центром сертификатов открытых ключей, протоколы установления защищенных соединений, имитирующие TLS 1.3, протоколы передачи сообщений по защищенным каналам, имитирующим TLS 1.3.

8. Реализация модели двустороннего защищенного чата в мессенджере по спецификации Signal.* В лабораторной работе требуется в соответствии с выданным учебным техническим заданием реализовать модели трёх участников криптосистемы: сервера мессенджера и двух клиентов. После этого необходимо реализовать следующие криптографические протоколы взаимодействия между моделями трёх участников криптосистемы: регистрацию клиента мессенджера, установление защищенного соединения, один раунд работы асимметричного храповика, один раунд работы симметричного храповика.

Во 2-м семестре предусмотрено выполнение четырёх лабораторных работ продолжительностью 4 часа каждая.

1. Протоколы консенсуса. Работа посвящена реализации моделей протоколов консенсуса, основанных на принципе лотереи: «доказательство выполнения работы» (proof-of-work), «доказательство обладания долей» (proof-of-stake) и на принципе голосования (протоколы византийского соглашения), а также сравнительному исследованию свойств протоколов на базе этих моделей.

2. Доказательства с нулевым разглашением. В лабораторной работе студенты реализуют простые протоколы аутентификации с нулевым разглашением (протоколы Фиата – Шамира, Шнорра), а также протокол компактного неинтерактивного доказательства знания с нулевым разглашением для простой булевой функции с использованием библиотечных функций.

3. Схемы разделения секрета. В лабораторной работе студенты реализуют простые пороговые СРС Шамира, Фельдмана и Педерсена, линейную СРС Брикелла, а также учатся использовать их в составе протоколов БМВ.

4. Исследование гомоморфных свойств криптосхем. В работе предлагается исследовать свойства гомоморфности некоторых частично и полностью гомоморфных криптосхем: RSA и Эль-Гамаля (гомоморфных по умножению), Пайе (гомоморфной по сложению), BGV или FGV (полностью гомоморфных), а также применить их в составе одного из криптографических протоколов, решающих простую прикладную задачу.

5. ЛАБОРАТОРНЫЙ ПРАКТИКУМ «ИССЛЕДОВАНИЕ АТАК НА КРИПТОГРАФИЧЕСКИЕ АЛГОРИТМЫ И ПРОТОКОЛЫ»

Лабораторный практикум, посвященный экспериментальному исследованию разнообразных атак на криптографические алгоритмы и протоколы, реализуется в 1-м семестре параллельно с описанным выше лабораторным практикумом. Общий его объём – 30 часов. Главная учебная задача этого лабораторного практикума – привить студентам специфические навыки исследования криптографических примитивов, повторив наиболее известные из литературы приёмы атак. Такие атаки основаны не на криптоанализе, а преимущественно на эксплуатации уязвимостей протоколов, ошибок реализации и различных особенностей, не предусмотренных создателями. Некоторые атаки реализуются при искусственно ослабленных параметрах криптосистем и демонстрируют важность правильного выбора параметров. Практикум включает в себя 13 лабораторных работ продолжительностью 2 часа каждая, из которых преподаватель выбирает подмножество работ, проводимых со студенческой группой, исходя из конкретных условий и доступного времени.

Ниже приводится перечень подготовленных лабораторных работ:

1. «Слепая» атака на схему цифровой подписи RSA. Атака Винера. Атака Хастада.

2. Атака при известной части закрытой экспоненты. Атака при внедрении ошибки в алгоритм расшифрования RSA с китайской теоремой об остатках.

3. Атака на оракула RSA по последнему биту. Атака Блейхенбахера на оракула RSA по PKCS#1 v1.5.

4. Атака на маленькие подгруппы в протоколе Диффи-Хеллмана по группе умножения в поле вычетов простого числа. Вычисление дискретного ло-

гарифма с помощью ро- и лямбда алгоритмов Полларда в группе умножения в поле вычетов простого числа.

5. Атака на маленькие подгруппы в протоколе Диффи-Хеллмана над группой точек эллиптической кривой. Атака с использованием точек других кривых.

6. Атака с использованием точки на квадратичном кручении эллиптических кривых Монтгомери. Атака на повторяющееся одноразовое заполнение (nonce) в схеме подписи DSA.

7. Атака на схемы подписи ECDSA с взаимозависимыми одноразовыми заполнениями. Подделка параметров подписи в схемах RSA и DSA при фиксированной подписи и сообщении.

8. Атака на режим шифрования OCB2. Атака на режим GCM с повторяющимися одноразовыми заполнениями.

9. Атака на режим GCM с укороченным кодом аутентификации сообщений.

10. Восстановление состояния вихря Мерсенна по выводу. Восстановление состояния генератора псевдослучайных чисел на основе регистров сдвига с линейной обратной связью.

11. Атака на игрушечный блочный шифр с плохими линейными характеристиками. Дифференциальная атака на алгоритм шифрования FEAL.

12. Атака на криптосистему Мак-Элиса (McEliece). Атака по побочному каналу при использовании эффективного алгоритма Евклида в криптосистеме RSA.

13. Атака на последний раунд AES по побочному каналу. Атака на последний раунд AES по побочному каналу с шумами. Атака на последний раунд AES методом индуцированных сбоев.

6. ЛАБОРАТОРНЫЙ ПРАКТИКУМ «ОСНОВЫ БЛОКЧЕЙН-ТЕХНОЛОГИЙ И ОБЕСПЕЧЕНИЯ ИХ БЕЗОПАСНОСТИ»

Лабораторный практикум, посвящённый блокчейн-технологиям, реализуется во 2-м семестре параллельно с лабораторным практикумом «Программная реализация криптографических протоколов и схем». Основная учебная задача – познакомить студентов с практическими основами применения технологий распределенного реестра, в первую очередь, в сфере криптовалют и цифровых финансовых активов (ЦФА), обучить их работе с широко распространенными программными средствами, привить навыки разработки программного кода смарт-контрактов. Практикум включает в себя четыре лабораторных работы продолжительностью 4 часа каждая.

В рамках практикума выполняются следующие лабораторные работы:

1. Инструментарий и приложения экосистемы Ethereum. В этой лабораторной работе студенты получают начальные навыки работы в сети Ethereum, подготавливают окружение для работы в сети Ethereum.

2. Виртуальная машина Ethereum и смарт-контракты. В этой работе студенты получают знания о внутреннем устройстве виртуальной машины Ethereum (Ethereum virtual machine – EVM), навыки программирования на языке Solidity, проектирования и создания смарт-контрактов. Результатом работы является написанный и размещенный в тестовой сети Ethereum смарт-контракт.

3. Межконтрактное взаимодействие. Основы обеспечения безопасности информации в блокчейн-технологиях. Выполняя эту работу, студенты приобретают навыки разработки и эксплуатации смарт-контракта, взаимодействующего с другим смарт-контрактом, знакомятся с особенностями обеспечения безопасности смарт-контрактов. В результате студенты создают смарт-контракт, который вызывает функции другого смарт-контракта, готовят пояснительную записку с отчетом о формальной верификации смарт-контракта.

4. Безопасность информации в смарт-контрактах. Смарт-контракты работают с данными, имеющими ценность, например, с цифровыми финансовыми активами, и, если логика обработки имеет уязвимость, то либо ценность данных снижается, либо ЦФА могут быть полностью утрачены пользователем. Для повышения качества и надёжности работы смарт-контрактов применяются различные методики, основная из которых – тестирование. Студенты знакомятся с техниками тестирования смарт-контрактов, разрабатывают интеграционные тесты на взаимодействие смарт-контрактов.

7. СБОРНИК ЗАДАЧ ПО ПРИКЛАДНОЙ КРИПТОГРАФИИ

Важной частью учебно-методического обеспечения учебной дисциплины является сборник задач по всем разделам лекционного курса.

Из сборника выбираются задачи для больших домашних заданий, выдаваемых студентам в каждом из двух семестров изучения курса в соответствии с темами лекционных занятий. Задачи из сборника также могут быть использованы для са-

мостоятельной работы студентов.

Перечислим основные темы задач сборника:

• протокол проверки совпадения элементов множества;

• словарные атаки;

• простые схемы разделения секрета;

• двусторонний протокол аутентифицированного обмена ключами с защитой от чтения назад;

• групповая рассылка кодов аутентификации сообщений;

• протокол забывающей передачи из схемы открытого шифрования;

• защита электронной почты с использованием схемы шифрования Эль-Гамаля;

• мультикоммитменты;

• атаки на схему цифровой подписи Шнорра;

• протоколы группового обмена ключами;

• стойкость криптографических хэш-функций в задаче доказательства выполнения работы (proof-of-work);

• небинарные деревья Меркле;

• малоресурсные клиенты блокчейн-платформ;

• уязвимости в реализации протокола сети Bitcoin;

• оценка количества электроэнергии, потребляемой сетью Bitcoin;

• надёжная широковещательная рассылка:

• построение квадратичной арифметической программы;

• нестойкость искажённых схем к активному противнику;

• генерация мультипликативных троек Бивера;

• ограниченно гомоморфные схемы шифрования на основе спариваний.

Этот список не является окончательным. Предполагается ежегодное пополнение фонда задач для более полного покрытия всех разделов курса и отражения современных направлений развития прикладной криптографии.

Комплект учебно-методических материалов включает в себя также списки вопросов и задач для проведения зачёта в 1-м семестре и экзамена во 2-м семестре.

ЗАКЛЮЧЕНИЕ

Соответствие университетских учебных дисциплин актуальному мировому уровню научных знаний и технологического развития является ключевым условием подготовки высококвалифицированных кадров для всех отраслей экономики, включая будущих научно-педагогических работников. Разработанное учебно-методическое обеспечение дисциплины «Прикладная криптография» служит решению этой задачи в части подготовки кадров в сфере информационной безопасности. Планы дальнейшей работы связаны с регулярной актуализацией содержания дисциплины, созданием современного русскоязычного учебника криптографии, расширением фонда задач и лабораторных работ. Приобретённый автором опыт в дальнейшем предполагается спроецировать и на другие дисциплины, читаемые студентам, обучающимся по направлению «Информационная безопасность».

СПИСОК ЛИТЕРАТУРЫ

1. CS255: Introduction to Cryptography. Stanford university, 2022. URL: https://crypto.stanford.edu/~dabo/cs255/ (дата обращения: 01.12.2022)

2. CS355: Topics in Cryptography. Stanford university, 2022. URL: https://crypto.stanford.edu/cs355/22sp/ (дата обращения: 01.12.2022)

3. CS251: Cryptocurrencies and Blockchain Technologies. Stanford university, 2022. URL: https://cs251.stanford.edu/ (дата обращения: 01.12.2022)

4. CS 127/227. An intensive introduction to cryptography. Boaz Barak, Harvard university, 2021. https://cs127.boazbarak.org/ (дата обращения: 01.12.2022)

5. CS459: Foundation of probabilistic proofs. Alessandro Chiesa, Berkeley university, 2022. URL: https://people.eecs.berkeley.edu/~alexch/classes/CS459-F2022.html (дата обращения: 01.12.2022)

6. CMSC 858T: Introduction to Secure Distributed Computation. Jonathan Katz, University of Maryland, 2021. URL: http://www.cs.umd.edu/~jkatz/gradcrypto2/s21/ (дата обращения: 01.12.2022)

7. Boneh D., Shoup V. A graduate course in applied cryptography. 900 pp. 2020. URL: https://toc.cryptobook.us/book.pdf (дата обращения: 01.12.2022)

8. Katz J., Lindell Y. Introduction to modern cryptography. 3rd edition. 649 pp.

9. Menezes A., van Oorschot P., Vanstone S. Handbook of Applied Cryptography. 816 pp. 2001. URL: https://cacr.uwaterloo.ca/hac/ (дата обращения: 01.12.2022)

Редакционное предисловие к статье «Природоведческая микробиология в эпоху цифровизации»

В этом номере мы с радостью, искренним уважением и благодарностью представляем вниманию наших читателей статью Петра Александровича Кожевина, доктора биологических наук, профессора, академика Российской Экологической Академии, профессора кафедры биологии почв МГУ.

Петр Александрович – продолжатель традиций научной школы С.Н. Виноградского, сторонник глубокого изучения и осознания проблемы «микроорганизма и его естественной среды обитания», телеономичности (целеполагания) микробных систем с механизмами “тонкой настройки“, включая антибиотики в качестве информбиотиков и почвенную резистому. Он разработал целый ряд принципиально новых подходов к изучению поведения микробных популяций и сообществ в природных местообитаниях, что позволило в полной мере представить “динамическую микробиологию” с пониманием событий в линейном времени (хронос), циклах (сукцессии) и управлением желательными и нежелательными микроорганизмами (кайрос). Предложил триаду приспособленности микроорганизмов к почве как природному местообитанию, которое характеризуется не только гетерогенностью, но и выраженной гетерохронностью.

Петр Александрович награжден золотой медалью XXVII Международного салона инноваций в Женеве (1999) и медалью «В память 850-летия Москвы», является членом ученого совета МГУ по специальности «Микробиология», ответственным секретарем редакционной коллегии журнала Вестник МГУ. Серия 17 «Почвоведение».

Окончил биолого-почвенный факультет МГУ в 1973 г. Защитил кандидатскую диссертацию по теме «Люминесцентно-микроскопическое изучение комплекса микроорганизмов и отдельных микробных популяций в почве» в 1976 г. и докторскую диссертацию по теме «Популяционная экология почвенных микроорганизмов» в 2000 г. Является автором более 250 статей, монографий, учебников для университетов и патентов.

Любезно предоставленная нашему журналу статья – плод размышлений Петра Александровича в области цифровизации биологии.

УДК: 579.26, 004.04

Природоведческая микробиология в эпоху цифровизации

П.А.Кожевин
Доктор биологических наук,
профессор кафедры биологии почв
факультета почвоведения
МГУ им. М.В.Ломоносова.
E-mail: kozhevinpa@mail.ru

P.A. Kozhevin

Microbial Ecology in the Digital Age

Abstract. *The article discusses the paradigm shift in modern microbiology as a result of the progress of molecular genetic methods (genocentrism) with the parallel development of digitalization (big data and methods of their analysis). Some possibilities, perspectives and problems associated with the above line of thought are discussed.*

Keywords: *microbial ecology, digital microbiology, microbial system.*

Аннотация. *В статье рассматривается изменение парадигмы современной микробиологии в результате прогресса молекулярно-генетических методов (геноцентризм) с параллельным развитием цифровизации (big data и методов их анализа). Обсуждаются некоторые возможности, перспективы и проблемы, связанные с указанным направлением научной мысли.*

Ключевые слова: *экология микроорганизмов, цифровая микробиология, микробная система.*

ВВЕДЕНИЕ

Микробиология – наука, объектами которой являются невидимые для невооруженного глаза организмы, в последние два десятилетия развивалась под существенным влиянием цифровых технологий. В частности, классификация микроорганизмов сейчас представляет собой рутинную техническую процедуру упорядочивания множества объектов по цифровым показателям. Для этого современные “охотники за микробами” используют преимущественно генетическую информацию, что не требует творческих усилий, крайне необходимых в “пещер-

ную" эпоху до появления молекулярно-генетических методов.

Развитие новых методов и подходов уже сейчас принципиально изменило работу микробиологических лабораторий. Еще более серьезные изменения ожидаются в ближайшем будущем в результате глубокой цифровизации микробиологических рабочих процессов посредством эффективного использования больших данных, машинного обучения и искусственного интеллекта. В первую очередь это касается медицинской микробиологии с задачами быстрой диагностики, определения уровня устойчивости конкретного возбудителя к препаратам, выбора оптимальной схемы лечения и динамического контроля эффективности лечения. Цифровые подходы будут предлагаться как прорывные и во всех других теоретических и прикладных областях микробиологии, включая экологию микроорганизмов, почвенную и водную микробиологию, биоиндикацию, биотестирование, биоремедиацию и другие области, которые связаны с контролем "здоровья" окружающей среды, экологической и продовольственной безопасности.

Автор начал использовать нейронные цепи в микробиологии более 20 лет назад и вместе с аспирантом С.А. Марченко убедился в их потенциале и эффективности. В частности, тогда мы обучили простую трехслойную сеть с небольшим числом нейронов в каждом слое на выборке данных по микробиологическим характеристикам почв с разными уровнями загрязнения канцерогенными полициклическими ароматическими углеводородами [1]. После обучения сеть показала свою высокую эффективность (с точностью примерно 80%) при прогнозировании уровней загрязнения и заодно, в ходе упрощения и вербализации, позволила сократить объем экспериментальной работы. Огорчило, правда, нежелание нейросети делиться своими секретами ("черный ящик"), тогда как, например, дискриминантный анализ в этом смысле ведет себя более дружелюбно и предоставляет исследователю информацию для размышлений.

Понятно, что путь к широкому использованию технологий искусственного интеллекта, если этим вообще можно и нужно заниматься для перехода на некий новый технологический уклад, должен пройти через стадию анализа преимуществ, ограничений, затрат, гарантий и понимания этической составляющей для лиц и организаций. Очевидно, что надо учитывать и присущие таким технологиям риски, связанные, например, с возможностью "отравления" искусственного интеллекта злоумышленниками на уровне обучающей выборки или деанонимизации объекта. Понятную тревогу вызывает игнорирование этических принципов, что просматривается в девизах локомотивов цифровизации (как пример, "Move fast and break things" у Facebook). Научная честность предполагает возможность проверки полученных результатов другими исследователями (тест на фальсифицируемость по Попперу), но в ситуации, когда технология закрыта по коммерческим или иным причинам, это сделать будет совсем не просто. Важнейшим представляется и вопрос о том, кто и с какой целью использует подобные цифровые технологии.

Микробиологи должны оценить возможности и ограничения цифровой трансформации их привычной работы. Речь идет не только об автоматизации процедур выявления и количественного учета микроорганизмов при микроскопии и на питательных средах с идентификацией популяций молекулярно-генетическими и другими методами, но и о целевом определении ключевых характеристик конкретных штаммов (например, спектра устойчивости к комплексу антибиотиков в медицине или к набору приоритетных загрязняющих веществ в городской среде). Такие подходы в значительной степени уже реализованы в практической работе. Визуализация данных с панелями мониторинга, обобщение информации и принятие решений являются частями аналитической работы. Вместе с тем, для автора остается открытым, например, вопрос о том, как повлияет на творческие способности аспиранта желание сделать в своей работе основной упор на искусственный интеллект.

С другой стороны, микробиологические проблемы могут заинтересовать и специалистов в области информационных технологий. В частности, им приходится сейчас продумывать цифровое обеспечение в проблемах "природоподобия", климата, загрязнения среды, "зеленой" энергетики, карбонового "следа". Именно здесь для понимания требуется информация о микробном мире. И как для принятия микробиологами цифровой технологии необходимо доверие к ней, так для специалиста в области информационных технологий важно понимать в первом приближении природоведческую проблему и критически оценивать ее актуальность.

Цель настоящей статьи - познакомить читателя с некоторыми ключевыми микробиологическими проблемами в эпоху цифровизации. Следует заметить, что эмпирический опыт и интересы автора статьи, на основе которых она построена, связаны с некоторыми объективными ограничениями.

ИЗ КРАТКОЙ ИСТОРИИ ВОПРОСА

Невидимый мир микроорганизмов стал видимым после изобретения в 17 веке микроскопа, с помощью которого Антони ван Левенгук выявил живые клетки микроскопических размеров. Его имя хорошо известно, поскольку результаты наблюдений с рисунками он регулярно отсылал в Лондонское королевское общество.

Момент появления микроскопа является начальной точкой отсчета для микробиологии как науки. Размер организма – это в некотором смысле его судьба, что проявляется в особенностях клеточного строения, физиологии, биохимии, генетики и экологии, включая темп размножения. Клетка микроскопических размеров почти не ощущает гравитации и может легко парить в воде (планктон) или в потоках воздуха (аэропланктон). Зато силы поверхностного натяжения, капиллярные эффекты, электростатические и другие силы взаимодействия с твердыми поверхностями выходят на первый план. Это проявляется в формировании микробных биопленок как сложно устроенных социальных структур, причем популяции в ходе колонизации могут вести активный информационный обмен между собой и своими потомками посредством химических мессенджеров по схемам, напоминающим амплитудную и частотную модуляцию радиосигнала.

Первые эксперименты в микробиологии связаны с прямыми микроскопическими наблюдениями в разнообразных природных местообитаниях – от воды из лужи до слюны (*in situ, in vivo*). Требование о приоритете информации из природы является характерной особенностью отечественной микробиологии до настоящего времени. Поэтому в названии нашей статьи упоминается именно природоведческая микробиология – термин, который с особым смыслом введен Г.А. Заварзиным [1]. Здесь уместно вспомнить афоризмы из сборника “Басни Харьковские“ Григория Сковороды: “Без природы, как без пути: чем далее успеваешь, тем беспутнее заблуждаешь… Многие без природы изрядные дела зачинают, но худо кончат“.

Очень быстро микробиологи научились выделять и культивировать некоторые микроорганизмы на специально подобранных питательных средах в лаборатории (*in vitro*). Сразу же появилась проблема согласования данных *in situ и in vitro*, а сейчас после появления виртуального мира математических моделей микробных популяций и сообществ *(in silico*) ситуация стала еще более запутанной.

Примечательно, что практическое применение микроорганизмов началось задолго до появления микробиологии. Классические примеры связаны с хлебопечением и виноделием. Бобовые культуры с азотфиксирующими симбиотическими бактериями в клубеньках на корнях обязательно включали в севооборот для повышения плодородия почв в Древнем Египте, а затем и в Греции и Риме.

Еще один яркий пример – использование микроорганизмов в военном деле, и касается он не бактериологического оружия. Речь идет о получении селитры для пороха посредством компостирования на основе собранной вблизи трактиров мочи. В “Уставе ратных, пушкарских и других дел, касающихся до воинской науки (по приказу его Светлости князя Григория Алексеевича Потемкина)” есть отдельный Указ 593 с исчерпывающей информацией о том, как “готовить и сыскивать“ селитру. Удивительно, но прописанные в Уставе режимы компостирования (температура, аэрация, время, pH) соответствуют параметрам современного оптимизационного эксперимента.

Примером масштабного применения уже научной микробиологии является советская технология, разработанная в рамках микробиологической программы. Основной целью этой программы был биосинтез кормового микробного белка. К началу “перестройки” эта цель была достигнута и по всей стране начали действовать крупнотоннажные заводы с мощными ферментерами. Западные ученые писали, что решение советскими учеными этой важнейшей проблемы в сельском хозяйстве практически привело к независимости от неблагоприятных климатических факторов.

Основным продуцентом белково-витаминного препарата (паприн) была популяция дрожжей, которую выращивали в ферментерах на углеводородах (парафинах) нефти. Использование такого ресурса позволило реализовать на практике экологический принцип – “отходы в доходы”, причем руководители программы (проф. Н.Б. Градова) серьезное внимание уделяли проблеме риска в случае аварийного выброса продуцента в окружающую среду [3]. Этот же вопрос изучали для бактериальных популяций, продуцирующих белково-витаминный препарат (гаприн) из природного газа [4]. Объемы выпуска паприна к 1987 году превысили 1 млн. тонн.

В результате в стране удалось быстро увеличить продукцию животноводства и резко повысить индекс потребления белка населением. Однако в 1989 году программа была закрыта, Главное управление микробиологической промышленности СССР ликвидировано, а заводы с ферментерами заброшены. На фоне кризиса отечественного сельского

хозяйства начался импорт продукции западного животноводства (куриные окорочка “ножки Буша”), продуктов с американским соевым белком.

Еще одна попытка ведения дел в сельском хозяйстве на основе использования микроорганизмов с упором на получение высококачественной продукции и минимизации загрязнения окружающей среды была предпринята в начале этого века в Белгородской области [5]. Удалось связать в функциональном плане растениеводство и животноводство. В частности, отходы бройлерных птицефабрик быстро компостировались на биополигонах микроорганизмами, которые разогревали компост до 70° и выше и превращали токсичные для природы вещества в ценнейшие биоудобрения с объемом сотни тысяч тонн в год.

Для повышения качества и количества урожая сельскохозяйственных культур использовались микробные удобрения и биофунгициды. Широкомасштабный опыт как в научном, так и в экономическом отношении был весьма успешным. В научном плане мы снова использовали мощный функциональный потенциал микроорганизмов. Однако и здесь мы убедились, что успех дела связан не столько с микроорганизмами, сколько с людьми. Можно даже сказать, что у добрых людей и микроорганизмы как добрые помощники. В те годы руководство области (Савченко Е.С., Анисимов А.И.) и “красные директора” разрушенных биотехнологических предприятий (В.Г.Правдин) много сделали в этом направлении, несмотря на сильное противодействие различных структур.

В ходе работы использовались комплексные микробные препараты, для получения которых применялись и математические методы, включая оптимизационные модели, марковские цепи и теорию игр. Основой был принцип динамической микробиологии С.Н. Виноградского с пониманием событий в линейном времени (хронос), циклах (сукцессии) и прицельным управлением популяциями (кайрос) с учетом не только гетерогенности, но и гетерохронности природных местообитаний микроорганизмов.

Завершая предельно краткий обзор некоторых фактов из истории, для демонстрации значимости микробного мира, представим специалистам по цифровым технологиям простейший (без машинного обучения и нейросетей!) рецепт получения эффективного микробного удобрения, разработанный, что примечательно, в военное время (1944 г.). Его автор – Николай Александрович Красильников, основатель кафедры биологии почв, член-корреспондент АН СССР.

По этому рецепту 10 чайных ложек водки добавляют в 100 мл воды, перемешивают и вливают жидкость в 1 кг отобранной заранее плодородной почвы. Затем при тщательном перемешивании почву постепенно увлажняют до состояния легко мажущейся массы. После этого весь образец делят на 4 части, каждую из которых намазывают ровным слоем (толщиной не более 2 см) на столовую тарелку. Поверхность заглаживают ложкой, а затем каждую тарелку накрывают стеклом или другой тарелкой и ставят в теплое место (25-30°С). Через 3-4 дня инкубации препарат готов к применению, а на поверхности почвы обычно появляются блестящие колонии бактерий и даже слизистая биопленка азотфиксаторов и других активаторов растений. Одна тарелка препарата (примерно 250 г почвы) достаточна для обработки гектарной порции семян злаков.

Мы же на основе столь простого “кухонного“ решения с помощью цифровых технологий получали комплексные микробные препараты с заданной целевой функцией (например, биологический контроль нежелательных грибов). Рецепты медицинского назначения мы рассматривать здесь не будем в силу понятных причин, хотя лечение почвой известно с давних времен (геофагия). Понятно, что это не относится к ситуации, когда житель современного мегаполиса ежедневно получает солидную дозу городской пыли. Можно лишь упомянуть утраченный рецепт почвенной катаплазмы (мазь) крупнейшего специалиста в области гнойной хирургии (“узника сталинских лагерей” и лауреата Сталинской премии) профессора В.Ф. Войно-Ясенецкого (св. Лука, архиеп. Симферопольский и Крымский).

Подобные примеры онтологического плана подчеркивают роль личности исследователя (озарение!) и поэтому вряд ли по силам искусственному интеллекту.

ТЕЛЕОНОМИЧНОСТЬ МИКРОБНЫХ СИСТЕМ

Невозможно определить точные показатели обилия микроорганизмов в природных местообитаниях, но при самой скромной оценке общая численность прокариотных микроорганизмов (бактерии и археи) на планете Земля составляет примерно 10^{30} клеток, что на 9 порядков превышает число известных звезд во Вселенной. В почвах нашей планеты обитает около $3x10^{29}$ клеток. Близкие по порядку величины показатели приводятся для океана и литосферы. А в качестве примера “минорных” микробных местообитаний ограничимся только попу-

ляцией *Homo sapiens* и атмосферой – $4x10^{23}$ и $5x10^{22}$ клеток соответственно [6]. Приведенные цифры столь велики, что заставляют вспомнить невообразимо большее число гугол и, конечно, учебные примеры с расчетом числа молекул в комнате с использованием числа Авогадро (примерно 10^{28}), что на порядок ниже численности микроорганизмов в почвах планеты. В последнем случае ситуация еще интереснее: в комнате набор молекул представлен малым множеством разновидностей (10-20) с идентичными характеристиками, тогда как в 1 г почвы может содержаться более 10^5 условных видов с совершенно разными характеристиками.

Таким образом, природные микробные системы настолько сложны, что волей-неволей вспоминаются неопределенности квантовой механики с заменой знаменитого «кота» Шредингера на «бактерию» Шредингера. На внутриклеточном уровне в нано-масштабах квантовые механизмы в той иной степени используются объектом, но сейчас физики пытаются оценить возможность перевода всей микробной клетки в когерентное квантовое состояние. Квантово-механический объект, как известно, описывается волновым уравнением Шредингера с введением принципиальной неопределенности характеристик, включая положение в пространстве (в любой точке всей Вселенной с определенной вероятностью). Понятно, что эти вопросы, связанные с криптобиозом (скрытая жизнь), в первую очередь волнуют астробиологов.

Итак, если для простых неживых физических объектов с идентичными свойствами даются две разные интерпретации (частица-волна), то в случае с микроорганизмами интерпретаций может очень много. Тем не менее, для микробиолога, который считает своими основными объектами клетки, популяции и сообщества, ситуация представляется совсем не безвыходной. Важно только не делать основной упор на исследование более низкого уровня организации. Сложность на одном уровне организации никоим образом не исключает простоту объяснения на более высоком уровне. Об этом свидетельствует наличие простых количественных феноменологических законов роста. Ферментативная кинетика проще квантовых законов “под капотом”, и обычно вполне достаточна для описания физиологии клетки. И в генетике многие классические закономерности, включая закон Менделя, были получены без знания о роли ДНК в молекулярных или клеточных процессах. Наиболее очевидна значимость простоты понимания за счет эмерджентности сложных систем при переносе внимания исследователя на функциональные характеристики объектов [7]. Приоритет функционального подхода с исследованием микроорганизмов в природном контексте характерен для отечественной микробиологической школы.

Зимой 1879 года перед членами Императорской фамилии с докладом о роли микроорганизмов на планете выступил великий русский ученый Сергей Николаевич Виноградский (1856-1953), совершивший ряд выдающихся открытий, включая описание нового типа питания (результат явно выше планок любых премий) – хемотрофии с доказательством того, что органическое вещество в биосфере планеты образуется не только в процессе фотосинтеза, но и в процессе хемосинтеза (в частности, так получают энергию для жизни микробные нитрификаторы в вышеприведенном примере с селитрой в ходе реакций окисления аммиака до нитрита и нитрита до нитрата).

Главная мысль доклада заключается в том, что организмы в природе функционируют как самодостаточная полноценная система, которую С.Н. Виноградский рассматривал “как один огромный организм, заимствующий свои элементы из резервуара неорганической природы, целесообразно управляющий всеми процессами своего прогрессивного и регрессивного метаморфоза и, наконец, отдающий снова все заимствованное назад мертвой природе“ [8]. Эта работа сразу же после появления попала в архив мировой науки, содержащий выдающиеся научные идеи и достижения за всю историю человечества. Только примерно через сто лет сходные идеи представлены физиком Д. Лавлоком и биологом Л. Маргулис в популярной «гипотезе Земли-Геи» (по имени древнегреческой мифологической богини Земли).

С.Н. Виноградский особо выделил важнейший атрибут системы – целесообразность (телеономичность) как согласованность и соответствие внутрисистемных элементов друг другу и внешней среде. Можно оценить степень согласованности осуществляемых биотой процессов биохимического синтеза и разложения органического вещества на планете. Расчет “физикалистов“ показывает, что в случае совпадения среднеглобальных скоростей синтеза и разложения с точностью около 1%, биота разрушила бы среду за времена порядка тысячи лет. Чтобы выполнить принятое сейчас в науке положение о более 3 миллиардах лет жизни на планете, средние скорости синтеза и разложения органического вещества должны совпадать с фантастической точностью до восьмого знака после запятой [9]. Можно сказать, что микроорганизмы чудесным образом подготовлены к решению вычислительной задачи

по поддержанию основных параметров биосферы в очень узком диапазоне значений на протяжении миллиардов лет.

Отмеченная С.Н. Виноградским телеономичность природных систем связана с их “тонкой настройкой” (“fine tuning“), которая в принципе не может быть заменена управлением человеком. Можно предположить, что важную роль в “тонкой настройке” играют, в частности, малые молекулы так называемых вторичных метаболитов, синтез которых не совпадает с удельной скоростью роста и приурочен к поздним этапам развития популяции. В первую очередь, это относится к антибиотикам. В полной мере эра антибиотиков началась после выделения из почвы в 1943 году С. Ваксманом (лауреат Нобелевской премии) стрептомицета, продуцирующего антибиотик широкого спектра действия (стрептомицин).

Топологию события можно описать следующим образом: мелкий инцидент в почвенной микрозоне с малым пространственно-временным масштабом (десяток микрометров – несколько суток) был быстро делокализован на планетарный масштаб и уже восемьдесят лет используется в медицине и других областях.

Этот пример также показывает мощь функционального потенциала микроорганизмов, однако роль антибиотиков в природе вопреки их названию (“против жизни”) скорее всего, связана как раз **с информационным поддержанием возможности жизни на системном уровне**. Для этого достаточно учесть возможность гормезиса – концентрационного эффекта, когда в зависимости от концентрации вещества меняется знак эффекта. Для природных местообитаний микроорганизмов характерны градиенты концентраций веществ. Поэтому “соседи“ могут располагаться рядом с продуцентом антибиотика на той дистанции, где они не пострадают и даже получат выгоду. Даже простые игровые модели (“камень-ножницы-бумага”) показывают, что наличие продуцента антибиотика не понижает, а повышает биоразнообразие. Поэтому антибиотики мы рассматриваем как **информбиотики** [10].

Здесь на примере антибиотиков мы выходим на чрезвычайно интересную для науки проблему роли **информационного фактора**. Для биолога знакомство с проблемой обычно завершается расчетом индекса Шеннона или разговорами о генетическом коде как программном детерминистском представлении экспрессии генов. Здесь специалисты по современным цифровым технологиям могут выразить биологам справедливый упрек.

Действительно, если уж мы применяем информационные индексы к микробным системам, то их следует рассматривать как **системы обработки информации**, т.е. **семиотические системы**, а, согласно самому краткому определению, «семиотика занимается всем, что может быть принято за знак». Под знаком понимается «что-то, что что-то значит для кого-то в каком-то контексте». Отсюда следует вывод, что все экосистемы, включая микробные, являются **коммуникационными системами** с обработкой информации, и у них есть свой язык [11]. Предполагается, что концепция языка позволит объединить синтаксический и семантический подходы в науках о жизни посредством сочетания формальных и смысловых аспектов информации [12].

Оценивая экологическую роль антибиотиков, мы можем представить, например, следующую микроскопическую картинку. В благоприятной почвенной микрозоне с наличием кусочка целлюлозы некая популяция завершает свой пир. Она является гидролитиком: своими экзоферментами поливает нерастворимый природный полимер и всасывает клеточной поверхностью (у микробов нет рта) легкодоступные сахара. При этом ближе к концу пира она образует антибиотик, который распространяется в среде с формированием концентрационного градиента. Одновременно в среде как открытой системе распространяется в силу диффузии и часть легкодоступного ресурса, который перехватывается микроорганизмами без способности к гидролизу полимеров.

Такие популяции с отсутствием внешних ферментов Г.А. Заварзин назвал диссипотрофами. В системном плане они не только не являются конкурентами гидролитикам, но, напротив, могут стимулировать скорость разложения полимера посредством снижения концентрации ресурса ниже порога концентрационного торможения.

Допустим теперь, что вблизи популяции гидролитика в водной пленке появляется подвижная клетка диссипотрофа. Она не направляется в пространство с летальной для нее концентрацией антибиотика, но останавливается в зоне, где антибиотик оказывает положительный эффект. Продуцент антибиотика тем временем спокойно завершает свой пир и может переходить в стадию покоя с последующей активной или пассивной миграцией в другое место.

Такой «простой» разговор на языке кооперации оказывается вполне удачным для двух условных объектов, причем автоматически обеспечивается оптимальное решение функциональной задачи разложения ресурса. Понятно, что при сильных внешних воздействиях (антибиотикотерапия в ме-

дицине, ксенобиотики в природе и т.д.) семиотические процессы прерываются, что ведет к сбою работы всей системы.

Природная микробная система построена на основе разнородных функциональных блоков (популяций) по кооперативной схеме (трофические взаимодействия) на основе термодинамических закономерностей для отношений продукт-субстрат. Потребление ресурсов микроорганизмами в любой природной среде с их ассимиляцией зависит от элементного состава самой микробной биомассы. Таким образом, процессы изменения содержания ресурсов в природном местообитании в результате жизнедеятельности микроорганизмов являются “зеркалом“, в котором отражается соотношение элементов в самой микробной биомассе как динамическом резервуаре. Поэтому экологическая стехиометрия как соотношение элементов (C:N:P) в биомассе и окружающей среде представляется важнейшей характеристикой природных систем.

Достаточно учесть только стехиометрические показатели, чтобы понять проблематичность некоторых политических лозунгов и планов (включая, Biden-Harris Plan) по климатической проблеме для поиска рецепта связывания углекислого газа почвой: для реализации подобных антисистемных планов надо обеспечить почвенную микробную систему огромным количеством других элементов. В первую очередь необходим азот удобрений, для получения которых потребуется колоссальное количество энергии.

Нам представляется, что для понимания значимости подобных глобальных проблем необходимы объективные научные оценки на основе системного взгляда с выделением реальных опасностей, включая определение “здоровья“ среды (где проблема углерода не цель, а один из частных результатов), разумный расчет “экологических услуг“ микроорганизмов по термодинамическим показателям (включая экологическую эксергию) и анализ рисков и решений в адаптационных иерархических циклах [13; 14].

С телеономичностью связаны и весьма содержательные аналогии между природными микробными сетями и, например, **блокчейном** и распределенными системами. Примером является реакция на окружающую среду и поддержание гомеостаза в алгоритме проверки работоспособности с контролем потребления ресурсов. Сети растут с удлинением блокчейна во времени за счет добавления дополнительных блоков и меняются с ростом числа узлов и при замене старых узлов на новые.

Кроме того, как для образования новой клетки требуется **репликация** ДНК, так и при присоединении нового узла сети к виртуальной машине происходит подобный процесс. Процессы воспроизводства и наследования проявляются во время события, называемого «hard fork», когда в ответ на давление отбора меняются параметры механизмов управления. Результатом является новая цепочка, называемая «дочерней», рост которой регулируется иначе, чем «материнская», но идентичная информация сохраняется в обеих цепях.

Функциональное сходство с биологическими клетками демонстрируют узлы распределенной виртуальной машины, которые содержат хранилище информации (память/жесткий диск), систему обработки информации, систему питания и защиту от внешней среды в виде физического корпуса и электрической изоляции. Аналогичные структуры представлены в микробных прокариотических клетках: нуклеиновые кислоты (ДНК/РНК) необходимы для хранения информации, рибосомы для обработки информации и клеточные мембраны для отделения от окружающей среды и производства энергии. Наконец, для блокчейнов реализован и работает под строгим контролем процесс латеральной (горизонтальной) передачи информации, который характерен для микробного мира [15]. Очевидно, что и в случае с загадочным для микробиологов блокчейном используются механизмы, которые по-своему применяют микроорганизмы.

Обычно предполагается, что способность к обучению и сложное поведение проявляются только у многоклеточных живых существ, наделенных нервной системой разной степени сложности. Тем не менее, сейчас появляются экспериментальные данные о том, что микроорганизмы являются разумными сенсомоторными агентами, способными решать, например, задачу лабиринта. Поэтому предлагается пересмотреть способности бактерий к обучению, проведя параллели между поведением прокариот и нейронным обучением. Ключевые реакции бактерий на изменения окружающей среды, например, направленное перемещение клетки в градиенте химических веществ (хемотаксис), возможны благодаря хеморецепторам, которые обнаруживают сигналы из окружающей среды для последующей обработки информации в сети передачи сигналов. Речь идет об интеллекте микроорганизмов как простых объектов “без головы” и нейронов. В последнее время появляется много работ на эту тему.

Иллюстрацией может служить микробное сообщество, в котором бактерии посредством зависимости экспрессии генов от популяционной плот-

ности (кворум-эффект) эмулируют **нейронную сеть** персептрона, способную распознавать 3x3-битные образы [16]. Предлагаются различные алгоритмы и протоколы создания "умных" бактерий на примере бактерий с обученным персептроном для решения сложной оптимизационной задачи по синтезу целевого продукта (полиоксигидробутират) из различных количеств мелассы, мочевины и пропионовой кислоты [17]. К сожалению, подобные работы по созданию суперэффективных "синтетических" микробных популяций для решения разных задач (от медицины до получения биотоплива и очистки среды обитания) обычно игнорируют очевидную возможность изменения экологической стратегии объекта после программирования и даже не упоминают проблему риска.

Настойчивое желание энтузиастов молекулярно-биологического подхода получить максимум генетической информации на первый взгляд нацелено на понимание сущности объектов микробного мира, использования их потенциала в биотехнологии и управления ими в природных местообитаниях. Такой подход, скорее всего, имеет фундаментальные ограничения и может даже привести к нежелательным результатам.

В самом деле, получение любой информации требует потребления энергии со снижением ее качества по уровню доступности [18]. Система должна удалять за пределы своих границ растущую энтропию со скоростью, превышающей скорость накопления внутренней информации. В силу второго закона термодинамики обеспечение локального роста информации возможно лишь за счет увеличения энтропии в окружающей среде.

В этом смысле, действительно, наша планета не убежище для жизни, а скорее квазиорганизм (в понимании С.Н.Виноградского или авторов концепции Геи), в котором множество подсистем разного уровня в ходе получения информации согласовывают друг с другом энергопотребление. Исследователи, которые заняты в основном накоплением молекулярно-генетической информации, пытаются выступить в роли классического демона Максвелла.

Как известно, демон Максвелла на основе непрерывного информационного анализа надеется навести порядок в системе, к которой он приставлен. Однако из комментариев Л. Сциларда, Л. Бриллюэна и Дж.Г. Беннета следует, что получение информации потребует затрат энергии с ростом энтропии выше порога управления порядком. К тому же демон Максвелла должен бороться с валом нарастающей информации и стирать ее, а это термодинамически необратимый процесс с ростом энтропии.

Примерно так в режиме "эффективного менеджера" необратимо удаляется информация с живого «жесткого диска» планеты, а надежды на спасение с помощью генно-инженерных организмов представляются наивными и рискованными. В этом случае создается избыточная информация посредством комбинаций из известных элементов, которая лишена позитивного смысла в рамках природоведческого контекста.

МИКРОБНОЕ РАЗНООБРАЗИЕ. СООТВЕТСТВИЕ ГЕНЕТИЧЕСКОЙ ИНФОРМАЦИИ СУЩНОСТИ ОБЪЕКТА

Описанием разнообразия микробного мира для создания "естественной" системы профессионально занимаются специалисты по систематике и таксономии (классификация, номенклатура и идентификация). По шутливому признанию авторитетного систематика (Коуэн С.Т.) работа в этой области выявляет в людях худшие черты, включая агрессивность, напыщенность, самоуверенность, раздражительность и инфантилизм в сочетании с забывчивостью. Поэтому мы осторожно и в самом общем виде обсудим вопросы, связанные со спорами о "естественной" системе микроорганизмов.

Проблема оценки разнообразия микроорганизмов на самом деле сводится к классическому вопросу: какие имена носят объекты? Анализом поставленной перед Адамом задачи занимались многие выдающиеся умы, среди которых можно упомянуть, в частности, Платона.

В идеале правильное имя объекта не только позволяет отличить его от всего иного, но и высвечивает смысл (функцию) этого объекта, что открывает канал для взаимодействия с ним. Автор статьи с ностальгией вспоминает свои студенческие эксперименты с клубеньковыми бактериями-ризобиями, поскольку в те времена число видов этих важнейших симбиотических азотфиксаторов (снабжение растений азотом из воздуха!) можно было показать на пальцах, а название вида полностью раскрывало смысл. Например, имя *Rhizobium phaseoli* практически однозначно определяло смысл популяции. В переводе с греческого *Rhizo* – это корень, суффикс – *bium (bia, bios)* – образ жизни, а *phaseoli* – фасоль. Ясно, что данная популяция живет в клубеньках на корнях бобового растения, а именно фасоли, которую она снабжает азотом из атмосферы. Отсюда и возможность разумного взаимодействия ("разговора") субъекта с объектом, включая применение

данной популяции в качестве микробного удобрения (только для фасоли, но не сои или клевера!).

Теперь семейство ризобий включает огромное число видов (соответственно, налицо информационный " взрыв") с полной ревизией и включением объектов, которые совсем не связаны с симбиозами с бобовыми растениями или даже являются нежелательными патогенами.

Причина перманентной революционной ревизии с потерей смысла в этом случае, как и во многих других микробных "коллекциях марок", – результат, как это не парадоксально, научного прогресса в последние 20-30 лет. Для понимания ситуации попробуем предельно кратко охарактеризовать некоторые "плоды" внедрения молекулярно-генетических методов и цифровизации в микробиологию, которая как раз и стала основным полигоном для поиска "прорывных" решений.

В самом общем виде это рассказ о торжестве крайнего редукционизма в создании новой картины микробного мира. "Естественная" система организмов в виде Дерева Жизни (здесь снова вспоминается Адам) — это система на основе происхождения объектов (родство, филогения). Родство определяется по информации, которая содержится в генах как некая постоянная эстафетная палочка для передачи от предка к потомку. Для этого используются консервативные гены, которые обеспечивают процессы самовоспроизведения, т.е. связаны с "домашним хозяйством" клетки (например, 16S рРНК). Гены, обеспечивающие взаимодействие с внешней средой, при таком подходе создают только информационный шум и исключаются из рассмотрения, хотя на самом деле именно "разговор" с окружающей средой в основном определяет сущность, т.е. смысл и возможность существования организма.

Еще в 1952 году до молекулярно-биологической революции против мечты о построении системы на основе родства резко выступил С.Н. Виноградский, который отрицал значимость филогении и призывал к созданию простых, рациональных и удобных классификаций микроорганизмов. Заметим, что на самом деле "естественные" классификации объектов совсем не обязательно должны базироваться на "родстве". Пример тому периодическая система элементов Д.И. Менделеева, где само положение объекта в таблице указывает на его основные характеристики.

Однако микробиология пошла другим путем. Современные методы анализа генетических последовательностей (секвенирование) быстро накапливали гигантскую информацию, которая позволила исследователям играть в увлекательную компьютерную игру по определению места микроорганизма на Дереве Жизни. Числовая информация из генетического кода, отражающая положение четырех букв (А, Т, Г, Ц), заменила сущность объекта. Геноцентризм привел сейчас к гигантской информационной перегрузке, постоянным ревизиям и малоуспешным попыткам найти связь топологии с экологией.

Полвека назад Г.А. Заварзин [19] показал, что пространство логических возможностей фенотипических (функциональных) признаков содержит очень мало запрещенных комбинаций (топология не дерева, а сетки). Возможность такой комбинаторики, как уже теперь в полной мере осознано, определяется механизмами не вертикального (от предка к потомку), а горизонтального (латерального) переноса генов в природной среде между разными микроорганизмами. Здесь можно вспомнить парадокс Тесея с кораблем, в котором постепенно в ходе ремонтов меняют части и возникает вопрос о том, остается ли он прежним сакральным объектом. В книге Г.А. Заварзина есть эпиграф. Это строчки из В.Шекспира: "Все зная, знаешь только имена... " Теперь вместо последнего слова мы можем, конечно, поставить "номера", т.е. числа.

Дело дошло уже до создания автоматической системы генерации множества новых имен бактерий и архей с мощностью около 1 млн. элементов [20]. На этом фоне более интересным представляется математический подход с полным отказом от таксономического видового описания микроорганизмов как неудачной идеи, которая навязывает объектам чуждую им структуру [21].

Изменилось до неузнаваемости и Дерево Жизни. Вместо привычных ветвей растений и животных в качестве основных стволов (эти множества высокого иерархического уровня теперь именуют не царствами или империями, а доменами) представлены Археи, Бактерии и Эукариоты. Если ранее понимали и принимали принципиальную разницу между бактериями (нет оформленного ядра в клетке) и "ядерными" эукариотами (от дрожжей и амеб до растений и животных), то Археи не просто появились здесь, но и стали ключевой особенностью Дерева Жизни именно благодаря молекулярно-генетическим методам. Многие из них были хорошо известны и ранее (метанобразующие и "любители" экстремальных местообитаний), по морфологическим и функциональным характеристикам мало отличались от других бактерий и были представлены среди них в определителях.

Идет постоянная перестройка некоторых базовых схем вплоть до курьезов, которые следуют из

самых фундаментальных обобщений вроде Дерева Жизни с тремя доменами. Для иллюстрации снова вернемся к нашему примеру с получением селитры. В микробных процессах азотного цикла в компостной куче участвуют популяции, которые выполняют одну и ту же функциональную задачу (реакцию), но по современным генетическим данным относятся к разным доменам бактерий и архей. Таким образом, они различаются на более фундаментальном уровне между собой по сравнению с парой дрожжи и человек, которые на этом условном фоне выглядят почти близнецами из одного и того же домена (эукариоты).

Правомерность такого взгляда трудно оправдать даже из педагогических соображений. Сейчас некоторые филогенетики говорят уже о двух основных доменах, где эукариотам вообще нет почетного места (только роль ветки из ствола архей). Правда, есть и специалисты, которые размышляют о том, не пора ли остановиться, а время, усилия и деньги потратить на что-то другое. Так, недавно руководитель ведущего центра с передовыми аналитическими платформами и элементами автоматизации Ной Фиерер (Noah Fierer) попросил в своем твиттере объяснить ему, зачем почвенная бактерия (*Clostridium tetani*) осуществляет сверхсинтез нейротоксина (до 5% сухой массы).

ЗАКЛЮЧЕНИЕ

В этой работе автору хотелось бы не столько дать ответы, сколько поставить некоторые вопросы, которые для многих исследователей пока являются бесспорными истинами. Секвенирование полных геномов и метагеномов или создание крупномасштабных сетей экологического мониторинга, конечно, характеризуют научный прогресс, но наивно ожидать, что для понимания достаточно накопить как можно больше информации о мире. Примером служат не слишком утешительные результаты по секвенированию генома человека. Одним из сюрпризов было относительно небольшое количество генов (примерно 22 000). Очевидно, что каталогизация генов сама по себе имеет ограниченное значение для объяснения жизненных процессов. Трудно представить, как исходная информация в коде генома (пусть даже миллиард битов) может определить всю структуру и организацию организма, только мозг которого содержит 10^{12} нейронов с числом связей на уровне 10^{16}.

Предполагается, что чем больше данных дают новые технологии, тем лучше, но история напоминает нам об эффективности альтернативных и более простых подходов, начиная от классической “бритвы“ Оккама. Пока же многие микробиологи верят в то, что цифровизация молекулярно-генетических данных является преобладающим направлением развития науки (mainstream) с полным пониманием объектов. Число самих объектов при этом стремительно нарастает.

Получается, что для понимания сущности микроорганизмов огромного массива имеющейся генетической информации по-прежнему не хватает. Даже в случаях с полностью прочитанными геномами (например, кишечная палочка) выясняется, что треть или даже половина генов несут неизвестные функции. При горизонтальном переносе генов легче всего переносятся как раз функциональные гены, связанные с метаболизмом и взаимодействием с окружающей средой.

Во многом загадкой остаются эпигенетические (“над-генетика”) механизмы изменения активности генов без изменения самого генетического текста, когда внешние сигналы включают или выключают отдельные гены. Если ген может находиться в одном из двух состояний, объем информации в системе существенно возрастает (для набора из N генов 2^N различных состояний). Эпигеном в этом смысле является вторым кодом. Эпигенетические изменения могут передаваться по наследству, но, как полагают, они обратимы, что предполагает возможность создания эпигенетических “таблеток“.

Эти и другие обстоятельства заставляют исследователей искать выход из тупика путем подключения к генетической информации данных других подходов, в названии которых присутствует греческий суффикс “-ом“ (“имеющий природу“). Характеристикой РНК занимается транскриптомика, белками – протеомика, а мелкими метаболитами (антибиотики, гормоны и другие соединения) – метаболомика. Для этих и других “омиков“ создаются гигантские базы данных с учетными записями. Например, для метаболитов MetaboCard включает химическую характеристику и взаимодействие с лекарствами. И в этом случае мы отмечаем лавинообразный рост информации (уже не только генетической), которую энтузиасты надеются переработать с помощью машинного обучения [22].

Завершая статью, еще раз отметим, что прогресс современных научных технологий, включая в первую очередь цифровизацию классификации микроорганизмов, принципиально изменил научную парадигму микробиологии. Многие микробиологи даже не заметили подмену объекта исследования в своей науке: вместо микробных клеток, популяций

и сообществ акцент исследований был перенесен на гены с надеждой, что математика позволит получить правильное понимание места популяции на дереве жизни и в экосистеме. Оказалось, что это не совсем так, а огромные информационные массивы данных даже после надлежащей обработки часто ведут к тривиальным выводам или тупику.

Как известно, наука развивается в ходе смены парадигм (Томас Кун) [23]. Несомненно, математические методы при понимании их возможностей и ограничений, включая и возможность злоупотребления, представляют большой интерес для микробиологов. Однако удивительный природный мир микроорганизмов, как нам представляется, гораздо интереснее тех или иных вариантов цифрового прокрустового ложа и по выражению микробиолога Томаса Брока не поддается тотальному контролю и подчинению.

Мир, в котором мы живем, постоянно преподносит нам сюрпризы, особенно если мы на основе своих трудов начинаем претендовать на что-то фундаментальное. Возможно, что надежда на успешное свертывание big data цифровыми технологиями в компактное знание вообще является наивной и нам следует больше уделять внимания развертыванию представлений на основе разных моделей и подходов. Микробиологи пока ошеломлены огромным количеством данных, которые можно получить современными молекулярно-генетическими методами из мира природы. Гигантские базы данных запускаются в анализ с помощью машинного обучения и других индуктивных подходов в расчете, что корреляций и алгоритмов будет достаточно для понимания.

В этой связи автор вспоминает выступления и работы руководителя межфакультетской Лаборатории статистических методов МГУ профессора В.В. Налимова, который скептически относился к прогнозированию как серьезному делу в силу “омнипотентности” факторов и “контринтуитивного” поведения природных систем: можно лишь обсуждать динамику сложной системы пока не произошли события, которые мы не можем предвидеть.

Для иллюстрации возьмем два известных примера из недавней истории. В 1912 году на Аляске произошло извержение вулкана Катмай, что сопровождалось, конечно, выбросом парниковых газов, но привело к сильному похолоданию в Европе и Америке в результате увеличения массы аэрозоля в стратосфере. На станции в Павловске (Петербург) солнечная радиация в течение более полугода была ниже нормы на 35%. Другой пример – “Событие Кэррингтона“ (28 августа – 2 сентября 1859 года), когда в результате мощной геомагнитной бури были разрушены телеграфные сети по всей Европе и Северной Америке. В.В. Налимов также настойчиво подчеркивал глубокий смысл теоремы Гёделя о неполноте логических систем при сравнении человеческого мышления и алгоритмов компьютерного искусственного интеллекта.

А завершить обзор злободневной проблемы цифровой микробиологии, которая все чаще использует алгоритмы машинного обучения и нейросети, можно написанными 150 лет назад строчками стихотворения Владимира Соловьева:

“Природа с красоты своей
Покрова снять не позволяет,
И ты машинами не вынудишь у ней,
Чего твой дух не угадает“.

СПИСОК ЛИТЕРАТУРЫ

1. Gorlenko M.V., Terekhov A.S., Marchenko S.A., Marchenko A.I., Vorobev A.V., Kozhevin P.A. Indication of soil contamination with polycyclic aromatic hydrocarbons by the functional response of soil microbial complex // Moscow University Soil Science Bulletin. 2003. V.58.N1. P.46-51.
2. Заварзин Г.А., Колотилова Н.Н. Введение в природоведческую микробиологию. М.: Книжный дом "Университет", 2001.- 256 с.
3. Кожевин П.А., Кочкина Г.А., Кириллова Н.П., Градова Н.Б., Зайцев С.А., Гаджиева В.И. Загрязнение почв дрожжами // Почвоведение.1982. N11. С.67-71.
4. Кожевин П.А., Полянская Л.М., Лукин С.А., Зайцев С.А., Гузев В.С., Левин С.В. Микробное загрязнение почв // Микроорганизмы и охрана почв. М.: Изд-во МГУ, 1989. С.151-162.
5. Кожевин П.А., Анисимов А.И., Правдин В.Г. Биотехнологический путь земледелия (теория и практика) // Белгородский агромир. 2005.N2. С.1-14.
6. Flemming, HC., Wuertz, S. Bacteria and archaea on Earth and their abundance in biofilms // Nat. Rev. Microbiol. 2019. 17, pp.247–260. URL: https://doi.org/10.1038/s41579-019-0158-9 (дата обращения: 09.10.2022).
7. Bergelson J., Kreitman M., Petrov D., Sanchez A.,Tikhonov M. Functional biology in its natural context: A search

for emergent simplicity // eLife .2021. 10:e67646. URL: https://doi.org/10.7554/eLife.67646 (дата обращения: 09.10.2022).

8. Виноградский С.Н. О роли микробов в общем круговороте жизни // Хемосинтез/ Ред. Иванов М.В. М.: Наука. 1989. С. 22-31.

9. Gorshkov V.G., Makarieva A.M., Gorshkov V.V. Revising the fundamentals of ecological knowledge: the biota-environment interaction //Ecological Complexity. 2004. 1. pp.17-36. URL: https://doi.org/10.1016/j.ecocom.2003.09.002 (дата обращения: 09.10.2022).

10. Kozhevin P.A., Vinogradova K.A., Bulgakova V.G. Natural functions of antibiotics as “informbiotics” // Moscow University Soil Science Bulletin. 2014. v.69. 3. pp.93-98. URL: https://doi.org/10.3103/S014768741403003X (дата обращения: 09.10.2022).

11. Nielsen S. N. Towards an ecosystem semiotics // Ecological Complexity. 2007. 4(3), pp. 93–101. URL: https://doi.org/10.1016/J.ECOCOM.2007.04.001 (дата обращения: 09.10.2022).

12. Tournebize R., Gaucherel C. Language: A fresh concept to integrate syntactic and semantic information in life sciences // Biosystems. 2017. v.160. pp. 1-9. URL: https://doi.org/10.1016/j.biosystems. 2017.07.005 (дата обращения: 09.10.2022).

13. Kozhevin P.A., Zhebrak I.S., Maslova O.A. The role of soil microorganisms in environmental and food security // Moscow Univ. Soil Sci. Bull. 2017.72, pp.191–198. URL: https://doi.org/10.3103/S0147687417050039 (дата обращения: 09.10.2022).

14. Emer N. R., Kostina N. V., Netrusov A. I., Zhebrak I. S., Kozhevin P. A. Analysis of the State of the Soil Microbial System under Prolonged Anthropogenic Load // Moscow University Soil Science Bulletin. 2019., 74(4), pp. 187-192. URL: https://doi.org/10.3103/S0147687419040045 (дата обращения: 09.10.2022).

15. Abramov O., Bebell K.L., Mojzsis S.J. Emergent Bioanalogous Properties of Blockchain-based Distributed Systems // Orig. Life Evol. Biosph .2021. 51. Pp. 131–165. URL: https://doi.org/10.1007/s11084-021-09608-1 (дата обращения: 09.10.2022).

16. Li X., Rizik L., Kravchik V. et al. Synthetic neural-like computing in microbial consortia for pattern recognition // Nat. Commun. 2021. 12, p.3139. URL: https://doi.org/10.1038/s41467-021-23336-0 (дата обращения: 09.10.2022).

17. Gargantilla Becerra A., Gutiérrez M., Lahoz-Beltra R. Computing within bacteria: Programming of bacterial behavior by means of a plasmid encoding a perceptron neural network // Biosystems. 2022.v.213.p.104608. URL: https://doi.org/10.1016/j.biosystems.2022.104608 (дата обращения: 09.10.2022).

18. Rodríguez R. A., Riera R., Delgado J. D. Ecology: Science or philately? An interdisciplinary analysis of sustainability by exploring if it is possible to get more and more information by reducing collateral environmental damages // Science of the Total Environment. 2017. v. 596. pp. 43-52. URL: https://doi.org/10.1016/j.scitotenv.2017.04.053 (дата обращения: 09.10.2022).

19. Заварзин Г.А. Фенотипическая систематика бактерий: Пространство логических возможностей (Изд.2-е, доп.). М.: ЛЕНАНД. 2018.-152 с.

20. Pallen M. J., Telatin A., Oren A. The next million names for Archaea and Bacteria //Trends in Microbiology. 2021. v. 29. №. 4. pp. 289-298. URL: https://doi.org/10.1016/j.tim.2020.10.009 (дата обращения: 09.10.2022).

21. Tikhonov M. Theoretical ecology without species //Bull. Am. Phys. Soc. 2016. v. 61. pp.1-13. URL: http://archive.ymsc.tsinghua.edu.cn/pacm_download/188/8250-TheoreticalEcology.pdf (дата обращения: 09.10.2022).

22. McElhinney J. M. W. R. et al. Interfacing Machine Learning and Microbial Omics: A Promising Means to Address Environmental Challenges //Frontiers in Microbiology. 2022. v. 13. pp. 851450-851450. URL: https://www.frontiersin.org/articles/10.3389/fmicb.2022.851450/full (дата обращения: 09.10.2022).

23. Кун Т. Структура научных революций / Пер. И.З. Налетова. – М.: Прогресс, 1977.

УДК 004.94

Применение сетей Петри при моделировании атак на системы АСУ ТП

V.Yu. Shevtsov, D.I. Pravikov

The Application of Petri Nets for Modeling Attacks on ICS

Abstract. *. In this paper, we present a method of modeling attack on ICS that is based on extended Petri nets. This approach allows to describe object of automatisation. It's possible through changing positions. The model has been created for a pumping station. A typical control scheme of a pumping station and scenarios of its operation in case of various attacks are given. The CPN Tools software is being used for model realizing.*

Keywords: *Petri net, subclass of Petri net, industrial control system (ICS), pumping station, programmable logic controller (PLC), Supervisory Control And Data Acquisition (SCADA system), decision support system (DSS), functional safety.*

В.Ю. Шевцов[1]
Д.И. Правиков[2]
[1]Аспирант, инженер кафедры комплексной безопасности критически важных объектов РГУ нефти и газа (НИУ) имени И.М. Губкина.
E-mail: vadim94.d@mail.ru
[2]Кандидат технических наук, заведующий кафедрой комплексной безопасности критически важных объектов РГУ нефти и газа (НИУ) имени И.М. Губкина.
E-mail: dip@gubkin.pro

Аннотация. *В статье предлагается метод моделирования атак на системы АСУ ТП на базе расширенного аппарата сетей Петри. Данный подход позволяет подробно описать процесс объекта автоматизации, благодаря поддержке изменений состояний. Модель выполнена для нефтеперекачивающей станции. Описана типовая схема управления нефтеперекачивающей станции, сценарии ее работы в случае различных атак злоумышленника. Для реализации модели используется программное обеспечение CPN Tools.*

Ключевые слова: *сеть Петри, подкласс сети Петри, автоматизированная система управления технологическим процессом (АСУ ТП), нефтеперекачивающая станция (НПС), программируемый логический контроллер (ПЛК), единая система диспетчерского управления (SCADA-система), система поддержки принятия решений (СППР), функциональная безопасность.*

ВВЕДЕНИЕ

Информационная безопасность (ИБ) автоматизированных систем управления технологическими процессами (АСУ ТП) продолжает оставаться актуальной проблемой, ввиду высокого уровня значимости таких систем и интереса со стороны злоумышленников [1]. При этом, даже не смотря на наличие систем защиты отдельных подсистем, функциональная безопасность всей системы может оставаться под угрозой.

Для понимания того, каким образом необходимо обеспечивать безопасность АСУ ТП, важно проводить моделирование различных сценариев работы таких систем. Но текущие исследования обычно рассматривают типовые АСУ ТП без привязки к специфичным процессам конкретного производства [2-6].

В данной работе за основу моделирования взят аппарат сетей Петри, т.к. он позволяет показать изменение состояний системы, а благодаря расширениям базового метода (использованы функциональные, цветные, ингибиторные, иерархические подклассы сетей Петри) возможно подробное описание АСУ ТП.

Для реализации модели АСУ ТП нефтеперекачивающей станции используется свободно распространяемое программное обеспечение CPN Tools версии 4.0.1. Оно предоставляет широкие возможности и гибкость при построении сетей Петри.

Статья состоит из следующих частей. В первом разделе рассматривается типовая схема управления нефтеперекачивающей станции в разрезе АСУ ТП, для которой будет разработана модель. Во втором разделе дается описание сети Петри для целевой системы на основе программной реализации в CPN Tools. В третьем разделе представлены возможные сценарии работы нефтеперекачивающей станции в случае реализации угроз злоумышленником на основе разработанной модели.

ТИПОВАЯ СХЕМА УПРАВЛЕНИЯ НЕФТЕПЕРЕКАЧИВАЮЩЕЙ СТАНЦИИ

Нефтеперекачивающая станция – комплекс раз-

личного оборудования и сооружений, который позволяет производить эффективную транспортировку нефтепродуктов по нефтепроводам.

В общем виде схема управления нефтеперекачивающей станцией представлена на рисунке 1. Она состоит из следующих элементов:

- автоматизированное рабочее место оператора (АРМ);
- система поддержки принятия решений (СППР);
- единая система диспетчерского управления (SCADA-система);
- программируемый логический контроллер (ПЛК);
- узел регулирования давления (УРД);
- входной и выходной манометры (датчики входного и выходного давления).

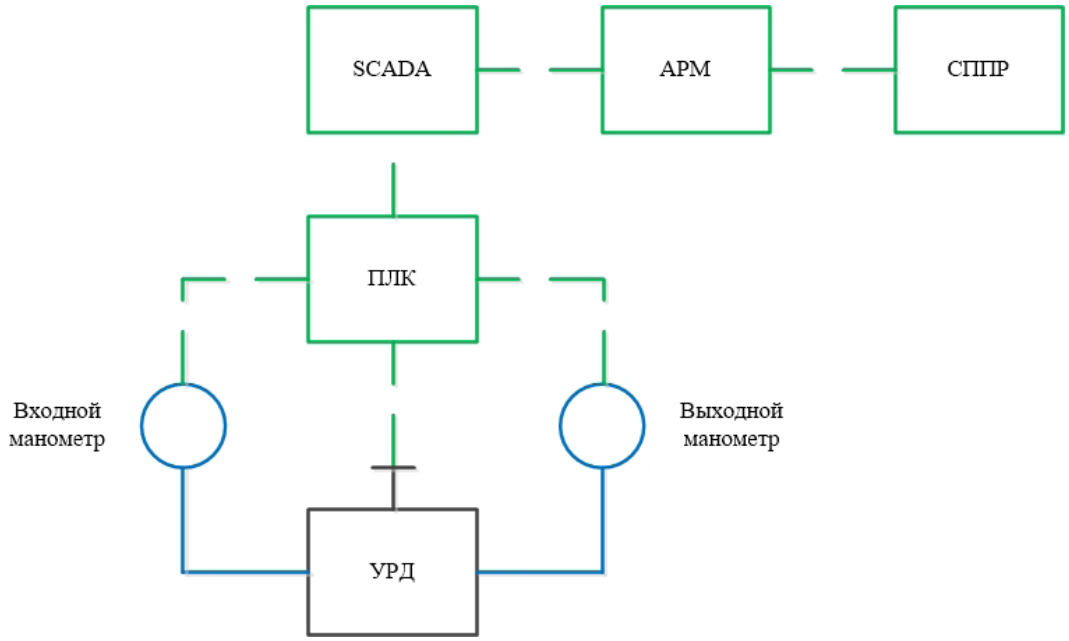

Рис. 1. Типовая схема управления нефтеперекачивающей станции

При нормальном режиме работы значения давления на манометрах находятся в определенном уровне допустимых значений, ручного изменения состояния УРД не требуется.

В случае выхода значений давления на датчиках за пределы допустимых оператор отправляет соответствующий сигнал на УРД, чтобы нормализовать давление в системе. Также может сработать система противоаварийной защиты и остановить НПС.

Для рассматриваемой НПС возможны следующие атаки:

- Атака на АРМ оператора;
- Атака на SCADA-систему;
- Атака на датчики (входного и выходного давления);
- Атака на ПЛК с заменой данных, поступивших от датчиков;
- Атака на ПЛК с отправкой данных на УРД.

При этом данные атаки направлены либо на открытие регулятора (в дальнейшем происходит остановка НПС или снижение надежности системы), либо на его закрытие (в дальнейшем происходит остановка НПС или снижение расхода).

МОДЕЛЬ НЕФТЕПЕРЕКАЧИВАЮЩЕЙ СТАНЦИИ НА ОСНОВЕ СЕТИ ПЕТРИ

Сеть Петри, выполняющая моделирование НПС, включает в себя 6 подсетей, соответствующих элементам схемы управления НПС (рисунок 2):

- ***2 подсети датчиков давления (Manometer1 и Manometer2):*** входные позиции атак на датчики (Attack Sensor1, Attack Sensor2); выходные позиции получения данных от датчиков (Get Sensor1 Data, Get Sensor2 Data).
- ***Подсеть ПЛК (PLC):*** входные позиции получения данных от датчиков (Get Sensor1 Data, Get Sensor2 Data), атака на ПЛК с заменой данных датчиков (Attack1 PLC, Attack2 PLC), атака с отправкой данных на УРД (Attack3 PLC); выходные позиции получения данных от PLC и получение сигнала управления (Get PLC data, Send rule signal).
- ***Подсеть SCADA (SCADA):*** входные позиции получения данных от ПЛК и отправки сигнала на SCADA-систему (Get PLC data, Send signal to SCADA); выходные позиции получения данных и отправки

данных на ПЛК (Get data, Send signal to SCADA).

• ***Подсеть АРМ оператора (Operator's PC):*** входные позиции получения данных и атаки на АРМ оператора (Get data, Attack operator's PC); выходная позиция отправки сигнала на SCADA (Send signal to SCADA).

• ***Подсеть УРД (Rule_Mechanism):*** входная позиция получения сигнала управления (Get rule signal); выходные позиции закрытия и открытия регулятора (Close regulator, Open regulator).

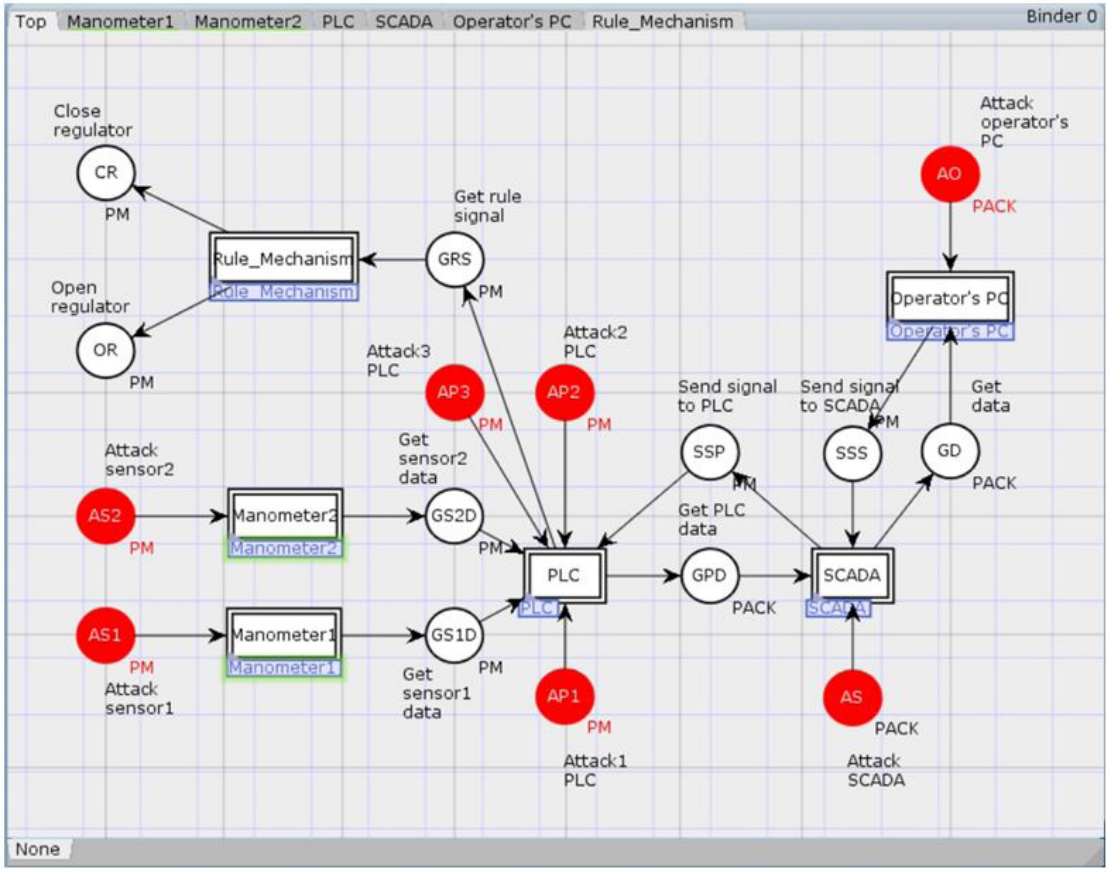

Рис. 2. Основная сеть Петри модели нефтеперекачивающей станции

Данная модель использует следующие объявления:

colset pm = with NP1 | LP1 | HP1 | NP2 | LP2 | HP2 | RP1 | RP2 | RP3 | PLC;

colset I = int;

colset PM = product pm * I;

var p1 : pm;

var i : I;

colset PACK = list PM;

var pack : PACK;

var pack1 : PACK;

var pack2 : PACK;

Позиции, имеющие цвет PM описываются двумя параметрами: pm – информация датчика/ПЛК, I – счетчик цикла. Для цвета PACK – список, содержащий несколько значений PM для последующей обработки.

Закрашенные позиции соответствуют атакам злоумышленника. В случае наличия фишки в одной из таких позиций произойдет вредоносное воздействие на систему, в результате чего сеть завершит свое выполнение в одной из конечных позиций: открытие регулятора (Open regulator) или закрытие регулятора (Close regulator).

СЦЕНАРИИ РАБОТЫ НПС ПРИ РЕАЛИЗАЦИИ УГРОЗ ЗЛОУМЫШЛЕННИКОМ

Рассмотрим подробнее сценарии проведения атак злоумышленником на НПС, озвученные в первой части.

• ***Атака на АРМ оператора*** (позиции внутри подсети: система поддержки и принятия решений: Decision support system; анализ данных – Analysis data), ***атака на SCADA-систему*** (позиции внутри подсети: отправка данных – Send data; получение сигнала оператора – Get operator's signal) представлены на рисунке 3.

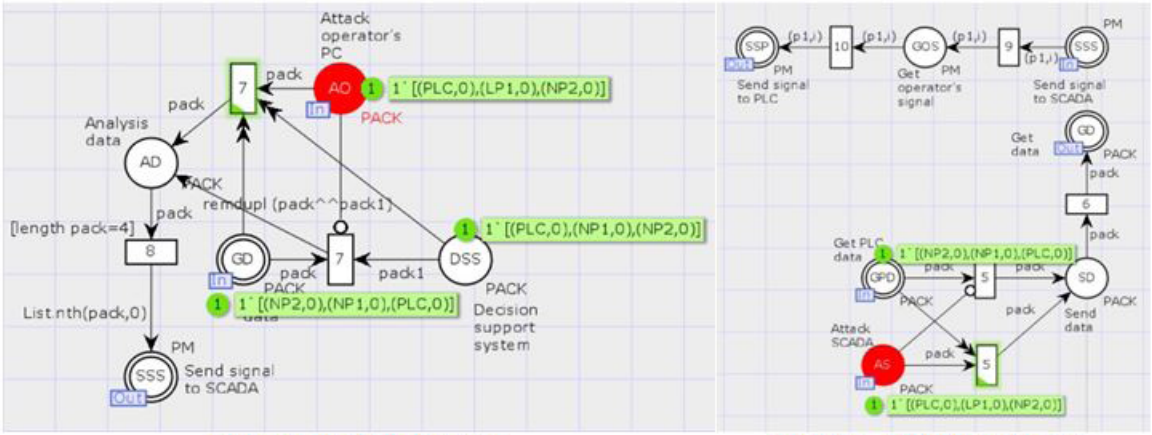

Рис. 3. Сети Петри, иллюстрирующие первую и вторую атаки

Особенность атак на автоматизированное рабочее место оператора и SCADA-систему в том, что эти объекты часто работают на базе операционных систем общего назначения и могут использовать распространенные программные решения (например СУБД). Поэтому для нарушения производственного процесса самым сложным для злоумышленника будет разобраться в специализированном ПО. В таком случае, как видно на рисунке 3, происходит блокирование передачи и сброс реальных данных из смежных объектов АСУ ТП (для этого в сети Петри использованы ингибиторные дуги и дуги сброса соответственно). Разрешенным переходом является переход из позиции атак со сбросом реальных данных (данный переход выделен на рисунке).

• ***Атака на датчики*** (позиции внутри подсети: считывание входного/выходного давления – Reading correct input/output pressure; отправка данных входного давления – Send manometer1 data) представлена на рисунке 4.

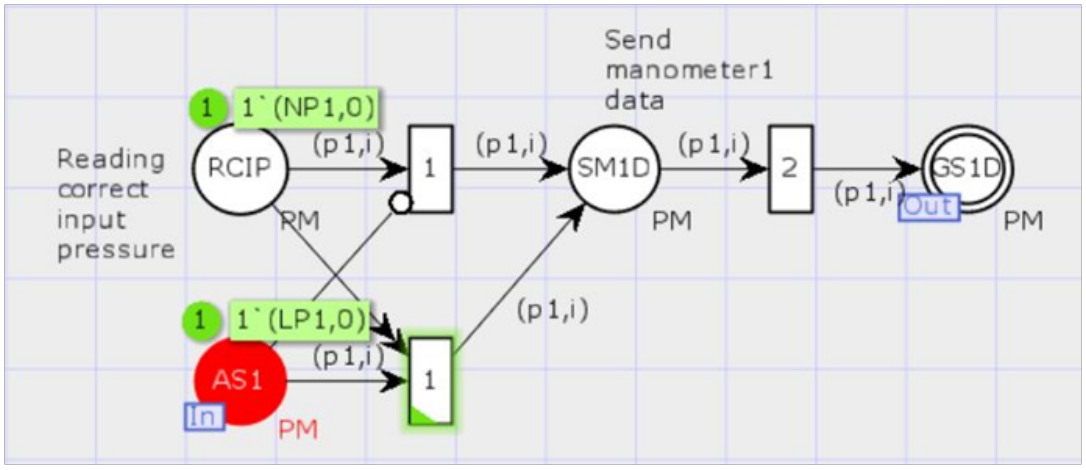

Рис. 4. Сеть Петри, иллюстрирующая третью атаку

Атака на датчики (входного и выходного давления) позволяет злоумышленнику точечным образом привести НПС в аварийное состояние, затратив минимум усилий. Оператор может не сразу понять, что датчик отправляет ложные значения, и в итоге отправит неправильные команды управления на УРД. Алгоритм атаки прост: реальные данные датчика блокируются и подменяются критическими.

• ***Атака на ПЛК с заменой данных, поступивших от датчиков, атака на ПЛК с отправкой данных на УРД*** (позиции внутри подсети: отправка полученных данных – Send getting data; получение сигнала от SCADA-системы – Get SCADA signal; отправка сигнала управления – Send rule signal) представлены на рисунке 5.

Данные атаки нацелены на программируемый логический контроллер, что требует от злоумышленника определенных знаний об атакуемом объекте. При этом в первом случае происходит атака, аналогичная третьей, при которой необходимо иметь

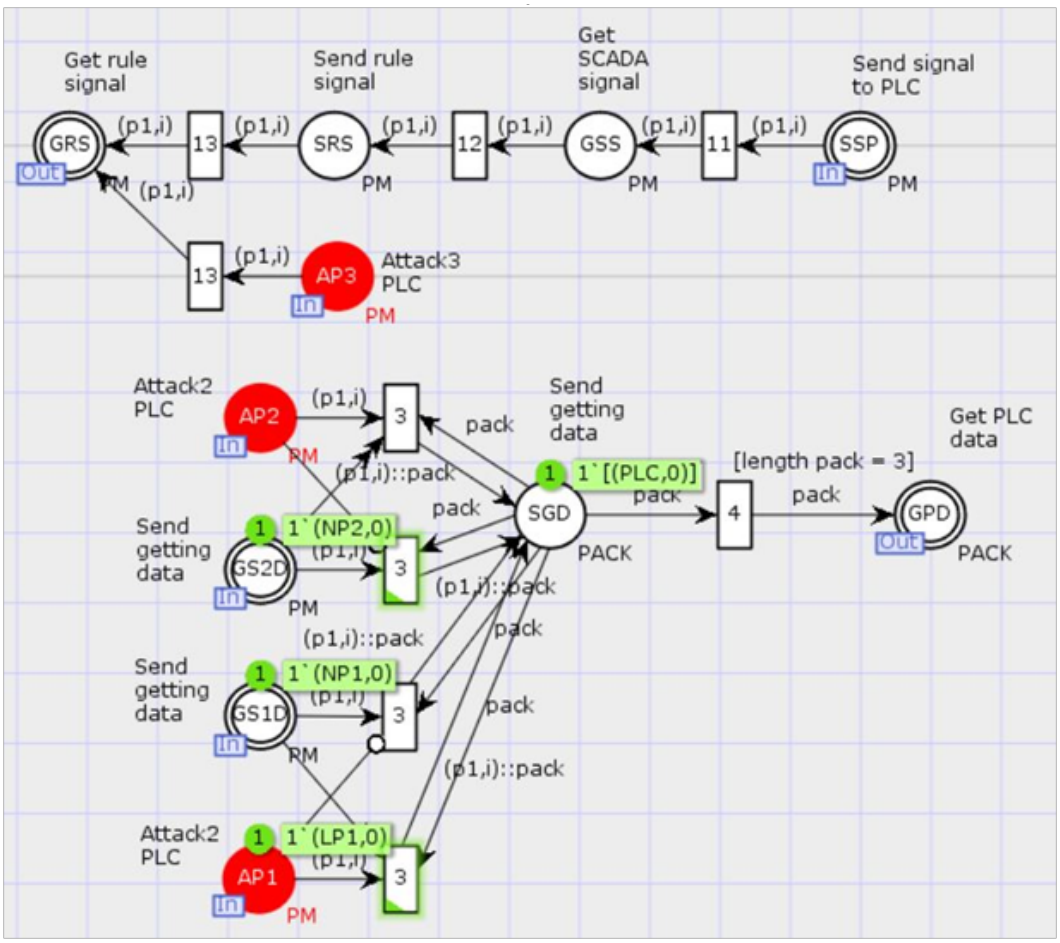

Рис. 5. Сеть Петри, иллюстрирующая четвертую и пятую атаки

представление о формате принимаемых и отправляемых данных уровня давления (на уровне устройств и сети). Во втором случае, злоумышленник должен обладать сведениями о самом технологическом процессе, чтобы успешно отправить управляющий сигнал с программируемого логического контроллера на узел регулирования давления.

ВЫВОДЫ

Моделирование атак на системы АСУ ТП с использованием различных подклассов сетей Петри позволяет алгоритмически описать входящие в их состав сложные объекты. При этом сценарии функционирования АСУ ТП легко проследить, что позволяет определить уязвимые места системы, а также предпочтительные цели для злоумышленника.

Построение имитационных моделей на основе сетей Петри дает не только подробное описание рассматриваемых систем, но и позволяет оценить анализируемый объект в целом при его нахождении в различных состояниях.

Приведенная модель нефтеперекачивающей станции является базовой, на основе которой планируется построить более сложную сеть, демонстрирующую реализацию более специфичных угроз и уязвимостей, а также использовать полученный опыт при создании других моделей АСУ ТП.

СПИСОК ЛИТЕРАТУРЫ

1. Реагирование на инциденты: аналитический отчет 2020 // securelist.ru : Блог Securelist – отчеты «Лаборатории Касперского» об угрозах информационной безопасности, анализ угроз, реверс-инжиниринг вирусов и статистика. 13.09.2021. URL: https://securelist.ru/incident-response-analyst-report-2020/103591/
2. Машкина И.В., Гарипов И.Р.. Разработка EPC-моделей угроз нарушения информационной безопасности автоматизированной системы управления технологическими процессами // Безопасность информационных

технологий. 2019. Т. 26. № 4. С. 6–20.

3. Васильев В.И., Вульфин А.М., Кириллова А.Д. Анализ и управление рисками информационной безопасности АСУ ТП на основе когнитивного моделирования. Моделирование, оптимизация и информационные технологии. 2022. №10(2).
4. Римша А.С. Метод и алгоритмы управления рисками информационной безопасности АСУ ТП критических инфраструктур. [Текст] : дис. … канд. техн. наук : 2.3.6 / Римша Андрей Сергеевич. – СПб., 2021. – 234 с.
5. Лившиц И.И. Модели и методы аудита информационной безопасности интегрированных систем управления сложными промышленными объектами. [Текст] : дис. … д-р техн. наук : 05.13.19 / Лившиц Илья Иосифович. – СПб., 2018. – 407 с.
6. Язов Ю.К., Анищенко А.В. Сети Петри-Маркова и их применение для моделирования процессов реализации угроз безопасности информации в информационных системах. Монография. – Воронеж, Кварта, 2020. – 173 с.

УДК: 004.8

Исследования и разработки в области искусственного интеллекта: достижения, выводы, перспективы

А.А. Рязанова
Ведущий специалист научно-образовательного центра социальной аналитики РГСУ, вице-президент Ассоциации РКЦФА по международной деятельности.
E-mail: a.ryazanova@c3da.org

A.A. Ryazanova

Research and Development in the Field of Artificial Intelligence: Achievements, Conclusions, Prospects

Abstract. *The article is devoted to the consideration of significant aspects and directions of development, results achieved, current trends and prospects in the field of artificial intelligence. The dynamics of performance indicators of new AI technologies in the field of image recognition, natural language processing, reinforcement learning, deep neural networks is presented. The ethical aspects of the development and application of artificial intelligence technologies, as well as the issues of financing projects in the field of AI, are considered.*

Keywords: *artificial intelligence, machine learning, deep learning, computer vision, semantic artificial intelligence, neural network model, reinforcement learning, ethics of artificial intelligence.*

Аннотация. *Статья посвящена рассмотрению значимых аспектов и направлений развития, достигнутых результатов, актуальных тенденций и перспектив в области искусственного интеллекта. Представлена динамика показателей эффективности новых технологий ИИ в области распознавания изображений, обработки естественного языка, обучения с подкреплением, глубинных нейронных сетей. Рассмотрены этические аспекты развития и применения технологий искусственного интеллекта, а также вопросы финансирования проектов в области ИИ.*

Ключевые слова: *искусственный интеллект, машинное обучение, глубокое обучение, компьютерное зрение, семантический искусственный интеллект, нейросетевая модель, обучение с подкреплением, этика искусственного интеллекта.*

ВВЕДЕНИЕ

В области искусственного интеллекта (ИИ), понимаемого как совокупность алгоритмов и инструментов, разрабатываемых с целью решения трудоемких управленческих, прогностических, творческих и многих других задач, которые обыкновенно решаются живым человеческим интеллектом, в последние годы происходят ощутимые количественные и качественные изменения.

Данные изменения отражают не только весьма активные процессы накопления полезного эмпирического опыта, но и появление прецедентов, связанных с признанием алгоритма искусственного интеллекта, разумеется, не вполне оправданным, в качестве субъекта права. Достаточно вспомнить решение Федерального суда Австралии о признании права нейросети Dabus на получение патента на изобретение [1]. Несмотря на четкую позицию патентных ведомств западных стран, невозможно отрицать влияние прецедента на дальнейшее признание технологий ИИ, как в случае с вызвавшим мировой резонанс признанием криптовалюты в качестве национального платежного средства Гондураса.

Однако следует помнить, что процессы, связанные с нейросетевыми технологиями, обладающими признаками «черного ящика», требуют четкого регулирования, и на сегодняшний день не должны выходить за рамки тех областей, в которых невозможны последствия для инфраструктуры, человеческой жизни и здоровья.

Кроме того, в результате замены человеческого интеллекта на искусственный и по причине неконтролируемого умножения сущностей, на которое способны такие технологии, многие процессы приведут к негативным последствиям, которые потребуют больших временных и финансовых ресурсов для устранения. Например, подача и рассмотрение патентной заявки будет выглядеть, как общение бота с ботом, а на выходе будет создаваться огромное количество документов, верных по форме, но бессмысленных по содержанию.

С появлением большого числа задач научных исследований в области ИИ, проблем, связанных с применением технологий ИИ, а также с формированием тесной международной научной кооперации, в значительной степени определяющей направления развития ИИ, возникает необходимость детального анализа современного состояния исследований и разработок в области ИИ.

ОБ АКТУАЛЬНОМ СОСТОЯНИИ ИССЛЕДОВАНИЙ В ОБЛАСТИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Рост публикационной активности

Несмотря на растущую геополитическую напряженность, наиболее активное сотрудничество в области ИИ происходило между США и Китаем. Количество их совместных публикаций только с 2010 по 2021 год увеличилось в пять раз и в 2,7 раза превысило число совместных китайско-британских публикаций. Весьма примечательно, что в двухлетний период с начала 2020 года, на фоне общемировой тенденции к снижению, кооперация Китая с Великобританией и Австралией также продолжала расти. Такую тенденцию можно объяснить очень высокой публикационной активностью Азиатско-Тихоокеанского региона в области ИИ, приблизительно в два раза превышающей как уровень Северной Америки, так и Европейского и Центрально-Азиатского региона.

За двенадцатилетний период (с 2010 до 2021г.) количество публикаций по тематике ИИ в мире в процентном соотношении с общим количеством научных публикаций выросло с 1,5% до 2,5%, а в абсолютных числах – удвоилось и достигло почти 335 тыс. Такой рост в большей степени определяется публикационной активностью в областях машинного обучения и распознавания образов, при этом около 60% публикаций подготовлено на базе образовательных организаций, около 20%- в некоммерческих организациях и всего около 5% - в частных компаниях.

За указанный период также зафиксирован очень высокий темп роста публикаций в репозиториях – почти тридцатикратный (их количество составило 56 тыс. в 2021 г.), при этом доля публикаций по тематике ИИ среди прочих тематик выросла приблизительно в 15 раз за тот же период и составила 15%. [2]

Следует также отметить тенденцию к более активной кооперации в области ИИ между образовательными и некоммерческими организациями, в сравнении с уровнем кооперации между образованием и частными компаниями, образованием и госучреждениями.

Патентование технологий искусственного интеллекта

За вторую половину 20 в. и начало 21 в. было подано около 340 тыс. заявок на изобретения, связанные с технологиями ИИ, однако более половины патентов было получено с 2013 г., причем также резко менялось соотношение научных трудов и изобретений (8/1 в 2010 и 3/1 в 2016 г.), что свидетельствует о постоянно возрастающих перспективах практического применения технологий ИИ [3]. Число патентов в период 2015-2021гг. увеличилось в 30 раз.

Анализ патентов, представленный в [3], показал пятикратный рост числа патентов в 2004-2014 гг. в азиатских странах. В 2014 г. около 30% патентов в области ИИ были выданы в США, по 16% от общего числа – в Японии и Южной Корее. В абсолютных цифрах в США почти 3 тыс. компаний разрабатывали технологии ИИ, в Китае – более 700, по убыванию следуют Великобритания, Израиль и Германия. Наибольшим количеством патентов владели IBM, Microsoft и Samsung. В России – всего 13 компаний. При этом Россия занимала в 2019 г. шестнадцатое место в мире по числу патентных заявок в области ИИ. [4]

Наиболее активно технологии ИИ применяются в транспортной сфере, в первую очередь в сегментах автомобильного и авиационного транспорта. Доля патентов в сфере транспорта составляла в 2019 г. прибл. 16%, в сфере персональных устройств и телекоммуникаций – около 14%, отрасли документирования и науки о жизни и здоровье – около 11%. По данным Международной организации по интеллектуальной собственности, 20 крупнейших в мире компаний реализуют технологии ИИ в транспортной отрасли, в области персональных устройств, телекоммуникации, управления документацией, науках о жизни и здоровье, а также в банковском деле, финансах и бизнесе.

Ниже рассмотрим актуальный уровень развития различных направлений технологий ИИ.

КОМПЬЮТЕРНОЕ ЗРЕНИЕ. КЛАССИФИКАЦИЯ ИЗОБРАЖЕНИЙ

Выполнение этих задач необходимо для выявления каких-либо отклонений на медицинских снимках, производственных дефектов на изображениях продукции и т.д. Использование методов машинного обучения и обширных баз данных, включающих миллионы изображений (таких как ImageNet) в последние годы привело к высоким результатам в классификации объектов и изображений.

Если в 2012 г. модели ИИ допускали ошибки в 4 случаях из 10, то в 2021г. вероятность ошибки составила 0,1 (соответствие при одном результате, полученном моделью, метке изображения). Уровень соответствия пяти результатов модели метке изо-

бражения при использовании дополнительных обучающих данных достигает уже 99% (Microsoft Cloud и Microsoft AI's Florence-CoSwim-H model) и превосходит не только результаты 2012г. почти на 15%, но и почти на 5%- средние результаты, показываемые человеком.

Следует отметить, что растет эффективность моделей, а стоимость их обучения падает. С 2018 года стоимость обучения системы классификации изображений снизилась более чем на 60 %, а время обучения сократилось почти в два раза [2].

Приведенные показатели уже свидетельствуют о высоком уровне развития автоматизированной классификации объектов и возможности делегирования этих задач системам ИИ.

Синтез и сегментация изображений

Модели ИИ, обученные на крупных базах изображений, научились синтезировать реалистичные изображения, в частности, несуществующих людей. Уже в 2021 г. показатель уровня отклонения от исходных изображениий (Frechet Inception Distance, FID) на наборе данных STL-10 снизился приблизительно в 5 раз по сравнению с 2018г., что является весьма значительным достижением [5]. Результаты с использованием набора данных CIFAR-10 представляются еще более впечатляющими [6]: FID снизился приблизительно в 15 раз за тот же период и составил 2. Однако этот показатель, очевидно, объясняется более низким разрешением изображений в CIFAR-10.

Одной из первостепенных задач создания новых эффективных алгоритмов ИИ на сегодняшний день является распознавание т.н. дипфейков [7]. Эту задачу также можно считать в высокой степени выполненной: если в 2012г. эффективность распознавания дипфейков с использованием четырех наборов данных FaceForensics++ была на уровне 70%, то к 2021г. она достигла 97,7%.

В последнее время наблюдается повышенный интерес к субзадачам компьютерного зрения, в первую очередь в области сегментации медицинских изображений и идентификации изображений лица.

Задачи сегментации изображений (причисления отдельных пикселей изображения к отдельным категориям объектов), важные в т.ч. для обнаружения отклонений на медицинских снимках, сегодня также выполняются существенно более эффективно. Так большим успехом был проект по сегментации 1000 изображений полипов желудочно-кишечного тракта (набор данных Kvasir-SEG), причем изображения были сегментированы также вручную гастроэнтерологами и ими же проверены на корректность соответствия. Новейшие алгоритмы способны корректно сегментировать около 94% (на 12% больше, чем в 2015г.) изображений на наборе данных CVC-ClinicDB и выявить наличие полипов. Почти такие же показатели (более 92%) достигнуты на Kvasir-SEG, причем на обоих наборах данных наилучшие результаты показала сверточная нейронная сеть MSRF-Net model [8].

Весьма заметным проектом в России стала платформа Botkin.AI компании «Интеллоджик» (резидент фонда «Сколково»), которая наряду с 24 компаниями была отобрана из тысяч заявок и прошла в финал международного конкурса Entrepreneurship World Cup (декабрь 2021, Саудовская Аравия) – крупнейшей конкурсной программы, поддержавшей с 2019 г. десятки тысяч участников, как с финансовой, так и с профессиональной точки зрения.

Платформа Botkin.AI проводит анализ медицинских изображений и с высокой точностью выявляет патологические изменения. Высокое качество платформы Botkin AI было подтверждено врачами в 25 проектах по всему миру. [9]

Модели ИИ уже достигли впечатляющих успехов и часто выступают в роли весьма эффективного помощника для человека, обрабатывая огромные объемы данных и непрерывно развиваясь в качестве выполнения задач. В частности, на новый уровень машинное обучение выводят алгоритмы глубинных нейронных сетей (DNN – Deep Neural Network), создаваемые для моделирования абстракций высокого уровня с применением нелинейных преобразований.

Крупным успехом в технологиях машинного обучения стала в 2021 году разработка компанией OpenAI нейронной сети DALL•E (версия GPT-3, третье поколение алгоритма обработки естественного языка), синтезирующей изображения по текстовым описаниям на датасете из пар текст-изображение. Результаты работы этой системы позволяют судить о ее высоком творческом потенциале. [10].

Доступ к модели GPT-3 является платным, однако команда SberDevices на основе кода модели GPT-2 разработала к концу 2021 г. аналог DALL•E – продукт ruGPT-3 (с открытым программным кодом), в котором поддерживается пять вариантов ПО: от 125 млн. до 13 млрд. признаков (закрытой является только модель верхнего уровня).

Создание и совершенствование инструментов ИИ в рамках данного направления весьма оправдано, поскольку в ходе проверки выходные данные нейросети сверяются с выходными данными обучающей выборки, при этом уровень соответствия пос-

тоянно растет.

Обнаружение и распознавание лиц

Сегодня распознавание лиц является одним из самых развитых направлений ИИ, а лучшие модели по распознаванию лиц показывают до 100% эффективности.

Тест для разработчиков технологий распознавания лиц (Face Recognition Vendor Test, FRVT) Национального института стандартов и технологий США (National Institute of Standards and Technology) проходят компании, институты и образовательные организации со всего мира [11]. Тест выявляет качество выполнения алгоритмом задач в интересах национальной безопасности, включая перекрестную проверку виз, идентификацию жертв торговли детьми и т.д. Если в 2017г. частота допущения ошибок лучшими алгоритмами распознавания лиц в процессе выполнения теста FRVT составляла приблизительно 50%, то в 2021г. лучшим результатом было корректное распознавание моделью 999 лиц из 1000. При этом наличие маски на лице, безусловно, снижает продуктивность модели, однако качество распознавания ухудшается только на 5-16% [2].

К пятерке российских лидеров в области ИИ, в частности компьютерного зрения, относятся компании «Яндекс», ABBY, Сбер AI, VisionLabs (совместно с МТС ИИ) и Тинькофф. При этом почти треть рынка ИИ составляют решения в области видеонаблюдения и безопасности, несколько ниже доли решений для промышленности, медицины и торговли. [12]

Инновационным стал проект «Ростелекома» (по инициативе Министерства цифрового развития, связи и массовых коммуникаций и Банка России) по созданию единой биометрической системы (ЕБС). Биометрическая идентификация позволяет получать услуги по открытию счета, получению кредита и т.д. В системе используются одновременно лицо, записанное на веб-камеру, и цифровой образец голоса (последовательность цифр). Данные пакетом отправляются в систему, где подтверждаются и регистрируются, после чего информация о зарегистрированной биометрии появляется в личном кабинете на портале госуслуг. Ей можно пользоваться вместо предъявления паспорта также в целях дистанционного заключения договоров, получения нотариальных услуг, оформления квалифицированной электронной подписи и совершения многих других юридически значимых действий.

В [13] отмечается, что уже в 2019 г. Почта Банк при помощи единой биометрической системы предотвратил более 1,2 тыс. попыток входа в систему с использованием чужих учетных записей, выявил сотни обращений в банк с поддельными паспортами.

Использование ЕБС также позволяет успешно решать проблему внутреннего злоумышленника. Например, сотрудник банка может получить доступ к счету клиента и провести все операции только в присутствии клиента и после его идентификации по фото. Таким образом, предотвращается несанкционированный доступ к счетам клиентов.

Распознавание видео

Что касается обнаружения объектов на видео – здесь результаты менее однозначны и в большей степени зависят совокупности свойств системы: модели, которые быстро обучаются, могут быть более производительными, но иметь меньшую точность, а более точные модели могут потребовать большее время на обработку видео. Видеоряд достаточно часто включает себя взаимосвязи и последовательности, выводы из которых возможно сделать, основываясь на здравом смысле, сформированном у человека к первому классу начального образования и включающем, например, рассуждения о «наивной физике» или намерениях и свойствах индивидуумов.

Рассуждения на основе здравого смысла (Visual Commonsense Reasoning, VCR) являются сравнительно новым подходом в этой области ИИ. При этом системе ИИ задаются провокационные вопросы о сути изображения в видеоряде, а она должна не только выбрать ответ из нескольких предлагаемых вариантов, но и обосновать его. В рамках этого подхода результат модели достигает около 72%. Очевидно, что с более сложными и творческими задачами алгоритмы справляются гораздо хуже.

Развитие алгоритмов в рамках данного подхода происходит медленно по сравнению с другими направлениями из-за очень широкого охвата знаний, основанных на здравом смысле, необходимых при распознавании объектов на изображении и видео, при интеллектуальном анализе текста и машинном переводе (эффективность повысилась только на 8% за три года и достигла приведенного выше показателя). [2]

ПОНИМАНИЕ И ОБРАБОТКА ЕСТЕСТВЕННОГО ЯЗЫКА

На сегодняшний день еще не решены сложные языковые задачи, но исходя из уровня производительности по базовым тестам на понимание про-

читанного (например, SuperGLUE и SQuAD) ИИ превосходит человеческий на 1-5%. При этом следует отметить, что речь в SuperGLUE идет в первую очередь о задачах на выбор верного варианта из представленных в рамках тестовой системы.

Набор данных SQuAD (Stanford Question Answering Dataset) содержит уже в т.ч. 50000 вопросов, часто не имеющих, при внимательном прочтении, однозначно правильного ответа. К 2019г. рост показателей моделей на SQuAD, достигнув базовой отметки результатов человека в тех же заданиях, резко замедлился. Новые наборы данных, такие как ReClor (Reading Comprehension Dataset Requiring Logical Reasoning), стали предлагать более сложные задачи для тестирования моделей, по уровню сопоставимые с экзаменационными билетами в области юриспруденции.

Однако если на простых задачах ReClor в 2021г. модели ИИ показали достаточно высокие результаты (более 91%), то на сложных задачах, решение которых требует логического обоснования, максимальный результат был равен приблизительно 69%. [2]

Задача современных моделей естественного языка – представление текста в векторной форме (embedding), то есть слова оцифровываются моделями и записываются в виде упорядоченного набора числовых значений (векторов), причем слова, близкие по значению, находятся близко друг к другу в пространстве. По данному принципу работают нейросетевые модели.

Многие модели ИИ уже протестированы на наборе данных Stanford Natural Language Inference (SNLI), содержащем приблизительно 600 тыс. пар предложений (утверждение и ассоциированная гипотеза) с метками, указывающими на наличие логического следования («entailment»), противоречия («contradiction») либо на отсутствие смысловой связи («neutral») между предложениями. В процессе тестирования модель определяет логическое соответствие гипотезы стартовому утверждению, при этом производительность модели рассчитывается как отношение правильно классифицированных пар утверждений к общему числу пар. Наибольшую производительность на SNLI (прибл. 93%) показала в 2021 г. модель Facebook AI USA's EFL. [2]

В таких сложных лингвистических задачах в естественном языке, как абдуктивные выводы, основанные на неопределенных (или логически не связанных) допущениях и ограниченной информации (Abductive natural language inference, aNLI) продвижение есть, но человек, априори способный рассуждениям по методу абдукции, по-прежнему показывает результаты, превышающие показатели системы ИИ. Использование метода абдукции в инструментах ИИ может оказаться весьма перспективным и полезным с точки зрения построения максимального количества гипотез на основе множества фактов (эмпирического опыта) и поиска ответа на вопрос (например, по каким причинам может происходить то или иное событие), а также практически применимым в медицине, юриспруденции и других областях.

На сегодняшний день компьютерная лингвистика позволяет, как было указано выше, представлять в виде векторов целые предложения и абзацы текста, при этом расположение векторов зависит от параметров используемой модели. Обучение нейронных сетей рассматривается как наиболее эффективный способ построения моделей естественного языка, способных определять совокупность признаков текста, что необходимо для его качественного анализа.

Однако следует учесть и такой весьма заметный недостаток данного подхода, как наличие вероятности несоответствия результата сравнения текстов в форме векторов при использовании известных метрик сходства (евклидово расстояние и косинус угла между векторами) их реальной смысловой емкости, при котором близкие по значению слова (предложения) могут оказаться в векторном пространстве дальше друг от друга, чем далекие слова (предложения). Таким образом, для развития указанного подхода необходимо использование непротиворечивых метрик, в частности, рассмотренных в работе [14].

ОБУЧЕНИЕ С ПОДКРЕПЛЕНИЕМ

За последнее десятилетие системы ИИ смогли освоить узкие задачи обучения с подкреплением, при котором испытуемая система обучается максимизировать производительность в определенном навыке (например, в шахматах) выполняя данное ей задание и основываясь, в отличие от обучения с учителем, на опыте своих предыдущих действий, а не на статичном наборе данных. Система (алгоритм ИИ), взаимодействуя в некоторой среде (компьютерной платформе), тестирует в ней различные стратегии решения поставленной задачи и выбирает стратегию с максимальным вознаграждением.

Обучение с подкреплением используется, например, в промышленности – для решения задач оптимизации производственных процессов, для предсказания будущих событий в рамках моделей

временных рядов, в коммерческой деятельности – для максимизации целевой функции или если нужно извлечь пользу из полученного ранее опыта.

Платформа ALE (Arcade Learning Environment) для разработки и оценки алгоритмов машинного обучения обеспечивает интерфейс к сотням игр Atari 2600. Существуют различные показатели производительности, но наиболее используемый – антропонормированный показатель, при котором 0% означает случайную производительность, а 100% - среднюю человеческую производительность. В 2021 г. лидировала модель ИИ GDI-H3 model, которая показала производительность на играх Atari-57, в два раза превышающую производительность более раннего эффективного алгоритма MuZero от DeepMind (она составляла около 48%) [15]. При этом GDI-H3 model требовала уже 200 млн. обучающих кадров, т.е. в 100 раз меньше, чем MuZero.

Таким образом, за несколько лет ощутимо выросла производительность моделей обучения с подкреплением, что многократно подтверждено на большинстве игр, однако чтобы достичь максимальной производительности, необходимо в разы увеличить эффективность алгоритмов.

ИССЛЕДОВАНИЯ В ОБЛАСТИ ЭТИКИ ИИ

С 2014 года резко возросло число исследований в области анализа объективности и прозрачности искусственного интеллекта: количество соответствующих публикаций в трудах конференций, посвященных этике ИИ, увеличилось в пять раз. Понятия алгоритмической достоверности и предвзятости прочно закрепились как в области академических исследований, так и на уровне практических проектов в экономике и промышленности. При этом на 71% больше публикаций на конференциях, посвященных этике ИИ, подготовлено исследователями от промышленности.

Очевидно, что частный бизнес и промышленность заинтересованы в повышении доверия к технологиям ИИ, которое напрямую зависит от закрепления этических норм в области искусственного интеллекта.

Как было указано выше (раздел «Синтез изображений»), достигнут прогресс в обучении моделей визуальной лингвистики, в решении задач классификации изображений, создания изображений из текстовых описаний. Применение технологий, изначально относящихся к NLP, привело к новому качеству компьютерного зрения. Так, эксперименты с CLIP [16] показали, что изображения людей с черной кожей были ошибочно не классифицированы как изображения людей примерно в два раза чаще, чем изображения представителей других рас. Таким образом, мы видим прогресс в решении проблемы измерения предвзятости в компьютерном зрении.

Безусловно, это направление демонстрирует новый уровень возможностей выполнения задач, связанных с изображениями и текстовыми описаниями (в том числе, использование моделей направлено на отражение социального предубеждения), однако существуют и негативные стороны, связанные со злоупотреблением инструментами в целях пропаганды, дезинформации и осуществления прочих неэтичных и незаконных действий.

Поскольку во многих странах стали обращать все больше внимания на этические аспекты применения ИИ, начали появляться различные конвенции и кодексы в этой сфере. Наблюдается более широкий охват законодательства об ИИ, чем когда-либо: анализ законодательных документов по ИИ в 25 странах показал, что количество принятых законов за период с 2016 по 2021 г. увеличилось примерно в пять раз.

Активно идет обсуждение международного урегулирования в области технологий ИИ: еще в ноябре 2021 г. ЮНЕСКО была принята первая всеохватывающая конвенция, посвященная рекомендациям в области этики ИИ, которые были поддержаны 192 странами мира (к ним не относятся США, Россия и Китай).

Российский Кодекс этики в сфере искусственного интеллекта, принятый в октябре прошлого года [17], разработан Альянсом в сфере искусственного интеллекта РФ, Аналитическим центром при правительстве РФ и Минэкономразвития на основе «Национальной стратегии развития ИИ на период до 2030 г.».

Актуальность задачи разработки была обусловлена, в первую очередь, существованием таких рисков и угроз, связанных с внедрением и развитием цифровых технологий, как дискриминация, потеря приватности, потеря контроля над ИИ, причинение вреда человеку ошибками алгоритма, применение в неприемлемых целях. Все они включены в принятый "Кодекс этики в сфере искусственного интеллекта" как угрозы правам и свободам человека. [18]

В Кодексе описаны шесть базовых принципов, в соответствии с которыми защита интересов групп людей и каждого человека, а также ответственное отношение в ходе разработки и практического применения являются главными приоритетами развития технологий ИИ. Большое значение имеет принцип полезности ИИ для людей, прозрачности

и правдивости в информировании о возможностях и рисках тех или иных технологий, принцип приоритета развития ИИ перед интересами конкуренции.

Так как цифровые технологии и в частности технологии ИИ постепенно охватывают все сферы нашей жизни, есть необходимость в регулировании этой области в соответствии с Кодексом. Однако поскольку он носит рекомендательный характер, сложно утверждать, сможет ли он кардинально изменить направление развития технологий ИИ в России.

ФИНАНСИРОВАНИЕ ПРОЕКТОВ В ОБЛАСТИ ИСКУСТВЕННОГО ИНТЕЛЛЕКТА

Одной из основных мировых тенденций в области искусственного интеллекта является рост частных инвестиций и увеличение их концентрации: размер частных инвестиций в ИИ в 2021 году (около 93,5 млрд. долларов США) более чем вдвое превышает общий объем частных инвестиций в 2020 году, при этом количество финансируемых в области ИИ компаний продолжает сокращаться, и если в 2019 г. финансирование получили более 1 тыс. компаний, то в 2021 г. – всего 746. [2] Данная тенденция, в частности, свидетельствует о наличии естественного процесса формирования отрасли искусственного интеллекта.

В последние годы активно финансируются системы ИИ, препятствующие распространению дезинформации (первичное выявление потенциально ложных утверждений для последующего анализа путем сравнения с предыдущими аналогичными утверждениями, прошедшими проверку). Автоматизированная проверка утверждений на истинность является предметом многих исследований. Известно, что крупная канадская венчурная компания еще в 2019г. инвестировала 1 млн. долл. в конкурс проектов по проверке утверждений на истинность.

Среди компаний, которые предоставили информацию о размерах финансирования, число первоначальных инвестиционных раундов в 2021 г. в размере 100-500 млн. долл., также и в размере 50-100 млн. долл. увеличилось более чем в два раза по сравнению с 2020 годом. Кроме того, в 2021 г. инвестиционных раундов размером свыше 500 млн. долл. отмечено 15 – почти в 4 раза больше, чем в 2020г.

Следует отметить, что на 2021г. наибольший объем частных инвестиций с 2013 г. получили компании США (около 52,9 млрд. долл.), за ними следует Китай (17,2 млрд.долл.), Великобритания (4,65 млрд.долл.), Израиль (2,4 млрд.долл.) и Германия (около 2 млрд.долл.). Совокупные частные инвестиции в Европейском Союзе составили около 6,42 млрд.долл.

Наибольший объем инвестиций получают проекты в области управления данными, обработки данных и облачных вычислений (в 2021г. составили около 12,2 млрд.долл.), а также в областях медицины и здравоохранения (11,3 млрд. долл.), финансовых технологий (10,26 млрд.долл.). Несколько меньший объем инвестиций направлен на проекты в области промышленной автоматизации (около 6 млрд. долл.), энергетики, кибербезопасности (по 3 млрд. долл.), распознавания лиц (около 2 млрд. долл.) и др.

В 2021 году в мире как по общему объему частных инвестиций в ИИ, так и по количеству основанных компаний в области ИИ лидировали Соединенные Штаты, которые по этим показателям, соответственно, в 2 и 3 раза превосходили Китай. Учреждениями гражданского сектора США в 2021г. направлено около 1,53 млрд. долл. на финансирование исследований и разработок в области ИИ, что почти в 3 раза превысило размер инвестиций 2018г. Такая тенденция свидетельствует о высокой приоритетности области ИИ для госорганов США.

В соответствии с открытыми данными о запросах на проведение исследовательских, конструкторских, испытательных и измерительных работ в области ИИ Министерство обороны США выделило в 2021г. 9,26 млрд. долл. на примерно 500 проектов, прежде всего по разработке различных прототипов ИИ для военных целей, технологий противодействия оружию массового уничтожения, средств ускорения интеграции технологий ИИ в системы Министерства обороны. За Министерством обороны с большой разницей в объемах финансирования проектов по ИИ в соответствующих областях следуют Министерство здравоохранения и социальных служб, Национальное управление по аэронавтике и исследованию космического пространства и другие.

Российские проекты в области ИИ нередко получают поддержку в виде субсидий, налоговых льгот, грантов (до 100 млн руб. на проект) со стороны государства. В настоящее время выполняется крупнейший федеральный проект «Искусственный интеллект» (до 2024 года) [19], частично финансируемый из средств федерального бюджета, включая средства, выделенные на реализацию национальной программы «Цифровая экономика РФ». Всего на проект отведено 86,5 млрд. рублей, из них 29,4 млрд. рублей – средства федерального бюджета,

остальные — средства из внебюджетных источников и финансирование Сбербанка.

В целом расходы на исследования и разработку инструментов ИИ в России в сотни раз ниже, чем в Китае и США, несмотря на то, что ВВП ниже только в 10 и 14 раз соответственно [20]. Однако для того, чтобы давать какие-либо оценочные суждения о часто упоминаемом отставании России в области цифровых технологий и искусственного интеллекта в частности, а также о влиянии размера финансирования на темп развития области, необходимо четко разделять стратегические направления, в рамках которых происходит, либо возможно развитие технологий ИИ. В настоящее время в области ИИ превалируют нейросетевые технологии, имитирующие биологический интеллект. Очевидно, чем сложнее образец, взятый для имитации, тем больше финансирования потребуется для его максимально точного воспроизведения. Поэтому отказ от имитационной модели может в сотни раз сократить расходы на исследования и разработку.

Стоит также учитывать, что развитие и внедрение технологий ИИ в России сдерживают некоторые важные факторы, например нехватка отечественных технологий ИИ, недостаток возможностей тестирования в высокотехнологичных отраслях, таких как авиакосмическая, фармацевтическая отрасли, автомобилестроение, приборостроение, производство компьютеров и их компонентов. Данные тенденции, явно прослеживаемые и в трудах российских ученых [21, 22], также усугубляются ввиду недостаточного финансирования.

ЗАКЛЮЧЕНИЕ

Результаты проведенного в данной работе анализа развития технологий искусственного интеллекта показывают стремительный рост как эффективности отдельных инструментов и моделей ИИ, так и их доступности в различных областях. Тенденция к низкой стоимости и высокой скорости обучения моделей проявляется во многих категориях задач машинного обучения, в том числе в задачах обнаружения объектов и обработки естественного языка, и способствует распространению технологий искусственного интеллекта.

В области распознавания лиц, сегментации и синтеза изображений достигнуты весьма высокие результаты, однако задачи, решение которых требует совершения сложных логических операций, таких как рассуждения на основе здравого смысла или по методу абдукции, по-прежнему выполняются существующими алгоритмами в рамках современной концепции нейросетевого ИИ с очень низкой эффективностью.

На сегодняшний день можно констатировать, что развитие проблемы пока практически полностью идет в сфере имитации, т.е. ИИ пытаются реализовать как в рамках имитации физиологии мозга (нейросети), так и в привычных человеку методах мышления (выработка суждений). В то же время очевидно, что проблема должна рассматриваться шире, в рамках системного анализа и расширения возможностей ИИ в сторону, отличную от человеческой логики.

Кроме того, ИИ в биологии и медицине также замыкается в рамках узких подходов исследования генома при помощи методов машинного обучения, что является контрпродуктивным подходом [23].

Подобные проблемы являются следствием в первую очередь жесткого давления бизнеса на ученых в области ИИ и недостатка добросовестности специалистов, продуцирующих «модные» подходы к решению проблем ИИ, а также выраженным низкопоклонством перед западными учеными и их результатами.

В современных системах ИИ важнейшими проблемами можно считать отсутствие предсказуемости и верифицируемости результатов обработки моделей (по принципу «черного ящика»), что с одной стороны делает их непригодными для производственных и инфраструктурных процессов в критически важных областях, с другой – приводит к нереализуемости платформенного подхода [24, 25].

Формирование системного подхода и согласованность в исследованиях и развитии инструментов ИИ будет способствовать их интеграции и созданию искусственного интеллекта как некой объединенной сущности. [26]

СПИСОК ЛИТЕРАТУРЫ

1. Австралийский суд подтвердил право нейросети на получение патента. URL: https://trends.rbc.ru/trends/industry/6109576b9a794779eed90de8 (дата обращения: 29.11.2022)

2. Artificial Intelligence Index Report 2022. URL: https://aiindex.stanford.edu/wp-content/uploads/2022/03/2022-AI-Index-Report_Master.pdf (дата обращения: 29.11.2022)

3. Токарев Б.Е., Токарев Р.Б. Анализ рынка искусственного интеллекта: динамика патентования технологий.

URL:https://cyberleninka.ru/article/n/analiz-rynka-iskusstvennogo-intellekta-dinamika-patentovaniya-tehnologiy/viewer (дата обращения: 29.11.2022)

4. WIPO Technology Trends 2019 Artificial Intelligence. URL: https://www.wipo.int/edocs/pubdocs/en/wipo_pub_1055.pdf (дата обращения: 29.11.2022)

5. Jeon, I., Lee, W., Pyeon, M., & Kim, G. (2021). IB-GAN: Disentangled Representation Learning with Information Bottleneck Generative Adversarial Networks. Proceedings of the AAAI Conference on Artificial Intelligence, 35(9), 7926-7934. https://doi.org/10.1609/aaai.v35i9.16967

6. Training cifar-10 in under 11 seconds. URL: https://github.com/apple/ml-cifar-10-faster (дата обращения: 29.11.2022)

7. Adversarial Threats to DeepFake Detection: A Practical Perspective. URL: https://arxiv.org/pdf/2011.09957.pdf (дата обращения: 29.11.2022)

8. A. Srivastava et al., "MSRF-Net: A Multi-Scale Residual Fusion Network for Biomedical Image Segmentation // IEEE Journal of Biomedical and Health Informatics, vol. 26, no. 5, pp. 2252-2263, May 2022, doi: 10.1109/JBHI.2021.3138024

9. Платформа Botkin.AI стала финалистом конкурса с призовым фондом $1 млн. URL: https://www.iksmedia.ru/news/5861542-Platforma-BotkinAI-stala-finalistom.html (дата обращения: 29.11.2022)

10. Обработка данных в глубинных нейронных сетях: достижения и вызовы текущего момента. URL: https://www.tadviser.ru/index.php/Статья:Обработка_данных_в_глубинных_нейронных_сетях:_достижения_и_вызовы_текущего_момента (дата обращения: 29.11.2022)

11. Алгоритм распознавания лиц [Название_Компании] признан лучшим в мире. URL: https://habr.com/ru/company/ntechlab/blog/594575/ (дата обращения: 29.11.2022)

12. Тенденции развития компьютерного зрения в России. URL: https://www.iksmedia.ru/articles/5894791-Tendencii-razvitiya-kompyuternogo.html (дата обращения: 29.11.2022)

13. Биометрия в банках: что это, зачем и к чему приведет. URL: https://trends.rbc.ru/trends/industry/5fd3ac6a9a79475333bfcb4f (дата обращения: 29.11.2022)

14. Рязанова А.А., Щербаков А.Ю. К вопросу о метриках сходства текстов для методов их автоматизированного сравнения // Приоритетные задачи и стратегии развития технических наук. Выпуск II. Сборник научных трудов по итогам международной научно-практической конференции (25 мая 2017 г.), г. Тольятти. С. 66-69.

15. DeepMind представила бота MuZero, который играет в старые игры и в шахматы. URL: https://habr.com/ru/news/t/534742/ (дата обращения: 29.11.2022)

16. Нейронная Сеть CLIP от OpenAI: Классификатор, который не нужно обучать. Да здравствует Обучение без Обучения. URL: https://habr.com/ru/post/539312/ (дата обращения: 29.11.2022)

17. Кодекс этики в сфере искусственного интеллекта. URL: https://a-ai.ru/wp-content/uploads/2021/10/Кодекс_этики_в_сфере_ИИ_финальный.pdf (дата обращения: 29.11.2022)

18. В России подписан "Кодекс этики искусственного интеллекта". URL: https://rg.ru/2021/10/26/v-rossii-podpisan-kodeks-etiki-iskusstvennogo-intellekta.html (дата обращения: 29.11.2022)

19. Более 30 млрд рублей направят на финансирование федерального проекта «Искусственный интеллект» до 2024 года. URL: https://www.economy.gov.ru/material/news/bolee_30_mlrd_rubley_napravyat_na_finansirovanie_federalnogo_proekta_iskusstvennyy_intellekt_do_2024_goda.html (дата обращения: 29.11.2022)

20. Искусственный интеллект в России. Состояние отрасли и прогнозы. URL: https://skillbox.ru/media/business/iskusstvennyy-intellekt-v-rossii/ (дата обращения: 29.11.2022)

21. Гафаров Ф.М., Галимянов А.Ф. Искусственные нейронные сети и приложения: учебное пособие // Изд-во Казан. ун-та, 2018. 121 с.

22. Остроух А.В. Интеллектуальные системы: монография // Красноярск: Научно-инновационный центр, 2020. 316 с.

23. Кожевин П.А. Природоведческая микробиология в эпоху цифровизации // Вестник современных цифровых технологий. 2022. № 13. С. 20-31.

24. Рязанова А.А. Цифровые платформы: интегративный потенциал, основные понятия и свойства // Вестник современных цифровых технологий. 2020. № 4. С. 28-39.

25. Рязанова А.А., Щербаков А.Ю. К формулированию положений платформенно-сервисной модели для информационно-телекоммуникационных систем // Научно-техническая информация. Серия 2: Информационные процессы и системы. 2021. № 5. С. 12-15

26. Индекс готовности приоритетных отраслей экономики Российской Федерации к внедрению искусственного интеллекта. URL: https://ai.gov.ru/upload/iblock/c16/xyvmsh4hgi850ninjhq90xi4t6yggu8c.pdf (дата обращения: 15.12.2022)

Homo digital

Егор Федоров
Республика Беларусь,
писатель, сценарист, драматург

За всю Одессу я не скажу, но лично меня озарения никогда не посещали просто так. Бамс – и озарило чем-нибудь эдаким. Просто так, за здорово живешь.

Озарение – это, как правило, продукт моего длительного размышления. Я вообще считаю, что если думать добросовестно, додуматься можно до чего угодно.

Хотя здесь надо сказать, что для озарения вовсе не обязательно сидеть в позе роденовского «Мыслителя» и напряженно морщить лоб. Для того чтобы озарило лично меня, нужно, чтобы это тесто забродило где-то внутри меня. Когда забросил в подсознание какие-то ингредиенты, исходники, и эти ингредиенты постепенно зреют. Конечно же, время от времени возвращаешься к теме. Перед тем, как заснуть, к примеру. Вспоминаешь о том, что там из этого теста должно получиться в итоге. Представляешь себе кулич. А может быть бублик. А может быть дырку от бублика.

И засыпаешь.

А оно продолжает зреть потроганное, размятое только что твоими руками, растревоженное.

Озаряет меня часто и на совершенно разные темы. Работа такая. Я же сценарист. И если у меня не будет озарений о том, как Главный Герой (ГГ) выбирается из кипящего жерла вулкана, или как он проворачивает комбинацию по отмыванию денег, или с помощью какой уловки избегает наказания, то как сценарист я очень быстро закончусь. Озарения – мой хлеб. При этом зачастую мне приходится изучать что-то новое. Меня не озаряет в одной области, как, к примеру, математиков. Или там химиков. Если ГГ авиатехник, то порой приходится читать, как работает подъемная сила крыла самолёта, если ГГ телефонных дел мастер, то надо знать, почему телефон нельзя зарядить за одну минуту, если ГГ жокей, то надо бы разбираться в различиях между аллюром и галопом.

Итак, позвольте представиться – Александр Стецкий, сценарист.

Кроме роли сценариста в этой жизни у меня есть ещё одна немаловажная роль –роль отца.

И на днях моей дочери Грации исполнилось 17 лет.

***

– Представь, что тебе встречается человек, – сказал я, – который знает ответы на все вопросы.

Мы сидели у костра на нашей даче, я разминал в руках сигарету. Сегодня Грэйси стала семнадцатилетней.

Мама убирала с праздничного стола. На этот стол сегодня я приготовил кету на углях – и этот новый опыт, кажется, удался. Все были сытыми и довольными. Может быть, «все» звучит здесь слишком громко, потому что «всех» было всего трое.

Тогда, когда я снял рыбу с углей, я набросал в наш камин дров покрупнее. И за то время, пока мы праздновали, дрова высохли и теперь весело и ярко занялись в металлическом корыте для размешивания цемента. Такой вот получился у нас камин. Надо сказать, достаточно уютно.

– Ну? – я порой злоупотреблял паузами в словах, дочь к этому привыкла и иногда знала, что меня нужно было немножко подтолкнуть, чтобы я продолжил.

– Так вот, – я сунул сигарету в рот и пошел к камину подкурить. Никогда у костра я не подкуривал спичками или зажигалкой. – Ты встретила человека, который знает ответы на все вопросы. О чем бы ты его спросила?

– Хм, – сказала дочь. Однако долго она не размышляла. – Наверное, я бы спросила его, есть ли во всем этом какой-то смысл?

Я захотел замереть вот так вот, с сигаретой, которой приклеился сейчас к полену, чтобы подкурить. Однако у костра было слишком жарко, и замирать я очень быстро передумал. Но вообще такой ответ застал меня врасплох.

– Любопытно, – в задумчивости сказал я, отошел от камина и сел обратно в своё кресло. Наши дачные кресла продал мне за бутылку водки Павлик. Были они плетеные из ореха и уже почти своё отслужили. Однако это «почти» длилось вот уже третий, что ли, год на нашей даче. А кресла все не сдавались.

Я сидел, курил, чесал нос и вспоминал, что именно этот вопрос интересовал меня в мои 17 лет. А потом, в 18, 19 и так далее – лет, кажется, до 25-27. А потом появилась Грация и этот вопрос не то, чтобы

отпал – нет. Я не решил, что смысл существования любого человека – это рожденные им дети. Просто вопрос этот сначала отодвинулся из орбиты вопросов первейшей важности, а потом и вовсе я завалил этот вопрос хламом и барахлом. Комодами. Рубахами в крупную клетку. Стройматериалами для дачи. Девушками, алкоголем, сигаретным дымом, тостами, заботами, проблемами, накладными, закладными и профсоюзным билетом члена «Союза кинематографистов».

– Знаешь, а я давно об этом не думал, – сказал я дочери. – Спасибо тебе.

***

Так вот, если продолжать мысль об озарениях, то вполне можно говорить о том, что вопрос дочери «бродил» во мне примерно уже лет 20-25.

В первую очередь я задумался, а один ли вообще это вопрос? По всему выходило, что не один, а два разных. Потому что, к примеру, муравейник – достаточно осязаемый и хорошо видимый результат существования всех муравьев муравейника. А вот результат существования одного муравья покрыт мраком.

По той же аналогии с муравьями плясать надо было бы от чего-то большого.

То есть от смысла существования всех людей, всей цивилизации. Потому как разглядеть большое обычно много проще, чем разглядеть малое.

Хотя аналогию с муравейником – то есть строительство городов и изменение лица планеты, как основной смысл и результат существования человеческой цивилизации – я отмел сразу. Кажется, наши города сейчас больше похожи на вредительство, чем на положительный смысл существования.

«Положительный смысл существования».... А кто мне вообще-то сказал, что смысл существования человека должен быть именно положительным? Незря ведь говорится «что русскому хорошо, то немцу – смерть». По аналогии, что хорошо землянину, то совсем не обязательно понравится инопланетянину. Хм. А может быть, наоборот? Что плохо для нас, то будет хорошо для них?

***

– Ну и чего ты её схватил, эту пешку? – спросил меня Павлик. – Выкручивайся теперь.

В парке было Лето. Лето – это дети, аттракционы, фонтаны, пиво, шашлыки, ощущение праздника, ощущение, что ты среди уж если не друзей, то просто интересных персонажей, которые точно не настроены к тебе враждебно.

Кроме шахмат здесь играли в карты, домино и шашки, а однажды я подумал, что надо бы сюда принести игру го. Но мне сказали, что никого ты этим не удивишь, сюда уже приносили и го, и нарды, и однажды Грек, видимо, со свалки приволок сюда даже настольный хоккей. В нём не было половины фигурок и отсутствовала шайба, однако кто-то составил Греку компанию и в этой игре.

Я смотрел на позицию, которая сложилась сейчас на доске, и кристально ясно понимал, что пешку прошлым ходом никак брать было нельзя. Но блиц есть блиц.

– Ну, иди, помогай мне, Павлик, – Паша уже отошёл от нашего стола. – Я ж пропаду!

– Ещё чего, – ответил Паша, мастер спорта по шахматам без соответствующего документа. На стол он уже не смотрел. Друзьями с Пашей мы не были, но испытывали уважение друг к другу. Он ко мне – как к сценаристу. Я к нему – как к мастеру спорта. Хоть и без документа. – Сдавайся, там проиграно.

– Да ладно, Павличка, – в этой партии у меня было серьёзное материальное преимущество. И сдаваться в этой уже выигранной, как я думал, партии, мне было до слез обидно. Но на доске, кажется, рисовался мат в 3-4 хода. Слишком гол был мой король. До неприличия просто обнажен. Не уверен даже, были ли сейчас на нем трусы, если уж доводить метафору до конца.

– Конь с5 , ферзь а7 и пешка а, – сказал Паша. – Мат.

Так и есть, мат в три хода. Я немного разозлился. Сказал сопернику спасибо, пододвинул ему проигранный рубль и вышел из-за стола.

– Все дуешь? – спросила Грация. Она стояла рядом, но смотрела не только на мою партию, рядом играли ещё.

– Но-но, – ответил я. – В папочку надо верить. А не указывать ему на его неудачи.

– Кому на кого?

Сегодня я действительно уже проиграл много. Может быть, дело было в литре красного сухого, что я в себя уже залил. А может быть в том, что играл я в целом не на уровне местной шайки-лейки. Встречались среди этой братии и КМСы и мастера спорта. И если я и выигрывал у кого-то, то с приличной форой.

Жизнь занесла меня в это место достаточно случайно. Знакомый однажды предложил – а пошли в парк к шахматистам? Там весело.

Я – человек на подъем легкий, тем более интересно было посмотреть на эту незнакомую, неизвестную жизнь. И согласился. Грация тоже заинтересовалась. Мы сходили раз, сходили два, там действительно было весело.

Я открыл второй пакет вина, посмотрел по сто-

ронам в поисках милиции, чтоб она внезапно не пришла меня беречь, милиции в поле видимости не было. Я сделал приличный глоток.

– Будешь? – пошутил я, показывая дочери глазами на пакет с вином.

– Ах, папичка, папичка, – вздохнула Грация. – А хотя давай.

– Ладно-ладно, – сказал я и спрятал пакет обратно в рюкзак. – Ремня сейчас дам.

– А чего предлагаешь тогда?

– Проверяю тебя. Может ты уже пьешь!

Подошел Олег. Он играл напротив с какими-то детьми. Надо сказать, что дети сюда тоже приходили порой непростые. И не всех их можно было обыграть.

– Ну что, выиграл? – спросил Олег.

– Проиграл, – ответил я.

– Ну, давай пять на полторы, – предложил мне Олег.

Я согласился.

Стали играть.

С Олегом мы обычно играли без денег – я просто угощал этого КМСа тем, что пил сам. Но сегодня случилось не «как обычно» и после третьей партии я сам отчего-то решил играть с ним по рублю. Олег был не против. Чего меня дернул черт, понятно было не до конца. Наверное, хотелось какой-то остроты. Но вместо остроты я получал раз за разом одни негативные эмоции. И проигрывал партию за партией. Олег сегодня или был в ударе или на него так подействовала игра на деньги. А может быть и совсем не в Олеге дело. А в том, что у меня уже почти закончился второй литр красного сухого. Дул я просто безнадежно. Когда сумма проигранного перевалила за десять рублей, я уже пребывал в каком-то гневе.. Хотя внешне этого никак не проявлял. Но мысли бродили самые скверные. Отчего-то мне пришли в голову все те случаи, когда Олег пил за мой счет, я был очень зол на Олега, но играть не прекращал.

– А смысл жизни не ищут, – услышал я сквозь пелену событий на нашей доске. Рядом сидел старый шашист и настойчиво внушал что-то мужику средних лет. – Смысл жизни вкладывают, ты пойми это.

Тут я мельком вспомнил ту задачу, которую загружал в свой котелок уже с неделю назад. Тот вопрос, что задала Маргарита.

Старый шашист ничего нового сейчас для меня не открыл, эти постулаты я уже читал и уже даже перетирал с кем-то. Тем более что занят я был не поиском смысла для индивидуального гражданина, а поиском смысла для всей человеческой цивилизации.

Когда я понял, что Олег готовит мне очередной мат, я опять испытал глубокое и яркое страдание.

Это страдание немедленно сплелось со смыслом существования, о котором бубнел за соседним столом старый шашист, и меня замкнуло.

Весь тот огромный негатив, что я испытывал от сегодняшних проигрышей, внезапно помог мне в решении того вопроса, который мне задала пару недель назад дочь. Личный опыт – все же дело очень весомое. И вот когда я сам раз за разом сегодня испытывал страдания и запускал поток черных мыслей от игры в шахматы, а потом случайно услышал рассуждения о смысле жизни, меня, как я писал выше, замкнуло.

Я выложил из кошелька очередной рубль и протянул его Олегу. Потом посмотрел на играющих в парке. Ещё раз обдумал мысль, которая только что посетила меня, и сказал:

– Пошли домой, Грэйси.

***

– Так, что-то я не поняла, – сказала Грация. – Ты хочешь сказать, что смысл существования человека и людей в целом – это выработка негативных эмоций?

– Бинго, Грассия! – порадовался я за своего понятливого ребенка. Когда мы вышли из Павильона, я всю дорогу путанно объяснял ей свою догадку, которой меня замкнуло тогда, когда я в последний раз проиграл Олегу. Выходило криво, но дочь меня поняла правильно и сделала вывод сама.

– Ну, а почему хотя бы не положительные эмоции? – спросила Грация. Мы остановились у блинной, и я стал в очередь.

– Во-первых, давай ты мне скажешь, что тебе сделать легче – порадоваться за кого-то или на что-то позлиться?

Грейси задумалась.

– Ну позлиться легче, конечно.

– Конечно. Это точно так же, как сказать человеку, что он плох во сто раз легче, чем сказать человеку, что он «хороший». Искренне только. Так?

– Ну пусть так.

– То есть тот, кто нас, людей, выводил, в прошивках так прописал, понимаешь? Чтоб мы заточены были под негатив, злобу и агрессию. А не под сострадание, доброту и разную там другую милоту. Два блина, пожалуйста.

– Это кто это? – не поняла дочь. – Ну, кто нас выводил?

– А этого я не знаю, – ответил я. – Да и не очень-то это важно, кто. Давай их назовем… ну высшими существами пусть. Сокращенно ВС.

– Но для чего они нас выводили-то?

– Да все для того же, Грация! Животное, вот наша кошка, например, не может страдать от того, что проиграла кому-то в шахматы! Или что потеряла все деньги на бирже. Или что от неё ушел парень. Это доступно только нам, людям. Эти ВС... Представь, что долгое время они могли собирать только страдания животных. Страдания простые: от отсутствия воды, еды, от боли, от ран. И питаться ими, этими страданиями. Назовем их Страданиями Первого Уровня. Пока понятно?

– Да.

– И вот однажды раз, и ВС совершают прорыв, они учатся производить Страдания Второго Уровня – они выводят человека! Это можно сравнить с тем, как люди тысячами лет сначала просто собирали забродившие фрукты, чтоб забалдеть. Потом научились делать брагу очень плохого качества. А потом кто-то придумал перегонный куб и научились делать виски!

Продавщица подала нам блины. Мы стали за столиком и с аппетитом принялись за них.

– Но я все же не могу понять, отчего нельзя собирать не негативные, а позитивные эмоции и питаться ими? – спросила Грэйси.

– Да потому что положительные эмоции это как будто уже что-то использованное, понимаешь? Ведь ты получила профит от того, что у тебя были положительные эмоции?

– Ну, вообще-то да.

– Ну и вот. Нельзя дважды съесть вот этот вот блин. Просто же.

– Ясно, понятно, – ответила Грация. Она подумала с минуту. – Ну, а эти накопители, которые собирают за нами наши негативные эмоции. Они к каждому человеку, что ли, приставлены?

– Я думаю да, – ответил я.

Мы доели блины, выбросили мусор и пустились дальше к выходу из парка.

– А как бы ты, кстати, представила себе этих сущностей? – спросил я. – Ну, которые собирают негативные эмоции?

– Да никак, – фантазию Грейси расшевелить было даже сложнее, чем мою.

– А я представляю их как некие сухие грибы. Которые наполняются соком из негативных эмоций. И превращаются... ну во что они могут превращаться?

– Понесло тебя... – ответила дочь. – В медуз. Раз уж были грибы. Мокрые грибы будут медузы.

– Годится! Так и назовем их, такие накопители – Медузы. После того, как они накопили достаточно негативных эмоций, их отжимают и снова превращают в грибы.

– Эх, папичка, папичка, – этой фразой дочь обычно показывала мне, что меня уже заносит на волне воображения.

– Что, не веришь мне? А хочешь... Хочешь, я словлю тебе одну такую медузу? Чтоб уж ты понимала, что я тут не просто фантазирую. А вообще-то все совершенно точно угадал про то, зачем нужны люди? Я словлю её, эту медузу, как ловят рыбу, и втяну из её пространства сюда, к нам, хочешь?

– Хочу.

***

На следующий день я проснулся и первым делом стал вспоминать вчерашний разговор с дочерью.

Все выходило действительно стройно. Не такая плохая теория. Люди существуют для того, чтобы выделять страдания, которые не умеют выделять животные. Что ж. Мне снова все понравилось.

Потом я вспомнил о том, как обещал Грейси втянуть в наше пространство Медузу-накопителя, и приуныл. С тем, чтобы втягивать кого-то из другого пространства в наше, были явные затруднения. Это меня, надо сказать, после двух литров сухого красного уже несколько действительно занесло.

Основная моя печаль была в том, что своего ребенка я никогда не обманывал в том, что касается обещаний. Так повелось с самого детства и, как мне кажется, на этом держалось многое в наших отношениях. Если уж я что-то обещал Грации, то мог расшибиться, однако сделать.

Но как расшибиться тут, чтобы втащить Медузу в нашу реальность, было совершенно непонятно.

Даже непонятно было, с чего начинать.

Однако тут же меня посетила мысль о том, что меня вообще-то никто не торопит. Потом я снова вспомнил о том, что если думать добросовестно, то додуматься можно до чего угодно. Загрузил всю информацию о Медузах в подсознание и стал заниматься своими делами.

Так прошло несколько недель.

***

– Добрый день, – сказал человек, которому я открыл дверь своей квартиры.

Я сразу узнал его, хотя до этого не видел ни разу в жизни наяву.

– Добрый, – ответил я.

Ступор, который охватил меня, не отпускал. Наяву этого человека я не видел, а вот во сне... Это произошло сегодняшней ночью. Даже нет, это было не ночью, это было утром. Дело в том... Дело в том, что в поисках ответа на вопрос, как мне втащить Медузу в нашу реальность, я стал практиковать ОСы – Осоз-

нанные Сновидения. Я занялся вопросом вплотную и набрел где-то на технику утреннего пробуждения. Состояла она в том, чтобы проснуться совсем ранним утром, а затем, находясь в легкой полудреме, попытаться попасть в пространство снов. Буквально два или три дня назад это у меня получилось, и я стал искать в этом пространстве Медузу. И вы знаете, у меня было ощущение, что она где-то здесь, Медуза, которую я искал.

Сегодня, когда я занимался поиском, в мой сон пришел господин, который сейчас стоял передо мной в дверях, погрозил мне тогда пальчиком и сказал буквально следующее:

– Что это вы тут балуете, Стецкий? Нехорошо. Сегодня к вам зайду, часа в три, будьте дома.

После этого я тут же проснулся. И сразу же понял, что влез в какую-то область, в которую соваться мне было никак нельзя. И тут же пришло железобетонное понимание, что этот человек, который грозил мне пальцем в моем ОСе, обязательно придет сегодня ко мне в три часа. Мне поплохело от страха. Я встал, сходил на кухню, выпил успокоительного и лёг обратно спать. На удивление, заснул я быстро. И когда я проснулся во второй раз, страх куда-то улетучился. Вообще вся эта история с угрожающим господином перестала казаться чем-то, что заслуживает большого внимания. А вот теперь этот человек стоял на пороге моей квартиры.

– Ну что, так и будем стоять? – спросил господин. Был он среднего роста, плечистый, восточного типа внешности. Глаза его в полумраке коридора показались мне непроницаемо черными. В ухе золотом блестела капля серьги.

– Проходите, – пробормотал я. Было совершенно ясно, что просто захлопнуть дверь перед этим человеком было никак нельзя. Ну, просто ни к чему хорошему это бы не привело.

Ассириец вошел – мне показалось, что это был именно ассириец – разулся, и я подал ему тапки. Мы прошли в кухню.

– Чаю? – как-то угодливо спросил я.

– Может быть, коньяку? – в руках ассирийца был пакет, которого я прежде не видел или не замечал. Не дожидаясь ответа, гость достал из этого пакета коробку с коньяком – это был семилетний «Арарат», и, пока я отлучался за бокалами, выложил на стол банку черной икры, багет и пачку сливочного масла. Я взял разделочную доску и стал сочинять бутерброды. Ассириец открыл коньяк и самостоятельно разлил коньяк по бокалам. Подал один бокал мне, сам взял второй.

– Ну, за сотрудничество, – сказал он, ударил своим бокалом о мой и влил коньяк в себя. Я поступил ровно также. Закусили бутербродами.

– За сотрудничество, – сказал я утвердительно. Коньяк несколько привел меня в чувство.

– Да, Саша, за него, – сказал гость и уселся на табурет. – Итак, вы назвали наши накопители Медузами и пытались втащить их в эту реальность.

Я промолчал. Эта осведомленность ввергла меня в столбняк.

– Ну во-первых, никакие это не Медузы, – сказал гость. – Скорее накопители похожи на большие тряпки. Вы были правы, их время от времени отжимают, когда они достаточно напитаются отрицательными человеческими эмоциями. Но втянуть их в нашу реальность… Александр Николаевич, таких самоуверенных людей, как вы – ещё поискать. Кто вам вообще сказал, что это возможно?

– Кто вы? – я налил ещё коньяку, себе и гостю. Теперь о его бокал я ударил своим и, не дожидаясь тоста, выпил.

– Зовут меня Анду Шмаил Шмувель Мирза Беньями, – ответил мой странный гость, и я отчего-то сразу же запомнил это имя. – Но для вас просто Тимур. Работаю я на тех, кого вы назвали высшими существами. Хотя тоже вопрос, насколько они высшие… Впрочем, ладно. Я из отдела Сотрудничества. Давайте теперь за него, за наш отдел.

Гость выпил. Слово «сотрудничество» прозвучало уже третий раз за последние пять минут. Я посмотрел на стол, понял, что Тимуру нечем закусить и стал торопливо мастерить следующий бутерброд.

– Благодарю, – сказал Анду Шмаил. Принял бутерброд и закусил. – Итак, вы думали добросовестно и додумались, верно?

– Ну, вам, мне кажется, видней, – ответил я.

– Верно, верно, – сказал ассириец. – Мне видней. В подпространство полезли зачем-то. Ларву хотели затащить сюда, вот умора. В общем, Саша. С такими, как вы, мы обычно заключаем контракт. С теми, кто додумался. Конечно, контракт мы заключаем и со многими другими. Изобретатель шахмат, к примеру, действительно получил столько зерен рису, сколько попросил, только платили ему мы, а не какой-то там падишах… Тот, кто придумал первым делать ставки на спорт, стал царем Микен. А тот, что придумал игру на бирже… У него сейчас свой остров. Вы понимаете, куда я клоню?

– Признаться, не до конца, – я скромничал. Пока мне вовсе не было понятно, куда клонит господин Беньями.

– С сегодняшнего дня вы будете работать над тем, чтобы совершенствовать количество сбора негативной людской энергетики, – сказал он. – А мы… Мы будем вам в этом всячески помогать.

В голове у меня заплясало сразу сто вопросов. Я задал тот, что показался мне наиболее логичным:

– И.... как вы будете мне помогать?

– В основном открывать каналы, по которым вы получаете творческие импульсы. Даже в вашем случае – просто чистить их, они у вас уже открыты. Но там столько всяких засоров, Саша, поверьте на слово, кошмарное количество мусора и грязи.

Я задумался.

– Так это что же получается... Вы меня ...эээ... нанимаете множить страдания?

– Ну хотите, назовите это так, – сказал ассириец и взял с тарелки ещё один бутерброд. – А то вы их не множите своими сценариями?

– Ну, как сказать... Стараюсь этого не делать.

– О душе печетесь?

– Ну, в общем-то, да.

– А с чего вы решили, что она у вас есть? Бросьте, Стецкий, никакой такой души у вас нет. Все, что с вами произойдёт – произойдет только в этой жизни. А после смерти свет потухнет – и всё.

– Ну, а если я вам скажу, что я вам не верю?

– Отчего же?

– Да просто оттого, что вам надо меня убедить работать на вас.

– Дурак вы, Стецкий, – сказал Анду Шмаил после некоторого размышления. – Богатым человеком бы вас сделал. Ерепенитесь чего-то... Душа какая-то. Ладно. Долгий разговор, нет на это времени. Или вы соглашаетесь с нами работать, Александр Николаевич. Или мы в 24 часа вас деактивируем. И никакого другого выбора у вас нет, Стецкий. Вам всё ясно?

– Да, – сердце у меня упало. Похоже, этот чёртов ассириец не блефовал.

– Ну, а раз ясно, так может станем договор подписывать?

– Э... вы сказали у меня есть 24 часа?

– Я сказал, что если вы откажетесь, то вы будете деактивированы в 24 часа.

– Ну хорошо... Понятно... Я не отказываюсь. Могу я подумать хотя бы до следующего утра?

Тимур посмотрел на часы.

– Хотя бы... Вы просите 18 часов, Саша. Впрочем, хорошо, – сказал он. – Но помните мою доброту, Стецкий!

Анду Шмаил Шмувель Мирза Беньями, сунул мне на прощание руку и пошел в коридор обуваться.

***

Я вылез из бассейна, взял полотенце, смахнул с себя воду, но тщательно вытираться не стал. На улице было ещё тепло, кажется градусов 25-27.

Я глянул на часы над входом в бассейн, подошел к столику и открыл ноут – трансляция должна была начаться через одну минуту. Зашел на наш сайт и включил необходимый канал. Понял, что хочу сейчас отведать шоколаду с горячим чаем, вышел с террасы на кухню, включил чайник. Тут ноутбук у бассейна выдал что-то похожее на аплодисменты и я попросил чайник закипать побыстрее.

– ... знаменательный день... ...несомненное достижение... – доносились из компьютера обрывки фраз, – не просто институт, а новый шаг в развитии человечества... историческое событие... многомиллионные инвестиции...

Чайник, наконец, закипел, я залил кипятком белый улун, который полюбил в последний месяц жизни здесь, в Касабланке, отломил от плитки порядочный кусок шоколаду и пошел смотреть трансляцию, которую ждал уже который день. Хотя, как ждал? Собственно, мне было почти фиолетово, откроют они вообще институт или нет – это уже была совсем не моя забота. Но детище, как ни крути, было моим, и определенный интерес к тому, что происходило вокруг него, у меня, конечно, был.

Выступающий с трибуны дядечка напомнил мне Евстигнеева из «Добро пожаловать...», который тоже был маленьким и у которого тоже была бабушка.

– Итак, мы собрали в нашем институте лучшие, не побоюсь этого слова, умы нашей планеты в области генетики, физиологии человека, химии, физики и программирования! Запольский, Гонтмахер, Мирошниченко, Браун, Иствальд, Гогенхейм, Хазин – разве вам ничего не говорят эти имена?

Лично мне эти имена на самом деле почти ничего не говорили. Но я верил Евстигнееву на слово, денег у проекта было столько, что было бы даже странно, если бы было по-другому. Я пил чай, ел шоколад, слушал этого почти лысого человека о сверкающих лабораториях в здании стекла и бетона и понимал, что директор нашего НИИ остался где-то в прекрасной стране с названием «СССР». Но что-то в нём было такое, за что его поставили руководителем нашего института, института «Homo digital». Может быть, чутье на лучших специалистов, может быть умение с ними ладить, может быть, способность объединить или увлечь всех этих людей. А может быть, и все сразу. Краем уха я однажды услышал, какая у нашего директора будет зарплата, и тогда на мгновение подумал, что ведь на его месте мог быть я.

– Не мог, – сказал я вслух. – Не глупи. Никто бы тебя не поставил директором.

Директор тем временем закончил, сошел с трибуны и на неё поднялся Анду Шмаил Шмувель Мирза Беньями.

– Кря, – только и сказал я. Интересно, а он какую будет занимать должность в институте? Ведь ничего, мерзавец, не сказал. Впрочем, Тимур оказался обычным пресс-секретарем. Кажется, этот человек не любил громких регалий.

Анду Шмаил, под которым сейчас находился титр «Тимур Азизбекян» говорил также, как и директор, то есть малозначащие патетичные фразы, а я вспоминал нашу с ним встречу на следующий день после того, как я узнал о существовании этого человека со странным именем.

– Понимаете, я не могу, – говорил я Тимуру на своей кухне. В этот раз мы пили чай – как раз белый улун, который я держал отдельно от других сортов чая специально для очень дорогих гостей.

– Если хотите, да, я пекусь о своей душе, – продолжил я. – И что если я сейчас стану работать тем, кем вы мне предлагаете, то ждет меня за это десятикратная расплата. Потому что в голове моей вбито намертво: если моя жизнь приносит окружающим страдания, пусть она будет как можно короче. Вы меня понимаете? То есть если говорить проще, то я должен согласиться с этой… как вы там назвали мою смерть?

– Деактивацией, – сказал Тимур.

– Ладно, – ответил я. – Деактивированным меня тоже быть не устраивает. В особенности, если окажетесь правы вы. И после деактивации меня ждет только свалка, гниение, распад и деструкция.

– Как ни печально, – сказал Анду Шмаил. – Так… Что же вы предлагаете?

– Я предлагаю Страдания Третьего Уровня, Тимур. Страдания, которые будут у нового, следующего типа человека.

Тут я сделал паузу, чтобы до Беньями дошел смысл сказанных мной слов.

До появления человека был только животный мир и у животных был только один вид страданий – страдания тела: голод, болезнь, боль, страх. У человека появился ещё один вид страданий – страдания ментальные. Страдания, не знакомые животным. Страдания из-за недостатка денег, страдания из-за несчастной любви, страдания из-за поражений в любого рода играх, или ставках, или спорах, страдания о будущих перспективах.

Когда я думал обо всем этом, меня посетила мысль: а почему это вдруг конец логической цепочки? Почему не может быть нового, следующего вида людей – я назвал их Digital Homo, которые будут вырабатывать новый вид страданий?

Шаг от нынешнего человека к Digital Homo мне представлялся таким же, как шаг от животного к человеку. И потому прямо сейчас даже сложно представить себе тот вид страданий, которые появятся у Digital Homo. Но в том, что они будут, я не сомневался. В конце концов точно так же, как для нового вида страданий выводили современного человека, будут выводить и Digital Homo.

– То есть точно также, как вы… ну или не вы, а кого вы там представляете… вывели человека, – продолжил я. – Я предлагаю вывести …ммм… ну давайте, пока у этого нового вида нет названия, назовем его упрощенно сверхчеловеком. С рабочим именем, скажем… Ну пусть Homo digital.

– Гм, – сказал Тимур. Он застыл на некоторое время с чашкой в руке. Когда я решил, что пауза затянулась, он, наконец, отмер.

– И почему это был не я? – сказал он.

– Простите?

– Очевидно, что идея проста, как все гениальное, – сказал, уставясь теперь в окно, Анду Шмаил. – И что, как и любую простую гениальную идею, это должен был высказать кто-то первым.

Тимур смотрел в окно и о чем-то, кажется, напряженно думал и, наконец, изрек:

– Присаживайтесь, давайте. Итак, мне нужны подробности.

Я пододвинул к себе стул и, ещё слегка зачарованный происходящим, произнёс.

– Ну, когда я вспомнил своё сравнение страданий разного уровня с брагой, которую пили веками – начал я, – и которую только в десятом веке кто-то догадался залить в перегонный куб. Я подумал, что в нашем богатом мире все не заканчивается только лишь виски…

Именно тогда, в ту секунду, происходило зарождение того, что я сейчас наблюдал в экране своего монитора. Зарождение огромного научного института с названием «Институт изучения цифрового человека». Коротко – НИИ «Homo digital». Вообще я был только за второе название. От первого веет каким-то неимоверным пафосом. Как можно изучать цифрового человека, если его пока нет? Но это уже был вопрос не моей компетенции.

Да и черт бы с ним, хоть горшком называйте.

Спасибо, что в печь не поставили.

Совсем отвертеться от контракта с ними мне, конечно же, не удалось.

Однако мой контракт подразумевает только лишь разработки по изобретению Homo digital. Сверхчеловека. У которого, возможно, будут сверхстрадания.

Перед тем, как я подписал документы, я пере-

брал все то, за что по моим представлениям на том свете полагается наказание. И не нашел ни одну статью, которую мне мог бы вменить архангел Гавриил. Или кто там наверху вменяет статьи?!

Я вроде бы не поступал так, чтоб перед смертью переживать о том, что же это я такое натворил за жизнь?

Даже смею надеяться на большее.

Вот скажите: лично вы рады, что кем-то когда-то был создан человек!?

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 *accda@c3da.org, info@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.