ISSN 2686-9373

ВЕСТНИК СОВРЕМЕННЫХ ЦИФРОВЫХ ТЕХНОЛОГИЙ

11. 2022 (ИЮНЬ)

Главный редактор

д.т.н., проф., академик РАЕН

Щербаков А.Ю.

Ученый секретарь Редакционного совета

Рязанова А.А.

Верстка Груздева Н.В.

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

№11
ИЮНЬ 2022

www.c3da.org

ISSN 2686-9373

Издатель: *Ассоциация специалистов в области развития криптовалют и цифровых финансовых активов*

Адрес редакции и издателя: 125167, Москва, Ленинградский пр-т, д.43, к.2, оф. 128
Тел/факс: *8 (499)157-37-34*
E-mail: accda@c3da.org, info@c3da.org

Подписано в печать 30.06.2022 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 – 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.

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.

Гостев Сергей Сергеевич, кандидат технических наук, первый заместитель генерального директора АО «Концерн «Гранит».

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 4

1. ЦИФРОВЫЕ ТЕХНОЛОГИИ В ОБРАЗОВАНИИ

С.В. Запечников – Актуальные зарубежные образовательные практики в области искусственного интеллекта: содержательное наполнение образовательных программ
S.V. Zapechnikov – Current foreign educational practices in the field of artificial intelligence: curricula and content of educational programs 5

А.Ю. Щербаков – Основные положения установочной лекции для введения в криптографию и криптографические методы защиты информации
A.Yu. Shcherbakov – The main thesis to the introductory lecture in cryptography and cryptographic methods of information security 27

2. ЭКОНОМИЧЕСКИЕ ПРОБЛЕМЫ ЦИФРОВЫХ ТЕХНОЛОГИЙ

Д.С. Мачихин – Индустрия криптовалют России в мировом контексте: анализ актуального состояния
D.S. Machikhin – Russian cryptocurrency market in a global context: analysis of the current state 33

3. ЦИФРОВЫЕ ТЕХНОЛОГИИ В ПРОМЫШЛЕННОСТИ

Д.С. Лазорин, Д.И. Правиков, А.Ю. Щербаков – О подходах к обеспечению информационной безопасности цифровых двойников
D.S. Lazorin, D.I. Pravikov, A.Yu. Shcherbakov – On approaches to the ensuring information security of digital twins 48

АССОЦИАЦИЯ РКЦФА

Ассоциация специалистов
в области развития криптовалют
и цифровых финансовых активов

Мы не предсказываем цифровое будущее.
Мы его создаём!

c3da.org
accda@c3da.org
info@c3da.org

Ассоциация РКЦФА - объединение ведущих российских специалистов в области цифровых технологий.

В нашем портфолио - целый ряд уникальных успешных проектов в области разработки и сертификации распределенных реестров, цифровых платформ и токенов, высокозащищеных систем технической и финансовой прогностики и мониторинга, а также семантического искусственного интеллекта.

Единственная в России ассоциация, занимающаяся фундаментальными и прикладными аспектами современных цифровых технологий, в первую очередь - распределенными реестрами и цифровыми активами.

Мы ведём
авторские обучающие программы и курсы
в области цифровых технологий и криптографии
для технологических лидеров России.

РЕДАКЦИОННОЕ ПРИМЕЧАНИЕ

Одиннадцатый номер нашего журнала выходит на фоне непростых мировых событий, касающихся, в том числе, сферы цифровых технологий и кардинально меняющих не только направление развития мировой и российской национальной экономики, но и социально-стратификационную структуру общества. При этом достаточно актуальными становятся, среди прочих, проблемы распространения криптовалют и связанных с ними технологий, а также вопросы трансформации подходов к образованию в области современных информационных технологий, так или иначе затрагиваемые в работах этого выпуска.

Раздел «Цифровые технологии в образовании» открывает статья Сергея Запечникова **«Актуальные зарубежные образовательные практики в области искусственного интеллекта: содержательное наполнение образовательных программ»**, которая является продолжением публикации десятого выпуска Вестника, посвященной организационным и методическим аспектам зарубежных образовательных программ в области искусственного интеллекта.

В статье представлен анализ содержательного наполнения зарубежных университетских дисциплин, сгруппированных по блокам: математические и теоретические основы искусственного интеллекта, теория и методология искусственного интеллекта, практические проблемы машинного обучения, интеллектуальный анализ больших данных, компьютерное зрение, обработка естественных языков, интеллектуальная робототехника. Рассмотрены возможности и перспективы использования зарубежного опыта в российском высшем образовании.

Раздел продолжается статьей Андрея Щербакова **«Основные положения установочной лекции для введения в криптографию и криптографические методы защиты информации»**, предлагающей новый взгляд на проблему совершенствования подачи учебного материала о современных методах криптографической защиты информации. Статья предназначена преподавателям, читающим курсы основ криптографии и компьютерной безопасности для слушателей, подготавливаемых в рамках вузовских программ и дополнительного профессионального образования.

Излагаемый материал будет полезен для формирования правильного понятийно-методологического взгляда на предмет криптографической защиты информации.

В разделе «Экономические проблемы цифровых технологий» представлена статья **«Индустрия криптовалют России в мировом контексте: анализ актуального состояния»** Дмитрия Мачихина, основателя сервиса для легализации и налогообложения криптовалют, инвестора и предпринимателя в области информационных технологий. В данной работе рассмотрена динамика показателей мирового рынка криптовалюты Биткоин, представлены показатели проектов, связанных с технологией блокчейн криптовалют и смежными технологиями, такими как невзаимозаменяемые токены, метавселенные и децентрализованные финансы.

Автором приведен подробный анализ мирового объема рынка, доли России в нем и перспектив майнинга в России. Весьма ценную информацию представляют собой расчет потенциального дохода от рассмотренных в статье видов деятельности для российского бюджета и оценка влияния возможного запрета криптовалют на экономику, скорость технического развития, инвестиционный климат в стране.

Раздел «Цифровые технологии в промышленности» открывает в журнале новую тему цифровых двойников. Студент РГУ нефти и газа имени И.М. Губкина Данил Лазорин, подкрепленный научно и методически нашими опытными членами редакционного совета, представил вниманию и критическому осмыслению читателей статью **«О подходах к обеспечению информационной безопасности цифровых двойников»**.

В статье рассмотрены существующие подходы и методы обеспечения информационной безопасности цифровых двойников, показано, что практически ни один из практикуемых подходов не обеспечивает достижения их системной безопасности. Предложена реализация комплексного подхода в рамках актуальных для цифровых двойников специфических моделей угроз и нарушителя.

УДК: 004.8

Актуальные зарубежные образовательные практики в области искусственного интеллекта: содержательное наполнение образовательных программ

S.V. Zapechnikov

Current Foreign Educational Practices in the Field of Artificial Intelligence: Curricula and Content of Educational Programs

Abstract. *The article analyzes the content of foreign university educational programs in the field of artificial intelligence (AI). The main design principles of educational trajectories of bachelors and masters in the field of AI are considered. The following briefly discusses the content of the main academic disciplines, grouped into several blocks, including mathematical and theoretical foundations of AI, theory and methodology of AI, practical problems of machine learning, intelligent analysis of big data, computer vision, natural language processing, intelligent robotics, bioinformatics, cognitive research and neuroscience. The article concludes with an analysis of the possibilities and prospects of using foreign experience in Russian higher education.*

The article is a continuation of the publication in the last issue of the journal, which was devoted to organizational and methodological aspects of foreign educational programs in the field of AI.

Keywords: *artificial intelligence technologies, machine learning, deep learning, computer vision, natural language processing, robotics.*

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 анализируется содержательное наполнение зарубежных университетских образовательных программ в области искусственного интеллекта (ИИ). Рассматриваются принципы формирования образовательных траекторий бакалавров и магистров в сфере ИИ. Далее кратко рассматривается содержание основных учебных дисциплин, сгруппированных по блокам: математические и теоретические основы ИИ, теория и методология ИИ, практические проблемы машинного обучения, интеллектуальный анализ больших данных, компьютерное зрение, обработка естественных языков, интеллектуальная робототехника. Завершается статья анализом возможностей и перспектив использования зарубежного опыта в российском высшем образовании. Статья является продолжением публикации в прошлом номере журнала, посвященной организационным и методическим аспектам зарубежных образовательных программ в области ИИ.*

Ключевые слова: *технологии искусственного интеллекта, машинное обучение, глубокое обучение, компьютерное зрение, обработка естественных языков, робототехника.*

ВВЕДЕНИЕ

В прошлом номере журнала была опубликована статья, посвященная анализу организационных и методических аспектов зарубежных образовательных программ в области искусственного интеллекта (ИИ). В результате проведенного анализа зарубежных образовательных практик были выявлены следующие принципиальные особенности сложившейся в западных университетах системы высшего образования:

1) образование имеет глубоко индивидуализированный характер;

2) отсутствует государственное регулирование содержания образования;

3) университетская среда высококонкурентна: учебные заведения конкурируют за профессоров и студентов, профессора конкурируют за студентов и за гранты, студенты конкурируют между собой;

4) большинство университетов относятся к университетам классического типа, поэтому способны к широкому охвату своей деятельностью многих областей знания и междисциплинарности;

5) университет является саморегулируемым сообществом, основанным на сплаве энтузиазма и бизнес-интересов, что определяет продуктивность и успешность его деятельности в

современном мире;

6) сложившаяся в западном мире модель высшего образования демонстрирует свою успешность в современном мире и высокий потенциал развития, в связи с чем заслуживает всестороннего изучения и интеграции лучших практик в отечественное высшее образование.

Настоящая часть работы (вторая и заключительная) посвящена анализу содержательного наполнения образовательных программ. Статья начинается с анализа принципов формирования образовательных программ бакалавриата и магистратуры в сфере ИИ. Далее анализируются отдельные учебные дисциплины по следующим направлениям: математические и теоретические основы ИИ, теория и методология ИИ, практика машинного обучения, интеллектуальный анализ больших данных, компьютерное зрение, обработка естественных языков, интеллектуальная робототехника. Завершается статья построением примерного учебного плана по направлению подготовки в области ИИ, сконструированному из наиболее заметных дисциплин зарубежных университетов.

В приложении к статье приводится перечень известных автору учебников по базовым дисциплинам в области ИИ.

1. ПРИНЦИПЫ ФОРМИРОВАНИЯ ОБРАЗОВАТЕЛЬНЫХ ТРАЕКТОРИЙ БАКАЛАВРОВ И МАГИСТРОВ В СФЕРЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Индивидуальные образовательные траектории студентов, обучающихся по программам бакалавриата и магистратуры, как отмечалось ранее, строятся в основном на принципах добровольного и осознанного выбора студентами изучаемых дисциплин. В современных условиях формирование индивидуальных учебных планов может быть полностью автоматизировано и осуществляться при помощи личного кабинета студента на сайте университета. Однако с целью сохранения преемственности между изучаемыми дисциплинами и системности получаемого образования всегда имеются некоторые ограничения в выборе студентом изучаемых дисциплин.

Ещё одна особенность «западной» модели многоступенчатого образования – отсутствие фиксированной продолжительности обучения по программе бакалавриата и магистратуры. Например, на освоение программы бакалавриата может быть предусмотрено от 2 до 4 лет, программы магистратуры – от 2 до 5 лет. За время обучения требуется набрать не менее порогового числа «кредитов», т.е. зачётных единиц трудоёмкости, в которых оценивается каждый успешно пройденный курс. Например, по программе бакалавриата – не менее 180, по программе магистратуры – не менее 120. При этом студент должен набирать за год учёбы не менее порогового количества «кредитов», например, не менее 45.

Отсутствие фиксированной продолжительности освоения учебной программы приводит к тому, что студент во взаимодействии с преподавателями работает «на результат», т.е. освоение программы бакалавриата (магистратуры) завершается тогда, когда соблюдены все необходимые и достаточные условия, включая выполнение промежуточных проектов и дипломного проекта, и получен качественный результат.

Рассмотрим на примере Стэнфордского университета основные принципы формирования ***учебного плана бакалавра***. Как утверждается в соответствующем разделе «Бюллетеня Стэнфорда» [1], миссия программы бакалавриата по компьютерным наукам состоит в том, чтобы развить у студентов широту знаний по предметным областям информатики, включая их способность применять основные положения информатики, пользоваться абстракциями, обладать способностями к проектированию и реализации для решения прикладных задач. Студенты проходят набор основополагающих курсов. После изучения основных методов программирования и математических основ информатики студенты проходят курсы в таких областях, как методы программирования, теория автоматов и сложности, системное программирование, компьютерная архитектура, анализ алгоритмов, искусственный интеллект и приложения. Программа готовит студентов к карьере в государственном, юридическом и

корпоративном секторах, а также к обучению в аспирантуре.

Студенты, поступающие в Стэнфорд, имеют совершенно разный опыт и цели, но большинство из них считают, что умение эффективно использовать компьютеры полезно для их образования. Университет предлагает множество вводных курсов для удовлетворения потребностей этих студентов. Вместе с тем, программа бакалавриата подразумевает выполнение студентом следующих базовых требований:

• освоение дисциплин в области математики в объёме не менее 26 «кредитов»;

• освоение общенаучных дисциплин в объёме не менее 11 «кредитов»: два обязательных курса физики и одна общенаучная дисциплина по выбору: химия, биология, науки о Земле и пр.;

• освоение по крайней мере одной дисциплины, посвященной технологиям в человеческом обществе в объёме 3-5 «кредитов»;

• освоение дисциплин в области инженерного дела в объёме не менее 13 «кредитов», в том числе курсов основ программирования и основ инженерии;

• освоение дисциплин в области основ компьютерных наук в объёме не менее 15 «кредитов», в том числе курсов организации компьютеров и вычислительных систем, принципов построения операционных систем, конструирования и анализа алгоритмов.

Перечисленные требования относятся к общенаучной подготовке. После её завершения студенту необходимо сконструировать траекторию таким образом, чтобы получить специализацию в одной из следующих областей:

• искусственный интеллект;
• биовычисления;
• компьютерная инженерия;
• компьютерная графика;
• человекомашинное взаимодействие;
• обработка информации;
• системная инженерия;
• теоретическая информатика;
• обучение без конкретной специализации.

Для всех специализаций предлагаются многочисленные дисциплины по выбору.

Детально все требования к студентам изложены в специальном ежегодно обновляемом справочнике Инженерной школы Стэнфорда [2].

Остановимся на требованиях по специализации в области ИИ. Студент должен выбрать дисциплины по крайней мере из двух из четырёх следующих областей: методы ИИ, обработка естественных языков, компьютерное зрение, робототехника. Кроме этого, необходимо выбрать хотя бы один непрофильный курс и хотя бы один курс по выбору из предлагаемых для каждой специализации списков. От студента бакалавриата требуется также пройти обучение хотя бы по одному курсу, развивающему навыки научного письма и презентации результатов своей работы, а также выполнить итоговый проект. Для получения диплома с отличием выдвигаются дополнительные требования как в части изучаемых дисциплин и оценок за них, так и в части требований к выполняемым студентом проектам. Следует отметить тщательную проработанность всех требований и рекомендаций, что сводит к минимуму повторы и (или) пересечения в содержании разных дисциплин, изучаемых студентами.

Ожидается, что студенты, завершившие обучение по программе бакалавриата, смогут продемонстрировать следующие результаты обучения:

• применять знания в области математики, естественных наук и инженерии;

• разрабатывать и проводить эксперименты, а также анализировать и интерпретировать данные;

• разрабатывать систему, компонент или процесс для удовлетворения желаемых потребностей в рамках реалистичных ограничений, таких как экономические, экологические, социальные, политические, этические, здоровье и безопасность, технологичность и устойчивость;

• работать в междисциплинарных командах;

• выявлять, формулировать и решать инженерные проблемы;

• понимать свою профессиональную и этическую ответственность;

• выстраивать эффективные коммуникации с коллегами;

• понимать влияние инженерных решений в глобальном, экономическом, экологическом и

социальном контексте;

• демонстрировать практическое знание современных проблем;

• применять методы, навыки и современные инженерные инструменты, необходимые для инженерной практики;

• переходить от инженерных концепций и теории к реальным инженерным приложениям.

Рассмотрим теперь на примере того же Стэнфорда основные принципы формирования ***учебного плана магистра***. Как отмечается в соответствующем разделе «Бюллетеня Стэнфорда» [3], цель магистерской программы – предоставить студентам знания и навыки, необходимые для профессиональной карьеры или соискательства степени Ph.D. Области возможной специализации студента в магистратуре включают ИИ, биокомпьютеры, компьютерную и сетевую безопасность, взаимодействие человека и компьютера, управление информацией и аналитику, вычисления в реальном мире, теорию программного обеспечения, системы и теоретическую информатику.

Требования к содержательной части образовательной траектории магистра складываются из пяти составляющих:

• основные требования;
• достаточный опыт реализации ПО;
• широта образования;
• наличие специализации;
• изучение курсов по выбору.

Рассмотрим более подробно эти требования. Основные требования включают в себя изучение ряда базовых курсов по логике, теории автоматов, теории вычислимости, теории вероятностей, анализу алгоритмов, организации компьютерных систем и принципам функционирования компьютерных систем в объёме не менее 10 «кредитов». Второе требование состоит в том, что студенты должны пройти по крайней мере один курс, обозначенный как имеющий значительный компонент реализации программного обеспечения. Требование широты образования подразумевает, что студенты должны пройти по крайней мере три курса, причем каждый курс выбирается из разных областей: математические и теоретические основы информатики, компьютерные системы, приложения, информатика и общество. Из каждой области должен быть выбран хотя бы один курс объёмом не менее 3 «кредитов». Четвёртое требование подразумевает, что студент в период обучения на магистерской программе должен приобрести специализацию. Университет предлагает 9 готовых специализаций. В особых случаях студент может приобрести иную специализацию, но она предварительно должна быть одобрена комитетом магистерских программ. Предлагаемые специализации таковы:

• искусственный интеллект;
• биовычисления;
• компьютерная и сетевая безопасность;
• человекомашинное взаимодействие;
• управление информацией и аналитика;
• вычисления для реального мира;
• теория программного обеспечения;
• компьютерные системы;
• теоретическая компьютерная наука (информатика);

Требование изучения курсов по выбору подразумевает, что студент за период обучения по магистерской программе должен выбрать дополнительные технические и нетехнические дисциплины, гармонирующие с его специализацией, согласованные с научным руководителем или администратором магистерской программы.

Всем студентам, обучающимся на магистерской программе, обеспечиваются консультации и научное руководство, однако инициатива в консультационных отношениях всегда возлагается на студента. Для получения диплома с отличием за период обучения на магистерской программе требуется выполнить расширенную исследовательскую программу и получить одобрение своих результатов по меньшей мере от двоих исследователей университета.

2. УЧЕБНЫЕ ДИСЦИПЛИНЫ ПО МАТЕМАТИЧЕСКИМ И ТЕОРЕТИЧЕСКИМ ОСНОВАМ ИИ

Перейдем к предметной характеристике зарубежных образовательных программ в области ИИ. За основу также был взят Стэнфордский

университет, по необходимости к учебным курсам Стэнфорда добавлялись программы других университетов, в ряде случаев – коммерческих компаний, для которых образование не является основным профилем деятельности. Однако это обстоятельство не является принципиальным – нашей целью в данном случае было выстраивание логического каркаса, являющегося основой содержательного наполнения образовательных программ в сфере ИИ.

В качестве общенаучного курса, подготавливающего к изучению дисциплин в области ИИ, в Стэнфордском университете рекомендуется курс вычислительной логики.

Курс ***«Введение в логику» (Introduction to Logic)*** [4] посвящен основам логики и рекомендуется будущим создателям систем ИИ, поскольку логика – самый мощный из инструментов человеческого интеллекта. Курс знакомит с различными логическими системами: пропозициональной, реляционной, функциональной логиками. В качестве предварительных требований к студентам выдвигается наличие представлений о математических основах вычислений.

Элементарные основы ИИ представлены в виде двух курсов: курса принципов и технологий ИИ и курса машинного обучения. От студентов, приступающих к изучению этих курсов, предполагается знание основ высшей математики (calculus), теории вероятностей и основ организации компьютерных систем. Для всех курсов также по умолчанию подразумевается уверенное владение приемами программирования.

Курс ***«Искусственный интеллект: принципы и технологии» (Artificial Intelligence: Principles and Techniques)*** [5] – обязательный базовый курс для студентов, обучающихся в сфере ИИ. В нем дается классификация моделей ИИ и обзорно изучаются четыре основных класса моделей: рефлексивные модели, модели, основанные на состояниях, модели, основанные на переменных, и логические модели. Для каждого типа моделей изучается цикл их обучения, применения, оценки.

Курс Стэнфордского университета ***«Машинное обучение» (Machine Learning)*** [6] – также обязательный. Это своего рода классика ИИ – курс, который составляет ядро знаний об ИИ. В курсе проводится обзор всех основных моделей машинного обучения от простейших до весьма сложных. Разделы курса посвящены концепциям обучения с учителем и без учителя, обучению с подкреплением, основам глубокого обучения, введению в теорию обучения, вопросам робастности и устойчивости обучения.

К этим двум курсам в сети имеется неплохой набор «шпаргалок», а фактически – справочник, созданный студентами [7].

Имеется специализация на платформе Coursera, состоящая из нескольких курсов, по содержанию (почти) эквивалентная этому курсу [8].

Похожий по содержанию базовый курс с таким же названием читается в Гарварде [9]. Он включает в себя следующие разделы: регрессия, классификация, нейронные сети, метод опорных векторов, кластеризация, понижение размерности, графические модели, модели статистических смесей, скрытые марковские модели, введение в обучение с подкреплением.

Следует отметить, что существенное внимание в обоих курсах уделяется, во-первых, сквозным технологиям современного машинного обучения, таким как численные методы градиентной минимизации, ядерные методы и др., во-вторых, методам повышения производительности вычислений и, в-третьих, эффективным методам подбора гиперпараметров алгоритмов.

Среди читаемых в российских университетах курсов машинного обучения наиболее полным и фундаментальным и в этом смысле идейно близким упомянутым выше курсам, пожалуй, можно считать курс «Машинное обучение» К. Воронцова [10].

Курс Стэнфордского университета ***«Глубокое обучение» (Deep Learning)*** [11] знакомит с основными идеями в этой весьма актуальной сегодня сфере ИИ: с архитектурой глубоких сетей, модульными принципами их построения, идеей автоматического выделения признаков объектов и пр. Этот курс – практико-ориентированный, в ходе которого студенты знакомятся со стратегиями реализации проектов в об-

ласти машинного обучения. В нем разбирается немалое число примеров: от медицинской диагностики и до машинного перевода, от трехмерной реконструкции изображений до игры в го. Одновременно это и своего рода профориентационный курс, в нем даются ориентиры по дальнейшим специализациям: что нужно изучить тем, кто хочет заниматься компьютерным зрением, обработкой естественных языков и др. направлениями.

Напомним, что в основе современного глубокого обучения лежит одна очень важная идея: все объекты обучающей и тестовых выборок, независимо от их природы (слова или отдельные морфемы в тексте, вершины, ребра, подграфы, графы и др.) сначала представляются в виде векторов латентного линейного пространства (при этом не требуется, чтобы измерения этого пространства имели какую-либо семантическую интерпретацию), а потом эти векторы могут обрабатываться какими угодно алгоритмами машинного обучения в зависимости от конкретной задачи: линейной регрессией, методом опорных векторов, нейросетями и др.

Имеется специализация на платформе Coursera, состоящая из нескольких курсов, по содержанию (почти) эквивалентная этому курсу [12].

Помимо вышеупомянутого курса, следует отметить ещё два примера базовых курсов по глубокому обучению.

Первый – это ***авторский курс Яна Лекуна*** с таким же названием [13]. Он читается как на открытых платформах, так и в ряде университетов (лично автором, либо его ассистентами). Курс включает следующие разделы: введение, параметризация моделей, энергетические модели, ассоциативная память, графы, управление, оптимизация.

Второй – ещё один ***авторский курс «Погружение в глубокое обучение» (Dive into Deep Learning)*** читается онлайн, в университетах и на школах по ИИ. Курс большого объёма, включает в себя следующие разделы: введение, линейные нейросети, многослойные перцептроны, вычисления в глубоком обучении, свёрточные нейронные сети, архитектура современных свёрточных нейросетей, рекуррентные нейронные сети, архитектура современных рекуррентных нейросетей, механизмы внимания, алгоритмы оптимизации, производительность вычислений, компьютерное зрение, обработка естественных языков: предварительное обучение и приложения, рекомендательные системы, генеративные состязательные сети.

По курсу имеется учебник [14], представленный в электронном виде и потому регулярно обновляемый. Два варианта учебника включают в себя примеры реализации рассматриваемых методов на языке Python с библиотеками MXNet либо PyTorch. Учебник имеет справочные разделы: математика для глубокого обучения, инструменты для глубокого обучения.

Три названные выше дисциплины являются основополагающими, поэтому их изучение (почти) обязательно для всех, кто специализируется на ИИ. Остальные курсы, рассматриваемые далее, посвящены отдельным очень большим и важным разделам ИИ (преимущественно, машинного обучения), но имеют уже более узкий фокус и глубокое содержание, поэтому предполагается, что студенты, как правило, будут выбирать некоторое подмножество этих курсов в соответствии со своими интересами и желанием специализироваться на конкретных разделах науки об ИИ.

3. ДИСЦИПЛИНЫ ПО ТЕОРИИ И МЕТОДОЛОГИИ ИИ

Первым по порядку рассмотрим блок дисциплин, предназначенных в первую очередь студентам, которые планируют строить карьеру в академической сфере. Отдельные дисциплины из этого перечня также могут быть полезны студентам, планирующим стать практиками, но нуждающимся в углублённых знаниях по своему профилю.

Курс ***«Принятие решений в условиях неопределенности» (Decision Making Under Uncertainty)*** [15] знакомит с основами науки об интеллектуальном (само-)управлении, которая является продолжением и развитием классической теории автоматического управления. Разделы курса посвящены вероятностному выводу причинно-следственных связей, после-

довательному решению задач, неопределенности моделей и состояний, мультиагентным системам. В курсе прослеживается множество междисциплинарных подходов на стыке с теорией игр, методами оптимизации, теорией марковских процессов, численными методами аппроксимации, динамическим программированием и другими дисциплинами.

Курс ***«Обучение с подкреплением» (Reinforcement Learning)*** [16] посвящен одноименной быстрорастущей отрасли машинного обучения. Он включает в себя множество разделов, знакомящих с идеями табличного планирования марковских процессов принятия решений, табличной оценки политик обучения с подкреплением, Q-обучением, обучением с подкреплением с аппроксимацией функций, поиска политик, быстрого обучения, пакетного обучения с подкреплением, древовидного поиска Монте-Карло, планированием ценности и вознаграждений. Курс является в значительной степени практико-ориентированным. На платформе Coursera также имеется специализация, по содержанию практически эквивалентная этому курсу.

Курс ***«Глубокие генеративные модели» (Deep Generative Models)*** [17] посвящен вероятностным основам и алгоритмам обучения глубоких генеративных моделей, включая вариационные автокодировщики, генеративные состязательные сети, авторегрессионные модели, модели нормализации потоков, энергетические и скоринговые модели. Приложения моделей включают в себя такие области, как компьютерное зрение, обработка речи и естественных языков, глубокий анализ графов, обучение с подкреплением, решение обратных задач.

Имеется специализация на платформе Coursera [18], состоящая из трех курсов:

- базовые генеративные состязательные сети (введение в генеративные сети, глубокие свёрточные генеративные сети, генеративные сети Вассерштейна с градиентными штрафами, условные генеративные сети и контролируемая генерация);
- расширенные генеративные состязательные сети (оценка генеративных состязательных сетей, недостатки и отклонения генеративных состязательных сетей, StyleGAN и достижения);
- применения генеративных состязательных сетей (генеративные состязательные сети для аугментации данных и приватности, трансляция из рисунка в рисунок при помощи Pix2Pix, непарная трансляция с CycleGAN).

Курс ***«Машинное обучение на графах» (Machine Learning with Graphs)*** [19] включает в себя следующие темы: введение в машинное обучение на графах, традиционные методы машинного обучения на графах, эмбеддинг узлов графа, анализ ссылок (PageRank), распространенные методы классификации узлов, графовые нейронные сети, приложения графовых нейросетей, теория графовых нейросетей, эмбеддинги графов знаний, вывод обоснований над графами знаний, поиск часто встречающихся подграфов, структура сообществ в сетях, традиционные генеративные модели для графов, глубокие генеративные модели для графов, дополнительные сведения о графовых нейросетях, масштабирование графовых нейросетей.

Графовые нейросети — это весьма специфические архитектуры, которые обладают свойствами инвариантности относительно перестановки вершин графа и эквивариантности относительно перестановки представлений вершин в латентном пространстве. Из-за этих требований к графам невозможно применять обычные нейросети. Однако, как это нередко бывает в науке, оказалось, что ранее известные архитектуры нейросетей, а именно, сверточные сети и сети-трансформеры, выводятся из графовых сетей как частные случаи.

Курс ***«Геометрическое глубокое обучение» (Geometric Deep Learning)*** [20] включает такие разделы как машинное обучение в признаковых пространствах большой размерности, геометрические основы симметрии, геометрические структуры данных, модели геометрического глубокого обучения, проблемы и приложения геометрического глубокого обучения, историческая перспектива.

Геометрическое глубокое обучение – это зарождающаяся наука об обобщении всех известных до сих пор форм машинного обучения, включая и графовое, которые будут выводиться из него как частные случаи. Кроме уже известных, из этой теории появится множество ранее

неизвестных концепций машинного обучения: обучение на группах симметрий, на многообразиях, алгебро-геометрическое обучение, машинное обучение многомерных признаковых пространств, геодезическое обучение и пр. Чем больше размерность признакового пространства, тем сильнее сказывается "проклятие размерности": если для объектов с 1 признаком в обучающей выборке достаточно иметь N прецедентов, то для объектов с 2 признаками – уже N2, чтобы с таким же качеством обучить модель, для объектов с M признаками- уже NM прецедентов и т.д. Чтобы преодолеть эту проблему, создатели геометрического глубокого обучения пошли по пути "универсальной геометрии", которую в свое время наметил Клейн в своей Эрлангенской программе: он сформулировал, что разные геометрии (евклидова, Лобачевского, риманова и др.) отличаются между собой инвариантами, которые можно выразить алгебраически. Идея геометрического глубокого обучения состоит в том, чтобы для исследования объектов различной природы (текста, изображений, графов и в будущем еще более сложных структур данных) строить глубокие сети, которые будут обладать свойствами инвариантности относительно каких-либо групповых операций (преобразований симметрии и др.).

Курс ***«Вероятностные графические модели: принципы и технологии» (Probabilistic Graphical Models: Principles and Techniques)*** [21] посвящен изучению следующих тем: теория вероятностей и байесовские сети, ненаправленные модели, обучение байесовских сетей, точное предсказание, формирование выборок, структурные предсказания, обучение параметров, байесовское обучение, структурное обучение, экспоненциальные семейства, вариационный вывод и некоторые другие темы.

Курс ***«Теория машинного обучения» (Machine Learning Theory)*** [22] включает в себя следующие разделы: обучение с учителем, минимизация эмпирического риска, асимптотический анализ, равномерное схождение, неравенство Хёффдинга, равномерная сходимость, конечный класс гипотез, дискретизация бесконечного пространства гипотез, расширенные неравенства концентрации, сложность по Радемахеру, в том числе эмпирическая, теория отступов и сложность по Радемахеру для линейных моделей, проблемы теории глубокого обучения, границы обобщения для нейросетей, связь с ядерными методами, подход покрывающих чисел, теорема Дудля и её следствия, границы обобщающей способности для глубоких сетей, невыпуклая оптимизация и её применения для метода главных компонент, умножения матриц и декомпозиции тензоров, тангенциальные ядра для нейросетей, неявная регуляризация градиентного спуска, неявный регуляризующий эффект инициализации, неявная регуляризация в задачах классификации, неявный регуляризующий эффект шумов, обучение без учителя, смесь гауссовских распределений, метод моментов, анализ алгоритмов самообучения, анализ алгоритмов контрастного обучения.

Курс ***«Глубокое многозадачное обучение и метаобучение»*** **(Deep Multi-task and Meta Learning)** [23] посвящен одному из самых бурно развивающихся направлений современного машинного обучения и включает в себя следующий круг вопросов: многозадачное обучение с учителем, трансферное обучение, постановка задачи метаобучения, метаобучение по принципу «чёрного ящика», оптимизационное метаобучение, обучение на небольшом числе примеров через метрическое обучение, байесовское метаобучение, многозадачное обучение с подкреплением и целеобусловленное обучение с подкреплением, основанное на моделях обучение с подкреплением для многозадачного обучения, метаобучение с подкреплением: адаптируемые модели и политики, обучение приобретению новых знаний, автономное (оффлайновое) обучение с подкреплением и многозадачное обучение с подкреплением, иерархическое обучение с подкреплением и приобретение знаний, обучение в течение всего жизненного цикла: постановка задачи, прямой и обратный перенос, новые горизонты и нерешённые проблемы и др. вопросы. Это курс без учебника – он строится на материалах многочисленных научных статей.

Курс ***«Актуальные вопросы искусственного интеллекта» (Topics in Artificial Intelligence)***

[24] задуман как продвинутый курс, в котором подробно исследуются несколько важных классов алгоритмов современного машинного обучения. Курс сосредоточен на понимании математических свойств этих алгоритмов, чтобы получить более глубокое представление о том, когда и почему они работают хорошо. Изучается применение каждого алгоритма в реальных условиях. Темы включают спектральную кластеризацию, тензорную декомпозицию, гамильтонов метод Монте-Карло, состязательное обучение и вариационную аппроксимацию.

4. ДИСЦИПЛИНЫ ПО ПРАКТИЧЕСКИМ ПРОБЛЕМАМ МАШИННОГО ОБУЧЕНИЯ

Рассмотрим теперь блок дисциплин, ориентированных на подготовку специалистов-практиков и вводящих в круг вопросов, связанных с реализацией и эксплуатацией систем машинного обучения и иных систем со встроенными в них функциями искусственного интеллекта.

Курс ***«Практическое машинное обучение» (Practical Machine Learning)*** [25] включает четыре раздела:

1) базовые модели машинного обучения: сбор, предобработка данных, обзор моделей машинного обучения, валидация моделей, комбинирование моделей;

2) невыполненные предположения: ковариационный сдвиг, сдвиг меток, неравномерно распределенные данные;

3) настройка производительности: тонкая настройка моделей: тонкая настройка глубоких сетей, трансферное обучение, дистилляция, мультимодальные данные;

4) за пределами моделей: развёртывание модели, критерии достоверности (fairness), ликвидация проблем достоверности, интерпретируемость модели.

В курсе «Конструирование систем машинного обучения» (Machine Learning Systems Design) [26] изучаются следующие темы: понимание продуктов машинного обучения, введение в конструирование систем машинного обучения, инженерия данных, разработка моделей, библиотека PyTorch и распределенное обучение, оценка моделей, протоколирование хода и версий экспериментов, этапы разработки, TinyML, масштабирование моделей машинного обучения: примеры с Uber и Ludwig, разработка моделей за пределами тестирования точности, мониторинг и поддержка, инфраструктура, интеграция машинного обучения в бизнес, будущее систем машинного обучения. Этот курс задуман как курс без учебника, он также строится на материалах многочисленных научных статей, практических руководств и стандартов.

Курс ***«Доверенное машинное обучение» (Trustworthy Machine Learning)*** [27] включает следующие основные разделы: объяснения моделей, достоверность моделей, конфиденциальность данных и робастность (устойчивость) моделей, включая множество частных вопросов по каждой из этих тем.

Курс ***«Аппаратные ускорители для машинного обучения» (Hardware Accelerators for Machine Learning)*** [28] включает такие темы как роль аппаратных ускорителей, ускорители линейной алгебры, ускорители сверточных сетей, ускорители обработки естественных языков, аппаратное масштабирование глубокого обучения. Особенность курса – большое число приглашённых лекторов (Facebook, Google, NVIDIA и др.). На вводных лекциях рассказывают общую историю, дают классификацию аппаратных устройств, далее каждый из приглашенных лекторов рассказывает о своих разработках. Курс без учебника – основан на чтении большого массива актуальных статей.

5. ДИСЦИПЛИНЫ ПО ИНТЕЛЛЕКТУАЛЬНОМУ АНАЛИЗУ БОЛЬШИХ ДАННЫХ

Интеллектуальный анализ данных – это, пожалуй, старейшая и одна из важнейших областей применения методов ИИ. В интеллектуальном анализе данных не пытаются выразить закономерности аналитически, так как зависимости могут быть очень сложными, аналитическая функция может вообще не существовать. Наконец, точные зависимости могут вообще не требоваться для прикладных задач.

Технология интеллектуального анализа данных состоит в том, что собираются данные о каком-либо процессе, строится модель процес-

са, результат оценивается, и делаются выводы (принимается решение). Модели данных могут быть описательными (дескриптивными) либо прогностическими (предиктивными). В интеллектуальном анализе данных используются как методы машинного обучения, так и методы, основанные на других принципах (в основном, алгебраические и комбинаторные).

В качестве примера учебного курса по интеллектуальному анализу данных рассмотрим стэнфордский курс ***«Интеллектуальный анализ больших массивов данных» (Mining Massive Datasets)*** [29]. Курс предполагает изучение следующих тем: поиск часто встречающихся наборов, локально-чувствительное хэширование, кластеризация, понижение размерности, рекомендательные системы, ранжирование страниц (PageRank), введение в социальные сети, обнаружение сообществ в в графах, обучение на представлениях графов, крупномасштабное машинное обучение, глубокое обучение, интеллектуальный анализ потоков данных, вычислительная реклама, обучение через эксперименты, оптимизирующие субмодульные функции, графовые нейронные сети.

Студентам, специализирующимся по этому направлению, обычно преподается значительное количество дисциплин, посвященных изучению конструирования и анализа алгоритмов, технологиям управления данными, системам управления базами данных, операционным системам, технологиям параллельной обработки данных и пр., которые мы в рамках настоящей статьи рассматривать не будем.

6. ДИСЦИПЛИНЫ ПО КОМПЬЮТЕРНОМУ ЗРЕНИЮ

Компьютерное зрение – ставшая уже классической сфера применения ИИ. Учебные дисциплины, посвященные этому важнейшему научно-техническому направлению, изучаются во многих университетах по всему миру. К основным задачам компьютерного зрения принято относить:

- классификацию объектов на изображениях;
- детектирование (захват и позиционирование) объектов на изображениях;
- семантическую сегментацию изображений;
- перенос стиля изображений;
- генерацию правдоподобных изображений (и объектов иной природы);
- реконструкцию пространственной глубины сцены по изображениям.

Приложения компьютерного зрения включают в себя медицинскую диагностику, интеллектуальную робототехнику, беспилотные транспортные средства, видеонаблюдение, системы безопасности, интеллектуальную фильтрацию изображений.

Базовый курс Стэнфордского университета по компьютерному зрению, который носит название ***«Компьютерное зрение: основы и применения» (Computer Vision: Foundations and Applications)*** [30], предусматривает следующую повестку:

- низкоуровневое зрение: фотометрическое формирование изображения, фильтры, векторы, признаки и их соответствие, оптические потоки.
- геометрическое зрение: формирование геометрического изображения, геометрия одной проекции, геометрия двух проекций, стереозрение, структура движения.
- распознавание визуальных шаблонов: обучение без учителя, обучение с учителем, глубокое обучение, самообучение.
- расширенные темы: понимание зрения, зрение для роботов и автономных устройств, трёхмерное зрение, этика компьютерного зрения.

Для изучающих компьютерное зрение рекомендуется дополнительный курс ***«Непрерывные математические методы с акцентом на машинное обучение» (Continuous Mathematical Methods with an Emphasis on Machine Learning)*** [31]. В курсе изучается решение систем линейных уравнений, операции с матрицами, в том числе специальными, итерационные методы решения, локальные аппроксимации, понятие «проклятия размерности», метод наименьших квадратов, базовые методы оптимизации, приближение методом наименьших квадратов, нулевые сингулярные величины, понятие регуляризации, методы оп-

тимизации, нелинейные системы, отыскание корней уравнений, одномерная оптимизация, вычисление производных, избежание производных, методы спуска, методы моментов.

Курс ***«Глубокое обучение для компьютерного зрения» (Deep Learning for Computer Vision)*** – один из самых авторитетных и популярных курсов Стэнфордского университета [32]. Курс состоит из трех разделов:

1. Основы нейросетей (обучение, управляемое данными, линейная классификация и метод k ближайших соседей, функции потерь, оптимизация, обратное распространение ошибки, многослойные перцептроны, нейросети).

2. Свёрточные нейросети (свёртки, pyTorch, функции активации, пакетная нормализация, трансферное обучение, аугментация данных, Momentum / RMSProp / Adam, конструирование архитектуры).

3. Приложения компьютерного зрения (рекуррентные сети, LSTM, трансформеры, захват изображения, интерпретация нейросетей, перенос стиля, примеры состязательности, честность и этика, человекоцентрированный ИИ, трёхмерное зрение, глубокое обучение с подкреплением, графы сцен, самообучение, мультимодальное обучение, обучение роботов).

Курс ***«Компьтерное зрение: от трёхмерной реконструкции к распознаванию» (Computer Vision***: From 3D Reconstruction to Recognition) [33] состоит из двух больших разделов:

1. Пространственная геометрия: оценка пространственных свойств объектов и сцен по изображениям геометрическими методами (модели камер, калибровка камер, метрология одной проекции, эпиполярная геометрия, геометрия нескольких проекций, структура, выявляемая из движения, объёмное стереоизображение).

2. Семантика и обучение: оценка семантических и динамических свойств элементов сцен по изображениям методами машинного обучения (подгонка и поиск соответствий, низкоуровневое представление, глубокая оценка и низкоуровневый трекинг, оптические и сценовые потоки, шестимерная оценка положения, трекинг объектов).

Курс ***«Системы визуальных вычислений» (Visual Computing Systems)*** [34] включает следующие вопросы: обзор архитектур и производительности компьютеров, конвейер обработки изображений с цифровой камеры, обработка изображений с камеры современного смартфона, эффективное распределение алгоритмов обработки изображений на параллельной аппаратуре, эффективное использование глубоких нейросетей для анализа изображений, аппаратные ускорители для глобальных сетей, алгоритмы для параллельного масштабируемого обучения глубоких сетей, увеличение уровня абстракции в машинном обучении, системная поддержка для генерации суперзрения (и её недостаток), эффективное использование видео посредством специализации, сжатие видео, конвейер обработки графики в реальном времени, распределение конвейера обработки графики в реальном времени на GPU, предметно-ориентированные языки затенения, платформенная поддержка трассировки лучей в реальном времени, рендеринг для обучения: конструирование рендеров для поддержки обучения моделей.

Стабильного учебника по этому курсу пока нет. Рекомендуется большое количество свежих научных статей и документации.

7. ДИСЦИПЛИНЫ ПО ОБРАБОТКЕ ЕСТЕСТВЕННЫХ ЯЗЫКОВ

Обработка естественных языков (англ. NLP – Natural Language Processing) – другое важнейшее направление применения ИИ, также уже ставшее классическим.

Вводный курс Стэнфордского университета по этому направлению носит название ***«От языков к информации» (From Languages to Information)*** [35]. Это, по сути, широкое введение в обработку естественных языков. Изучаемые в курсе темы посвящены самым разным аспектам этой специализации: введению в обработку естественных языков, вычислительную лингвистику и распознавание речи, обработке текста с помощью Unix-инструментов, моделированию языка, информационному поиску, ранжированию страниц, рекомендательным системам, анализу социальных сетей, чатботам.

На платформе DeepLearning.ai есть специализация в области обработки естественных языков [36], состоящая из четырех курсов: NLP с классификацией и векторными пространствами, NLP с вероятностными моделями, NLP с последовательностными моделями, NLP с моделями внимания.

Базовый курс Стэнфорда по обработке естественных языков – ***«Обработка естественных языков при помощи глубокого обучения» (Natural Language Processing with Deep Learning)*** [37]. В курсе изучаются следующие темы: векторы слов, классификация на основе окон слов, обратное распространение ошибок и нейронные сети, разбор зависимостей, рекуррентные нейронные сети и языковые модели, исчезающие градиенты, seq2seq, машинный перевод, механизм внимания, модели подслов, трансформеры, предобучение, ответы на вопросы, генерация естественного языка, ссылки в языке, разрешение перекрёстных ссылок, T5 и другие языковые модели, интеграция знаний в языковых моделях, социальные и этические соглашения в NLP-системах, анализ и объяснение моделей, будущее NLP и глубокое обучение.

Курс ***«Обработка устной речи» (Spoken Language Processing)*** [38] включает в себя следующие темы: акустическая фонетика, введение в диалоговые системы, машинное обучение в диалоге, введение в автоматическое распознавание речи, глубокое обучение в автоматическом распознавании речи, синтез речи, преобразование текста в речь, извлечение смысла из речи.

Курс ***«Понимание естественного языка» (Natural Language Understanding)*** [39] охватывает следующий круг вопросов: высокоуровневые цели и гипотезы, конструирование матриц, сравнение векторов, базовое перевзвешивание, понижение размерности, модернизация, статическое представление из контекстуальных моделей, обзор анализа тональности высказываний с учителем, общие практические советы, поиск гиперпараметров и сравнение классификаторов, представление признаков, классификаторы на основе рекуррентных нейросетей, обзор контекстных репрезентативных моделей, трансформеры, модели BERT, RoBERTa, ELECTRA, практическая тонкая настройка параметров, обзор «заземлённых» языковых представлений, дикторы, слушатели, варианты контекстного «заземления», модель рационального речевого акта, нейронные модели RSA, обзор предсказаний естественного языка. SNLI, MultiSNLI, Adversarial NLI, артефакты датасетов и состязательное тестирование, моделирование стратегий, механизмы внимания, обзор NLU и информационного поиска, классический информационный поиск, нейронный информационный поиск.; обзор извлечения связей с удалённым учителем, ресурсы данных, формулирование проблемы, оценка, простые базовые показатели, направления поиска; обзор методов и метрик, метрики классификаторов, метрики генерации естественного языка, организация данных, оценка моделей; обзор методов анализа в NLP, состязательное тестирование, состязательное обучение, испытания, атрибуция признаков.

Курс ***«Диалоговые виртуальные ассистенты, основанные на глубоком обучении» (Conversational Virtual Assistants with Deep Learning)*** [40] предполагает изучение следующих разделов: ответы на вопросы по структурированным данным, семантический разбор для диалоговых агентов, генерация транзакционных агентов из схем и API, связанные технологии.

Курс ***«Поиск информации и веб-поиск» (Information Retrieval and Web Search)*** [41] включает в себя следующие вопросы: инвертированные индексы, конструкция индексов, алгоритмы для сжатия списков, коррекция правописания, рейтингование, взвешивание терминов, модели векторного пространства, вероятностный поиск, методы оценки, системные аспекты поиска и рейтингования информации, классификация и кластеризация в векторных пространствах, классификация текстов, распределенное представление слов для информационного поиска, обучение ранжированию, анализ ссылок, взаимосвязанные и близко-дублированные страницы, ответы на вопросы, персонализация.

Курс ***«Этические и социальные аспекты обработки естественных языков» (Ethical and Social Issues in Natural Language***

Processing) [42] посвящается изучению таких вопросов как источники, участники, разметчики и данные в NLP, гендерные распределения в моделях NLP и данных, расовые распределения в моделях NLP, NLP как инструмент для обнаружения стереотипов и отклонений, законодательные и правовые приложения NLP, NLP для указания и идентификации токсичности, ненависти, злоупотреблений, NLP для изучения пропаганды и политической дезинформации, NLP для проверки фактов и обнаружения фейковых новостей, NLP для изучения фрейминга и его отклонений, этические аспекты чатботов, осторожные экспериментальные методы в NLP, приватность, аспекты NLP, связанные с медициной. Курс строится на основе материалов актуальных статей.

8. ДИСЦИПЛИНЫ ПО ИНТЕЛЛЕКТУАЛЬНОЙ РОБОТОТЕХНИКЕ

Ещё одно важнейшее направление применения ИИ – робототехника. Главное отличие современной интеллектуальной робототехники от ранних этапов ее развития состоит в том, что роботы позволяют не просто автоматизировать некоторые процессы (например, производственные), но обеспечить возможность самостоятельного принятия роботами тактических решений по целеполаганию, оптимизации траектории движения, эффективному применению рабочих инструментов и пр.

Базовый курс Стэнфордского университета по этому направлению носит название ***«Введение в робототехнику» (Introduction to Robotics)*** [43]. Принимая во внимание междисциплинарный характер робототехники, в нем предлагается изучить следующие разделы: кинематика роботов, динамика роботов, управление роботами, планирование движения, генерация траектории, программирование и конструирование роботов.

Для более глубокого погружения в предмет предлагается изучить большой двухчастный курс под названием ***«Принципы автономии роботов» (Principles of Robot Autonomy I и Principles of Robot Autonomy II)*** [44, 45].

В первом курсе изучаются следующие темы: введение в ОС роботов, оптимизация траекторий, отслеживание траекторий и контроль замкнутых петель, планирование движения, робототехнические сенсоры и введение в компьютерное зрение, обработка изображений, детектирование и описание признаков. Экстракция информации, классическое распознавание образов, введение в теорию локализации и фильтрации, параметрическая и непараметрическая фильтрация, обнаружение и отслеживание объектов, одновременная локализация и картирование, мультисенсорная чувствительность и слияние данных сенсоров, стереозрение, машины состояний.

Во втором курсе изучаются: марковские процессы принятия решений, введение в обучение с подкреплением, обучение с подкреплением для управления роботами на основе моделей и без моделей, чувствительность на основе обучения, основы захвата, оптимизация силы захвата, захват и манипуляция на основе обучения, интерактивная чувствительность, имитационное обучение, обучение на основе попарных сравнений и физической обратной связи, интерактивное управление и разделяемая автономия, системные архитектуры, спецификации и проверки моделей, формальная верификация нейронных сетей. Этот курс изучается по материалам актуальных научных статей.

Курс ***«Проблемы сложных манипуляций в робототехнике» (Topics in Advanced Robotic Manipulation)*** [46] содержит обзор наиболее важных и влиятельных концепций в области автономных роботизированных манипуляций. Он включает в себя классические концепции, которые все еще широко используются, и более новые подходы, которые изменили взгляд на автономные манипуляции. Рассматриваются подходы к планированию и управлению движением с использованием визуального и тактильного восприятия, а также машинного обучения. Этот курс акцентирует внимание на новых подходах к преодолению трудностей в обобщении опыта, исследовании окружающей среды и представлении обучения, чтобы эти методы можно было масштабировать до реальных проблем. Курс построен на изучении набора актуальных статей.

Курс ***«Интерактивное имитационное***

моделирование для обучения роботов» (Interactive Simulation for Robot Learning) [47] посвящен изучению взаимодействия между агентом и внешней средой, а также мультиагентных и человекомашинных взаимодействий роботов. В курсе изучается среда iG [48], которая обеспечивает быстрый визуальный рендеринг и физическое моделирование в сотнях реальных сред. Это позволяет исследователям обучать и оценивать роботов-агентов, которые используют визуальные датчики для решения задач навигации и манипулирования внутри помещений, таких как открытие дверей, выбор и размещение предметов или поиск в шкафах. От студентов ожидается предварительное освоение среды имитационного моделирования iGibson (проводится тренинг в ходе курса), а также умение пользоваться Jupyter Notebooks.

9. ВОЗМОЖНОСТИ И ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ ЗАРУБЕЖНЫХ ПРАКТИК В ОТЕЧЕСТВЕННОМ ВЫСШЕМ ОБРАЗОВАНИИ

Анализ состава и содержания учебных дисциплин в области ИИ, реализуемых в ведущих зарубежных вузах, позволяет сделать ряд выводов о возможностях использования зарубежного опыта в российской системе высшего образования.

1. Организационные, методические и в особенности содержательные аспекты зарубежных образовательных практик в области ИИ могут служить ориентиром при создании новых образовательных программ в сфере ИИ (специалитет, бакалавриат, магистратура, аспирантура) в российских вузах, а также новых дисциплин в рамках уже существующих образовательных программ. Содержание образовательных программ обычно более консервативно по сравнению с развитием научных знаний, поэтому даже того ядра образовательных программ, которое выглядит стабильным на текущий момент, будет достаточно на нынешнем переходном этапе для конструирования качественных образовательных программ в сфере ИИ. Более того, по мнению автора, даже в условиях действующих нормативно-методических документов, в том числе государственных образовательных стандартов, преподаватель высшей школы обладает достаточной творческой свободой для того, чтобы реализовывать привлекательные для него элементы зарубежных образовательных практик в своей повседневной учебно-методической деятельности.

2. Необходимо создание оригинальных русскоязычных университетских учебников по новым направлениям компьютерных наук, в первую очередь, в сфере ИИ. Текущая ситуация состоит в том, что в ведущих зарубежных университетах регулярно издаются фундаментальные учебники по различным дисциплинам в сфере компьютерных наук (типичный их объём – 600…1200 стр. и даже более). В то же время в России практически отсутствуют изданные за последние 30 лет учебники российских авторов по важнейшим новым разделам компьютерных наук, включая ИИ. В учебном процессе вузов используются либо глубоко устаревшие учебники, либо литература популярного жанра, руководства для практиков и тому подобные источники, далекие от идеала. Этот пробел необходимо как можно скорее восполнить.

На основе проведенного анализа можно предложить примерную модель рабочего учебного плана по направлениям подготовки в сфере ИИ, показанную в табл. 1. Очевидно, что структура модели в гораздо большей степени соответствует целям, задачам и уровню магистерских образовательных программ, хотя нельзя исключать и возможности использования её в качестве источника идей для конструирования образовательных программ бакалавриата.

Таблица 1

Примерная модель рабочего учебного плана по направлениям подготовки в сфере искусственного интеллекта

Направление подготовки «Информатика и вычислительная техника»	Направление подготовки «Информационная безопасность»

<table>
<tr><td>Теория и методология искусственного интеллекта</td><td>Компьютерное зрение</td><td>Обработка естественных языков</td><td>Интеллектуальная робототехника</td><td>Информационная безопасность искусственного интеллекта</td></tr>
<tr><td colspan="5">Принципы и технологии искусственного интеллекта</td></tr>
<tr><td colspan="5">Основы машинного обучения</td></tr>
<tr><td colspan="5">Анализ больших массивов данных</td></tr>
<tr><td colspan="5">Глубокое обучение</td></tr>
<tr><td colspan="5">Глубокие генеративные модели</td></tr>
<tr><td colspan="5">Обучение с подкреплением</td></tr>
<tr><td colspan="5">Обучение на графах</td></tr>
<tr><td colspan="4">Принятие решений в условиях неопределённости</td><td>Основы доказательной криптографии-1</td></tr>
<tr><td colspan="4">Принципы и технологии вероятностных графических моделей</td><td>Основы доказательной криптографии-2</td></tr>
<tr><td>Когнитивная и вычислительная нейронаука</td><td>Оптика</td><td>Основы лингвистики</td><td>Основы машиноведения и материаловедения</td><td>Прикладная криптография-1</td></tr>
<tr><td>Вычислительная логика</td><td>Проективная геометрия</td><td>Статистические методы в лингвистике</td><td>Введение в робототехнику</td><td>Прикладная криптография-2</td></tr>
<tr><td colspan="3">Методы оптимизации</td><td>Оптимальное управление и управление, основанное на знаниях</td><td>Искусственный интеллект в информационной безопасности</td></tr>
<tr><td colspan="3">Тензорные вычисления</td><td>Динамика, управление и идентификация систем</td><td>Конфиденциальное машинное обучение</td></tr>
<tr><td>Статистическая теория машинного обучения</td><td>Компьютерное зрение в задачах трёхмерной реконструкции и распознавания объектов</td><td>Обработка естественных языков на основе глубокого обучения</td><td>Сложные манипуляции в робототехнике</td><td>Распределенные и децентрализованные системы</td></tr>
<tr><td>Глубокое многозадачное и мета-обучение</td><td>Свёрточные нейронные сети для распознавания визуальных объектов</td><td>Понимание естественных языков</td><td>Принципы автономной робототехники-1</td><td>Системы распределенного реестра и их применение</td></tr>
<tr><td colspan="3">Основы обеспечения доверия и безопасности систем ИИ</td><td>Принципы автономной робототехники-2</td><td>Введение в интернет вещей</td></tr>
<tr><td colspan="5">Научно-исследовательская работа (практика)</td></tr>
<tr><td colspan="5">Выпускная квалификационная работа</td></tr>
</table>

ЗАКЛЮЧЕНИЕ

Подводя итог анализу актуальных зарубежных образовательных практик в сфере искусственного интеллекта, следует отметить, что зарубежный опыт формирования образовательных программ в области ИИ представляет значительный интерес для отечественного образования в части организационных, методических аспектов и содержательного наполнения образовательных программ. Очевидна необходимость приведения отечественного высшего образования в сфере компьютерных наук в соответствие с передовым мировым опытом и тенденциями развития теоретических и прикладных исследований в области ИИ.

В качестве наиболее перспективных направлений исследования зарубежного опыта, на наш взгляд, следует выделить изучение актуальной научно-исследовательской повестки в сфере ИИ, а также принципов функционирования института соискателей ученой степени Ph.D. в зарубежных университетах.

СПИСОК ЛИТЕРАТУРЫ

1. Stanford bulletin. BS – Bachelor of Science. Computer Science. URL: https://bulletin.stanford.edu/programs/CS-BS (дата обращения: 30.06.2022)

2. Handbook for undergraduate engineering programs. Stanford University. School of Engineering. 2021-2022. 360 pp. URL: https://drive.google.com/file/d/16FrNs5EJNko1rfFM6owVzlXKTioB8jrE/view (дата обращения: 30.06.2022)

3. Stanford bulletin. MS – Master of Science. Computer Science. URL: https://bulletin.stanford.edu/programs/CS-MS (дата обращения: 30.06.2022)

4. CS 157: Introduction to logic. Stanford University. Autumn 2021-2022. URL: http://intrologic.stanford.edu/stanford/index.php (дата обращения: 30.06.2022)

5. CS 221: Artificial Intelligence: Principles and Techniques. Stanford University. Autumn 2021-2022. URL: https://stanford-cs221.github.io/autumn2021 (дата обращения: 30.06.2022)

6. CS 229: Machine Learning. Stanford University. Fall 2021. URL: http://cs229.stanford.edu/ (дата обращения: 30.06.2022)

7. Shervine Amidi's homepage. Cheatsheets on computer science. URL: https://stanford.edu/~shervine/teaching/ (дата обращения: 30.06.2022)

8. Coursera. Специализация «Машинное обучение». URL: https://www.coursera.org/specializations/machine-learning-introduction (дата обращения: 30.06.2022)

9. CS 181: Machine Learning. Harvard University. 2022. URL: https://harvard-ml-courses.github.io/cs181-web/ (дата обращения: 30.06.2022)

10. Воронцов К.В. Машинное обучение: курс лекций. 2022. URL: https://bit.ly/1bCmE3Z (дата обращения: 30.06.2022)

11. CS 230: Deep Learning. Stanford University. Autumn 2021. URL: https://cs230.stanford.edu/ (дата обращения: 30.06.2022)

12. Coursera. Специализация «Глубокое обучение». URL: https://www.coursera.org/specializations/deep-learning (дата обращения: 30.06.2022)

13. Yan LeCun. Deep Learning course. Spring 2021. URL: https://cds.nyu.edu/deep-learning/ (дата обращения: 30.06.2022)

14. Zhang A., Lipton Z., Li M., Smola A. Dive into deep learning. 2022. URL: https://d2l.ai/d2l-en.pdf (дата обращения: 30.06.2022)

15. AA 228/CS 238: Decision Making under Uncertainty. Stanford University. Autumn 2021. URL: https://web.stanford.edu/class/aa228/cgi-bin/wp/ (дата обращения: 30.06.2022)

16. CS 234: Reinforcement Learning. Stanford University. Winter 2022. URL: https://web.stanford.edu/class/cs234/ (дата обращения: 30.06.2022)

17. CS 236: Deep Generative Models. Stanford University. Fall 2021. URL: https://deepgenerativemodels.github.io/ (дата обращения: 30.06.2022)
18. Coursera. Специализация “Generative Adversary Networks (GANs)” URL: https://www.coursera.org/specializations/generative-adversarial-networks-gans (дата обращения: 30.06.2022)
19. CS 224W: Machine Learning with Graphs. Stanford University. Fall 2021. URL: http://web.stanford.edu/class/cs224w/ (дата обращения: 30.06.2022)
20. Bronstein M., Bruna J., Cohan T. Geometric Deep Learning: Grids, Groups, Graphs, Geodesics, and Gauges. URL: https://geometricdeeplearning.com/ (дата обращения: 30.06.2022)
21. CS 228: Probabilistic Graphical Models. Stanford University. Winter 2022. URL: https://ermongroup.github.io/cs228/ (дата обращения: 30.06.2022)
22. STATS 214/CS 229M: Machine Learning Theory. Stanford University. Autumn 2021. URL: https://web.stanford.edu/class/stats214/ (дата обращения: 30.06.2022)
23. CS 330: Deep Multi-Task and Meta Learning. Stanford University. Fall 2021. URL: https://cs330.stanford.edu/ (дата обращения: 30.06.2022)
24. CS 329M: Topics in Artificial Intelligence: Algorithma of Advanced Machine Learning. Stanford University. Spring 2017. URL: https://cs330.stanford.edu/ (дата обращения: 30.06.2022)
25. CS 329P: Practical Machine Learning. Stanford University. Autumn 2021. URL: https://c.d2l.ai/stanford-cs329p/ (дата обращения: 30.06.2022)
26. CS 329S: Machine Learning Systems Design. Stanford University. Winter 2022. URL: https://stanford-cs329s.github.io/ (дата обращения: 30.06.2022)
27. CS 329T: Trustworthy Machine Learning. Stanford University. Spring 2022. URL: https://web.stanford.edu/class/cs329t/index.html (дата обращения: 30.06.2022)
28. CS 217: Hardware Accelerators for Machine Learning. Stanford University. Winter 2020. URL: https://cs217.stanford.edu/ (дата обращения: 30.06.2022)
29. CS 246: Mining Massive Data Sets. Stanford University. Winter 2022. URL: http://web.stanford.edu/class/cs246/ (дата обращения: 30.06.2022)
30. CS 131: Computer vision: Foundation and applications. Stanford University.Fall 2021. URL: http://vision.stanford.edu/teaching/cs131_fall2122/ (дата обращения: 30.06.2022)
31. CS 205L: Continuous mathematical methods with an emphasis on machine learning. Stanford University. Winter 2022. URL: http://web.stanford.edu/class/cs205l/index.html (дата обращения: 30.06.2022)
32. CS 231N: Deep learning for computer vision. Stanford University. Spring 2022. URL: http://cs231n.stanford.edu/index.html (дата обращения: 30.06.2022)
33. CS 231A: Computer Vision, from 3D Reconstruction to Recognition. Stanford University. Spring 2022. URL: https://web.stanford.edu/class/cs231a/index.html (дата обращения: 30.06.2022)
34. CS 348: Visual Computing Systems. Stanford University. Spring 2020. URL: https://gfxcourses.stanford.edu/cs348k/spring20/home (дата обращения: 30.06.2022)
35. CS 124: From languages to information. Stanford University. Autumn 2021. URL: https://web.stanford.edu/class/cs124/ (дата обращения: 30.06.2022)
36. Natural Language Processing specialization. URL: https://www.deeplearning.ai/courses/natural-language-processing-specialization/ (дата обращения: 30.06.2022)
37. CS 224N: Natural language processing with deep learning. Stanford University. Winter 2022. URL: http://web.stanford.edu/class/cs224n/ (дата обращения: 30.06.2022)
38. CS 224S: Spoken language processing. Stanford University. Spring 2022. URL: https://web.stanford.edu/class/cs224s/ (дата обращения: 30.06.2022)
39. CS 224U: Natural language understanding. Stanford University. Spring 2022. URL: https://web.stanford.edu/class/cs224u/index.html (дата обращения: 30.06.2022)
40. CS 224V: Conversational virtual assistants with deep learning. Stanford University. URL: https://web.stanford.edu/class/cs224v/index.html (дата обращения: 30.06.2022)
41. CS 276/LING 286: Information retrieval and web search. Stanford University. Spring 2019. URL: https://

web.stanford.edu/class/cs276/ (дата обращения: 30.06.2022)
42. CS 384. Ethical and social issues in Natural language processing. Stanford Ubiversity. Spring 2020. URL: https://web.stanford.edu/class/cs384/index.html (дата обращения: 30.06.2022)
43. CS 223A/ME 320: Introduction to robotics. Stanford University. Winter 2022. URL: https://cs.stanford.edu/groups/manips/teaching/cs223a/ (дата обращения: 30.06.2022)
44. AA 174A/AA 274A/CS 237A/EE 260A: Principles of Robot Autonomy I. Stanford University. Fall 2021. URL: https://stanfordasl.github.io/aa274a/ (дата обращения: 30.06.2022)
45. AA 174B/AA 274B/CS 237B/EE 260B: Principles of Robot Autonomy II. Stanford University. Winter 2022. URL: https://web.stanford.edu/class/cs237b/ (дата обращения: 30.06.2022)
46. CS 326: Topics in advanced robotic manipulation. Stanford University. Fall 2021. URL: https://web.stanford.edu/class/cs326/index.html (дата обращения: 30.06.2022)
47. CS 331B: Interactive simulation for robot learning. Stanford University. Spring 2021. URL: https://web.stanford.edu/class/cs331b (дата обращения: 30.06.2022)
48. iGibson: Interactive simulation of large scale virtualized realistic scenes for robot learning. URL: https://svl.stanford.edu/igibson (дата обращения: 30.06.2022)

Приложение. Ссылки на находящиеся в открытом доступе учебники по дисциплинам в сфере ИИ (дата обращения ко всем ресурсам: 30.06.2022)

Дисциплина Artificial Intelligence: Principles and Techniques – «Принципы и методы искусственного интеллекта»:

1. Russell S., Norvig P. Artificial Intelligence: A Modern Approach. 4th ed. 2021.
Официальная страница книги: http://aima.cs.berkeley.edu/
Файл с текстом книги: https://doc.lagout.org/science/Artificial%20Intelligence/General/Artificial%20Intelligence%20A%20Modern%20Approach%20-%20Stuart%20J.%20Russell%20%2C%20Peter%20Norvig.pdf
2. Koller D., Friedman N. Probabilistic Graphical Models.
Официальная страница книги: https://mitpress.mit.edu/books/probabilistic-graphical-models
Файл с текстом книги: https://djsaunde.github.io/read/books/pdfs/probabilistic%20graphical%20models.pdf
3. Sutton R., Barto A. Reinforcement Learning: An Introduction. 2015.
Официальная страница книги: https://mitpress.mit.edu/books/reinforcement-learning
Файл с текстом книги: http://web.stanford.edu/class/psych209/Readings/SuttonBartoIPRLBook2ndEd.pdf
4. Hastie, Tibshirani, and Friedman. The elements of statistical learning. 12th ed. 2017.
Официальная страница книги: https://hastie.su.domains/ElemStatLearn/
Файл с текстом книги: https://hastie.su.domains/ElemStatLearn/printings/ESLII_print12_toc.pdf
5. Tsang E.P.K. Foundations of constraint satisfaction. 2014.
Официальная страница книги: https://www.bracil.net/edward/fcs.html

Дисциплина Machine Learning – «Машинное обучение»:

1. Текст и слайды лекций на сайте курса в Стэнфордском университете (Andrew Ng):
https://docs.google.com/spreadsheets/d/1OEsqqhihH-n2OPHsT8jSA8BkLdqUMWY-GiWHgkBs3Z8/edit#gid=0
2. Christopher Bishop, Pattern Recognition and Machine Learning. Springer, 2006.
Файл с текстом книги: https://www.microsoft.com/en-us/research/uploads/prod/2006/01/Bishop-Pattern-Recognition-and-Machine-Learning-2006.pdf
3. Richard Duda, Peter Hart and David Stork, Pattern Classification, 2nd ed. John Wiley & Sons, 2001.
Официальная страница книги: https://www.wiley.com/en-us/Pattern+Classification,+2nd+Edition-p-9780471056690

Файл с текстом книги: https://docs.google.com/file/d/0B78A_rsP6RDSVjBTa1ZUSXBGYzA/edit?resourcekey=0-ieDlJmoTUv2WllxQDQcY2Q

4. Tom Mitchell, Machine Learning. McGraw-Hill, 1997.

Файл с текстом книги: https://www.cin.ufpe.br/~cavmj/Machine%20-%20Learning%20-%20Tom%20Mitchell.pdf

5. Richard Sutton and Andrew Barto, Reinforcement Learning: An introduction. MIT Press, 1998

Официальная страница книги: https://mitpress.mit.edu/books/reinforcement-learning

Файл с текстом книги: http://web.stanford.edu/class/psych209/Readings/SuttonBartoIPRLBook2ndEd.pdf

6. Deuschle W. Undergraduate fundamentals of machine learning. 2017-2022. 738 pp.

Файл с текстом книги: https://github.com/harvard-ml-courses/cs181-textbook/blob/master/Textbook.pdf

7. Трёхтомное издание:

7.1. Murphy K.P. Machine Learning: A Probabilistic Perspective

7.2. Murphy K.P. Probabilistic Machine Learning: An Introduction

7.3. Murphy K.P. Probabilistic Machine learning: Advanced Topics

Официальная страница книги и файлы с текстом 2-го и 3-го томов: URL: https://probml.github.io/pml-book/

Дисциплина Deep Learning (Стэнфорд) – «Глубокое обучение»:

1. Текст и слайды лекций на сайте курса в Стэнфордском университете (Andrew Ng): https://cs230.stanford.edu/syllabus/

2. Goodfellow I., Bengio Y., Courville A. Deep learning.

Официальная страница книги и html-файлы по главам: https://www.deeplearningbook.org/

Pdf-файл с текстом книги: https://studentweb.uvic.ca/~leizhao/Reading/deeplearningbook.pdf

3. Zhang A., Lipton Z., Li M., Smola A. Dive into deep learning. 2022.

Файлы с текстом книги: https://d2l.ai/d2l-en.pdf , https://d2l.ai/d2l-en-pytorch.pdf

Дисциплина Computational Logic – «Вычислительная логика»:

Hurley P. A concise introduction into logic. 2012.

Файл с текстом книги: https://home.iitk.ac.in/~avrs/PH142/Books/Patrick2012.pdf

Дисциплина Decision Making Under Uncertainty – «Принятие решений в условиях неопределенности»:

Kochenderfer M. et al. Algorithms for Decision Making. 2022. 700 pp.

Файл с текстом книги: https://algorithmsbook.com/files/dm.pdf

Дисциплина Reinforcement Learning – «Обучение с подкреплением»:

1. Текст и слайды лекций на сайте курса в Стэнфордском университете: https://web.stanford.edu/class/cs234/modules.html

2. Sutton R., Barto A. Reinforcement Learning: An Introduction. 2015.

Официальная страница книги: https://mitpress.mit.edu/books/reinforcement-learning

Файл с текстом книги: http://web.stanford.edu/class/psych209/Readings/SuttonBartoIPRLBook2ndEd.pdf

3. Goodfellow I., Bengio Y., Courville A. Deep learning.

Официальная страница книги и html-файлы по главам: https://www.deeplearningbook.org/

pdf-файл с текстом книги: https://studentweb.uvic.ca/~leizhao/Reading/deeplearningbook.pdf

4. Курс лекций «Imitation Learning for Robotics»: http://www.cs.toronto.edu/~florian/courses/imitation_learning/

Дисциплина Deep Generative Models – «Глубокие генеративные модели»:

1. Текст и слайды лекций на сайте курса в Стэнфордском университете: https://deepgenerativemodels.github.io/notes/index.html

2. Goodfellow I., Bengio Y., Courville A. Deep learning.

Официальная страница книги и html-файлы по главам: https://www.deeplearningbook.org/
pdf-файл с текстом книги: https://studentweb.uvic.ca/~leizhao/Reading/deeplearningbook.pdf

Дисциплина Machine Learning with Graphs – «Машинное обучение на графах»:

1. Слайды лекций на сайте курса в Стэнфордском университете: https://jingboyang.github.io/stanford-cs224w-graph-ml/stanford_cs224w_graph_ml.pdf

2. Hamilton W., Graph Representation Learning. 2020.

Официальная страница книги: https://www.cs.mcgill.ca/~wlh/grl_book/

Файл с текстом книги: https://www.cs.mcgill.ca/~wlh/grl_book/files/GRL_Book.pdf

3. Easley D., Kleinberg J. Networks, Crowds, and Markets^ Reasoning about a Highly Connected World. 2009.

Файл с текстом книги: https://jmvidal.cse.sc.edu/library/easley10a.pdf

4. Barabasi A.-L. Network Science Book.

Официальная страница и текст книги: http://networksciencebook.com/

Дисциплина Geometric Deep Learning – «Геометрическое глубокое обучение»:

Bronstein M., Bruna J., Cohan T. Geometric Deep Learning: Grids, Groups, Graphs, Geodesics, and Gauges.

Файл с текстом книги: https://arxiv.org/abs/2104.13478

Дисциплина Probabilistic Graphical Models: Principles and Techniques – «Вероятностные графические модели: принципы и технологии»:

1. Probabilistic Graphical Models: Principles and Techniques by Daphne Koller and Nir Friedman. MIT Press.

Файл с текстом книги: https://djsaunde.github.io/read/books/pdfs/probabilistic%20graphical%20models.pdf

2. Christopher Bishop, Pattern Recognition and Machine Learning. Springer, 2006.

Файл с текстом книги: https://www.microsoft.com/en-us/research/uploads/prod/2006/01/Bishop-Pattern-Recognition-and-Machine-Learning-2006.pdf

3. Трёхтомное издание:

3.1. Murphy K.P. Machine Learning: A Probabilistic Perspective

3.2. Murphy K.P. Probabilistic Machine Learning: An Introduction

3.3. Murphy K.P. Probabilistic Machine learning: Advanced Topics

Официальная страница книги и файлы с текстом 2-го и 3-го томов: URL: https://probml.github.io/pml-book/

4. Information Theory, Inference, and Learning Algorithms by David J. C. Mackay.

Файл с текстом книги: https://inference.org.uk/itprnn/book.pdf

5. Bayesian Reasoning and Machine Learning by David Barber.

Файл с текстом книги: http://web4.cs.ucl.ac.uk/staff/D.Barber/textbook/090310.pdf

6. Graphical models, exponential families, and variational inference by Martin J. Wainwright and Michael I. Jordan.

Файл с текстом книги: https://people.eecs.berkeley.edu/~wainwrig/Papers/WaiJor08_FTML.pdf

Дисциплина Machine Learning Theory – «Теория машинного обучения»:

Ma T. Lecture Notes on Machine Learning Theory. 2021.

https://docs.google.com/viewer?url=https://raw.githubusercontent.com/tengyuma/cs229m_notes/main/master.pdf

Дисциплина Topics in Artificial Intelligence – «Актуальные вопросы искусственного интеллекта»:

Blum A., Hopcroft J., Kannan R. Foundations of Data Science. 2019.

Файл с текстом книги: https://www.cs.cornell.edu/jeh/book%20no%20so;utions%20March%202019.pdf

Дисциплина Practical Machine Learning – «Практическое машинное обучение»:

Слайды лекций на сайте курса в Стэнфордском университете: https://c.d2l.ai/stanford-cs329p/syllabus.html

Дисциплина Mining Massive Datasets – «Интеллектуальный анализ больших массивов данных»:
Leskovec J., Rajaraman A., Ullman J. Mining of Massive Datasets.
Официальный сайт и файл с текстом книги: http://www.mmds.org/#book

Дисциплина Computer Vision: Foundations and Applications – «Компьютерное зрение: основы и применения»:
Szeliski R. Computer Vision: Algorithms and Applications. 2nd ed. 2022. 1232 pp.
Официальный сайт и файл с текстом книги: https://szeliski.org/Book/

Дисциплина Continuous Mathematical Methods with an Emphasis on Machine Learning – «Непрерывные математические методы с акцентом на машинное обучение»:
Heath T. Scientific Computing: An Introductory Survey. 2nd ed.
Официальная страница книги (доступны только слайды по главам): http://heath.cs.illinois.edu/scicomp/

Дисциплина Computer Vision: From 3D Reconstruction to Recognition – «Компьютерное зрение: от трёхмерной реконструкции к распознаванию»:
1. По геометрической части курса – лекции на сайте: https://web.stanford.edu/class/cs231a/course_notes.html
2. D. A. Forsyth and J. Ponce. Computer Vision: A Modern Approach (2nd Edition). Prentice Hall, 2011.
Файл с текстом книги: https://ru.b-ok.global/book/1129548/ed6f80
3. R. Hartley and A. Zisserman. Multiple View Geometry in Computer Vision. Cambridge University Press, 2003.
Файл с текстом книги: https://www.r-5.org/files/books/computers/algo-list/image-processing/vision/Richard_Hartley_Andrew_Zisserman-Multiple_View_Geometry_in_Computer_Vision-EN.pdf
4. Sebastian Thrun, Wolfram Burgard, Dieter Fox. Probabilistic robotics. The MIT Press, 2005. https://docs.ufpr.br/~danielsantos/ProbabilisticRobotics.pdf

Дисциплина Convolutional Neural Networks for Visual Recognition – «Свёрточные нейронные сети для распознавания зрительных образов»:
1. Слайды лекций на сайте курса в Стэнфордском университете: https://cs231n.github.io/ – материалы курса
2. Goodfellow I., Bengio Y., Courville A. Deep learning.
Официальная страница книги и html-файлы по главам: https://www.deeplearningbook.org/
pdf-файл с текстом книги: https://studentweb.uvic.ca/~leizhao/Reading/deeplearningbook.pdf
3. Marc Peter Deisenroth, A. Aldo Faisal. Cheng Soon Ong “Mathematics for machine learning”.
Файл с текстом книги: https://mml-book.github.io/book/mml-book.pdf
4. Zhang A., Lipton Z., Li M., Smola A. Dive into deep learning. 2022/
Файлы с текстом книги: https://d2l.ai/d2l-en.pdf , https://d2l.ai/d2l-en-pytorch.pdf

Дисциплина From Languages to Information – «От языков к информации»:
1. Dan Jurafsky, James H. Martin “Speech and Language Processing”
Файл с текстом книги: http://web.stanford.edu/~jurafsky/slp3/ed3book_sep212021.pdf
2. C. Manning, P. Raghavan, H. Schutze “Introduction to Information Retrieval”
Официальная страница книги и файл с текстом книги: https://nlp.stanford.edu/IR-book/

Дисциплина Natural Language Processing with Deep Learning – «Обработка естественных языков при помощи глубокого обучения»:
1. Dan Jurafsky and James H. Martin. Speech and Language Processing. 3rd ed.
Файл с текстом книги: https://web.stanford.edu/~jurafsky/slp3/ed3book.pdf
2. Jacob Eisenstein. Natural Language Processing. 2018.
Файл с текстом книги: https://cseweb.ucsd.edu/~nnakashole/teaching/eisenstein-nov18.pdf
3. Yoav Goldberg. A Primer on Neural Network Models for Natural Language Processing
Файл с текстом книги: https://arxiv.org/pdf/1510.00726.pdf
4. Goodfellow I., Bengio Y., Courville A. Deep learning.

Официальная страница книги и html-файлы по главам: https://www.deeplearningbook.org/
pdf-файл с текстом книги: https://studentweb.uvic.ca/~leizhao/Reading/deeplearningbook.pdf

Дисциплина Spoken Language Processing – «Обработка устной речи»:

1. Dan Jurafsky and James H. Martin. Speech and Language Processing. 3rd ed.
Файл с текстом книги: https://web.stanford.edu/~jurafsky/slp3/ed3book.pdf
2. Yoav Goldberg. A Primer on Neural Network Models for Natural Language Processing
Файл с текстом книги: https://arxiv.org/pdf/1510.00726.pdf
3. Goodfellow I., Bengio Y., Courville A. Deep learning.
Официальная страница книги и html-файлы по главам: https://www.deeplearningbook.org/
pdf-файл с текстом книги: https://studentweb.uvic.ca/~leizhao/Reading/deeplearningbook.pdf

Дисциплина Information Retrieval and Web Search – «Поиск информации и веб-поиск»:

1. C. Manning, P. Raghavan, H. Schutze “Introduction to Information Retrieval”
Официальная страница книги и файл с текстом книги: https://nlp.stanford.edu/IR-book/
2. Managing Gigabytes, by I. Witten, A. Moffat, and T. Bell.
Файл с текстом книги: http://cyber.sibsutis.ru/%D0%A1%D0%9F%D0%98/%D0%9F%D0%B5%D1%80%D0%B2%D0%B0%D1%8F%20%D1%87%D0%B0%D1%81%D1%82%D1%8C/Managing%20Gigabytes;%20Witten,%20%D0%9Coffat,%20Bell.pdf
3. Foundations of Statistical Natural Language Processing, by C. Manning and H. Schütze.
Файл с текстом книги: https://github.com/shivamms/books/blob/master/nlp/Foundations%20of%20Statistical%20Natural%20Language%20Processing%20-%20Christopher%20D.%20Manning.pdf
4. Search Engines: Information Retrieval in Practice, by B. Croft, D. Metzler, and T. Strohman.
Файл с текстом книги: https://ciir.cs.umass.edu/downloads/SEIRiP.pdf
5. Information Retrieval: Implementing and Evaluating Search Engines, by S. Büttcher, C. Clarke, and G. Cormack.
Файл с текстом книги: https://github.com/KnowNo/books-7/blob/master/Information%20Retrieval/Information%20Retrieval%20Implementing%20and%20Evaluating%20Search%20Engines.pdf

Дисциплина Introduction to Robotics – «Введение в робототехнику»:

1. Robotics- Modelling, Planning and Control by Siciliano, B., Sciavicco, L., Villani, L., Oriolo, G.
Файл с текстом книги: https://www.studmed.ru/siciliano-b-sciavicco-l-villani-l-oriolo-g-robotics-modelling-planning-and-control-springer-2009_65928b782b2.html
2. Introduction to Robotics: Mechanics and Control, John J. Craig, Addison-Wesley Publishing Company, 3rd Edition, 2003
Файл с текстом книги: http://mathdep.ifmo.ru/wp-content/uploads/2018/10/John-J.Craig-Introduction-to-Robotics-Mechanics-and-Control-3rd-edition-Pearson-Education-Inc.-2005.pdf
3. Robot Modeling and Control, M. Spong, M. Vidyasagar, S. Hutchinson, 1st ed. Wiley & Sons, 2005.
Файл с текстом книги: https://bayanbox.ir/view/8445052974254475991/Robot-Modeling-and-Control-Spong.pdf

Дисциплина Principles of Robot Autonomy – «Принципы автономии роботов»:

1. R. Siegwart, I. R. Nourbakhsh, D. Scaramuzza. Introduction to Autonomous Mobile Robots. MIT Press, 2nd Edition, 2011, ISBN-10: 0262015358.
Файл с текстом книги: https://www.ucg.ac.me/skladiste/blog_13268/objava_56689/fajlovi/Introduction%20to%20Autonomous%20Mobile%20Robots%20book.pdf
2. S. M. LaValle. Planning Algorithms. Cambridge University Press, 2006,
Файл с текстом книги: http://planning.cs.uiuc.edu/
3. J. M. O’Kane. A Gentle Introduction to ROS. 2013,
Файл с текстом книги: https://cse.sc.edu/~jokane/agitr/

УДК: 004.056

Основные положения установочной лекции для введения в криптографию и криптографические методы защиты информации

A.Yu. Shcherbakov

The Main Thesis to the Introductory Lecture in Cryptography and Cryptographic Methods of Information Security

Abstract. *This article is intended to help lecturers of cryptography and information security in the formation of an introductory lecture on cryptography for students and listeners, prepared both within the framework of university programs and additional professional education.*

The presented material is necessary for the formation of a correct conceptual and methodological view of the subject.

Keywords: *cipher, cryptanalysis, cryptographic scheme, conformance check, key, encryption algorithm, encryption system, quantum cryptography.*

А.Ю. Щербаков

Доктор технических наук, профессор кафедры комплексной безопасности критически важных объектов РГУ нефти и газа (НИУ)имени И.М. Губкина, ведущий научный сотрудник Государственного университета управления.

E-mail: x509@ras.ru

Аннотация. *Данная статья предназначена для содействия преподавателям, читающим курсы основ криптографии и компьютерной безопасности, в подготовке вводных лекций по криптографии для обучаемых и слушателей, подготавливаемых как в рамках вузовских программ, так и дополнительного профессионального образования.*

Излагаемый материал необходим для формирования правильного понятийно-методологического взгляда на предмет.

Ключевые слова: *шифр, криптоанализ, криптографическая схема, проверка соответствия, ключ, криптографический алгоритм, система шифрования, квантовая криптография.*

ВВЕДЕНИЕ

Исторически сложилась практика, когда изучение криптографии начинается с экскурсов в историю предмета и рассмотрения сравнительно простых конструкций, связанных с подставочными (простая символьная замена) или перестановочными шифрами. Кажущаяся простота предмета внушает обучаемым ложные иллюзии, что современная криптография столь же проста и очевидна.

Однако мы полагаем, что преподаватель должен донести не только сложности современной криптографии, но также ее комплексный характер и общую зависимость предмета от установок и позиций государственных регуляторов [1].

СОДЕРЖАНИЕ ТЕРМИНОЛОГИИ И МЕТОДОЛОГИИ СОВРЕМЕННОЙ КРИПТОГРАФИИ

С точки зрения обычного восприятия криптография – это наука, изучающая процессы шифрования информации.

Основная цель шифрования – сделать содержание послания от одного воспринимающего субъекта (например, человека) к другому таким, чтобы не имеющие отношение к этой передаче субъекты не смогли его воспринять.

Эта цель позволяет более четко сформулировать или глубже прояснить, возможно, уже знакомое обучаемым понятие «нарушителя» и связать задачи криптографической защиты информации с целями и возможностями нарушителя.

Воспринимаемость – это существенное свойство для информации, поскольку, например, нарушитель древности или средних веков, не умеющий читать, не мог воспринять информацию зашифрованного послания, а позже нарушитель, не имеющий радиоприемника, не смог бы воспринять информацию в радиоканале. Таким образом, криптография с точки зрения атак – это область действия высококвалифицированных и хорошо оснащенных нарушителей.

Криптография при этом позиционируется в

классе математических наук, связанных с процессами преобразования форм информации (для передачи информация должна принять некую форму и в рамках этой формы должна быть преобразована).

С другой стороны, очевидно, что с развитием технологической цивилизации субъектами передачи и приема начинают становиться технические системы, а информация принимает существенно более разнообразные формы представления, чем текст на бумаге или свитке папируса.

Кроме того, процесс передачи становится таким, что потенциальным нарушителям гораздо проще становится не только перехватывать информацию (например, по радиоканалу), но изменять ее или целиком формировать новую, не принадлежащую отправителю.

Процессы автоматизации передачи и обработки информации обуславливают необходимость реализации математических алгоритмов преобразования в рамках технических систем, делая криптографию технической наукой.

Современная криптография в основном опирается на вычислительные алгоритмы и системы как при реализации шифров, так и при их анализе, следовательно, использует информационные и компьютерные системы.

Таким образом, криптография оказывается «встроена» в информационную технологию, когда важными являются вопросы практической реализации криптоалгоритмов в конкретной компьютерной или технической системе. Поэтому часто и обоснованно полагают, что криптография – отдельная часть компьютерной безопасности.

Самой важной задачей криптографии логично представляется создание «хороших» шифров с точки зрения их качества, чтобы их невозможно было «прочитать».

Шифр, как система преобразования информации, должен быть «устойчивым «или «стойким» в некотором математическом смысле. Кроме того, логично возникает некоторый «секретный элемент», который должен быть как у отправителя, так и у получателя.

Кроме синтеза качественных шифрующих преобразований (шифров) современная криптография изучает:

• оптимизацию криптоалгоритмов (чтобы шифрование в технических системах «работало» быстрее);

• свойства датчиков случайных чисел (чтобы получать «секретные элементы» — ключи шифра хорошего качества);

• надежность программной или аппаратной реализации шифров (чтобы ошибки разработчиков или программистов, а также сбои оборудования не приводили к снижению качества).

Предметом изучения современной криптографии также являются:

• возможности улучшения криптоанализа («взлома» шифра) с использованием побочных электромагнитных излучений или других сигналов от работы компьютерной или шифрующей техники;

• криптографические протоколы, в том числе различные алгоритмы распределения и хранения ключей, включая квантовые;

• алгоритмы авторизации и защиты целостности (электронная подпись);

• прикладное применение криптографии (банковские системы, блокчейн, голосование, интернет вещей).

Изучая основы современной криптографии, следует напомнить обучаемым, что безопасный обмен информацией является не только предметом научных изысканий, но и объектом художественного отражения в искусстве и литературе, и сопровождает человека в течение всей его осмысленной (т. е. использующей письменность) истории.

С древних времен зашифрование и стеганографирование (изготовление невидимых сообщений) представляло актуальную и интересную задачу, часто жизненно важную для судеб отдельных исторических личностей и даже государств. Соревнование и драматическая судьба шифровальщиков и дешифровальщиков не раз становились сюжетом различных произведений XX века [2], таких как «Алан Тюринг: «Энигма», «В круге первом» и другие.

Заслуживает внимания художественный фильм «Игра в имитацию» (англ. The Imitation Game) — фильм-драма, снятый по сценарию Грэма Мура, основанному на биографической книге Эндрю Ходжеса о криптографе времени Второй мировой войны Алане Тьюринге, кото-

рый «взломал» процесс шифрования немецкой шифровальной машины «Энигма». Дисковая электромеханическая шифровальная машина «Энигма» является и по сей день весьма примечательным устройством, дешифрование которого в то время явилось беспрецедентным успехом.

«В круге первом» — роман Александра Солженицына, написанный в 1955—1958 годах по его воспоминаниям о работе во время тюремного заключения на «шарашке» (спецтюрьме МВД — МГБ) в Марфино, где после Второй мировой войны работали заключённые инженеры. Этот роман является первым произведением, опубликованным в серии «Литературные памятники» при жизни автора, посвященным работам над первым в мире шифратором голосовых сообщений.

«Утоли моя печали» - заключительная книга автобиографической трилогии известного писателя, литературного критика, германиста Льва Копелева, в которой также описана «шарашка», где вместе жили и работали заключенные А. Солженицын, Л. Копелев, Д. Панин - прототипы героев романа А. Солженицына «В круге первом».

Исторические и литературные экскурсы в сложность проблем криптографии, её значимость для исторического развития народов и государств могут вызвать неформальный интерес обучаемых к предмету.

Необходимо заметить, что криптография, как никакая другая наука, отражала тенденцию ускорения обработки информации, подсознательно апеллируя к различным вычислительно трудоемким алгоритмам, являясь и фактором ускорения развития информационных технологий (пример — упомянутая выше операция «Ультра» по дешифрованию шифровальной машины «Энигма», которая, по мнению известных современников и историков существенно сократила время Второй мировой войны).

Современные шифры и их анализ — в первую очередь информатика, большие данные, новая математика и инженерные прорывы.

Понятие шифра традиционно имеет как практические, так и более «академичные» определения.

Шифр – совокупность алгоритмов или отображений открытой (общедоступной) информации, представленной в формализованном виде, в недоступный для восприятия шифрованный текст (также представленный в формализованном виде). Шифр обязательно зависит от внешнего параметра (ключа), без знания которого невозможно шифрованную информацию преобразовать в открытую. Ключ должен быть задан или сконструирован таким образом, чтобы его нельзя было определить ни по шифрованной, ни по открытой информации.

Шифрование информации – взаимнооднозначное математическое (криптографическое) преобразование, зависящее от ключа (секретный параметр преобразования), которое ставит в соответствие блоку открытой информации в некотором цифровом представлении блок шифрованной информации, также представленной в цифровом виде. Термин шифрование объединяет в себе два процесса: зашифрование и расшифрование информации.

Шифратор – аппарат или программа, реализующая шифр. В современной литературе вводится понятие “средства криптографической защиты информации” (СКЗИ), которое включает в себя шифратор, но в целом является более широким.

Альтернативным «академическим» определением шифра, приведенным в [3], является:

Шифр [cipher] — семейство обратимых отображений множества последовательностей блоков текстов (сообщений) открытых в множество последовательностей блоков текстов (сообщении) шифрованных и обратно, задаваемых функцией шифрования. Каждое из отображений определяется некоторым параметром, называемым ключом, и описывается некоторым алгоритмом шифрования, реализующим один из режимов шифрования. Математическая модель шифрования включает алгоритм зашифрования, алгоритм расшифрования, определение режима шифрования, а также модель множества текстов открытых сообщений.

В зависимости от способа представления текстов открытых (сообщений) различают блочные, поточные и другие шифры.

Основными требованиями, определяющими качество шифрования, являются: стойкость криптографическая, имитостойкость, помехо-

устойчивость шифра.

Ключ – некоторый неизвестный параметр шифра, позволяющий выбрать для шифрования и расшифрования конкретное преобразование из всего множества преобразований, составляющих шифр. Простая ассоциация – ключ от замка – во многом проясняет смысл термина. Есть много одинаковых качественно ключей, но лишь некоторые (или чаще один) откроют замок.

Шифрование – процесс получения шифрованного текста, основанный на знании ключа.

Дешифрование – восстановление открытого текста или ключа по шифрованному тексту.

Злоумышленник (нарушитель) – субъект (или физическое лицо), не знающий ключа или открытого текста и стремящийся получить его. Полагается, что нарушитель контролирует канал обмена информацией между абонентами, использующими шифрование.

Разработку и применение шифров называют криптографией, в то время как науку о раскрытии шифров — криптоанализом.

Поскольку проверка шифров на стойкость является обязательным элементом их разработки, криптоанализ также является частью процесса разработки.

Криптология — это наука, предметом которой являются математические основания как криптографии, так и криптоанализа одновременно.

Криптоаналитической атакой называют использование специальных методов для раскрытия ключа шифра и/или получения открытого текста. Предполагается, что атакующей стороне известен алгоритм шифрования, и ей требуется только найти конкретный ключ.

Другая важная концепция связана со словом «взлом». Когда говорят, что некоторый алгоритм был «взломан», это не обязательно означает, что найден практический способ раскрытия шифрованных сообщений. Здесь может иметься в виду, что найден способ существенно уменьшить ту вычислительную работу, которая требуется для раскрытия шифрованного сообщения методом «грубой силы», то есть простым перебором всех возможных ключей.

При осуществлении такого взлома практически шифр все же может оставаться стойким, поскольку требуемые вычислительные возможности будут все еще оставаться за гранью реального. При этом существование метода взлома не означает еще реальной уязвимости алгоритма, обычно такой алгоритм более не используют или модифицируют.

Понятие «нарушитель» в криптографии тесно связано с понятием “твердого незнания” им ключа. В соответствии с методологией, принятой в современной криптографии, надежность шифра определяется степенью безопасности используемых в нем ключей, поскольку все долговременные элементы криптографической системы (множество правил шифрования, его механизм) рано или поздно станут известными злоумышленнику. Этот принцип был сформулирован еще в конце XIX в. и получил название “правила Керкгоффса” (Kerckhoffs’s desiderata).

В [3] правило Керкгоффса — общепринятое в криптографии предположение проведения криптоанализа, впервые сформулированное голландским криптографом Н. Керкгоффсом («компрометация системы не должна причинять неудобств корреспондентам»). В современном понимании это правило означает, что описание криптосистемы (криптопротокола) может быть полностью известно противнику и/или нарушителю, а стойкость криптографическая основана только на том, что не известен ключ (секретный) [3].

В современной криптографии считается, что злоумышленник имеет возможность также произвольным образом изменять сообщения.

Поэтому вводится еще один термин: подлинность – принадлежность сообщения конкретному автору и неизменность содержания сообщения. Подлинность естественным образом делится на «неизменность» и «авторство».

Для описания шифра может быть использовано текстуальное или символьно-математическое описание криптографического преобразования. Кроме того, разумно представлять схему работы шифра (криптосхему) в виде конструкций одного из «общеупотребительных» языков программирования. Это весьма наглядно для программистов и специалистов в области реализации криптографических алгоритмов.

Такого рода представление ставит вопрос о проверке соответствия описания криптографи-

ческого преобразования и его реализации на языке программирования, либо в виде аппаратного изделия.

Криптографическая схема (криптосхема) – описание алгоритма криптографического преобразования в виде наглядно-графической модели, чаще всего в виде схемы или блок-схемы, в которой блоки представляют собой некоторые законченные функции, входящие в состав криптографического преобразования.

Эти функции, как правило, имеют «элементарный» характер – например, поэлементная (побайтовая) сумма двух массивов по модулю 2. В частности, такая операция используется в алгоритме шифрования «Кузнечик [4].

Несколько шире криптографической схемы формулируется система шифрования.

Система шифрования [cryptosystem, син. шифрсистема] — система криптографическая, предназначенная для защиты информации от лиц, не имеющих права доступа к ней. Защита обеспечивается путем зашифрования информации. Математическая модель системы шифрования включает способ кодирования исходной и выходной информации, шифр и систему ключевую. Основными требованиями, определяющими качество системы шифрования, являются: стойкость криптографическая, имитостойкость, помехоустойчивость шифра и др. [3].

Соответствие реализации криптографического преобразования его описанию – категория тождества, выраженная в соотнесении аналогичных или тождественных входных и выходных массивов информации, а также внутренних состояний криптографического преобразования, описанных в криптографической схеме и реализованных функционально в виде программы или аппаратного изделия.

Проверка соответствия реализации криптографического преобразования его описанию – комплекс процедур, позволяющий детерминированно или вероятностно (с высокой вероятностью) убедиться в их соответствии, и выполняемый, как правило, при помощи тестов или тестовых процедур.

С точки зрения системного анализа криптографическое преобразование (зашифрование) рассматривается в виде «белого ящика» (т. е. преобразование имеет известную структуру), на входе которого – открытый текст и ключ зашифрования, на выходе – зашифрованный текст. Такое представление соответствует принципу Керкгоффса.

При этом «белый ящик» погружен в некоторую «окружающую среду», которая представляет собой среду реализации криптографического преобразования в виде программного или аппаратного окружения.

Достаточно часто используют термин «среда функционирования криптографического средства (криптосредства)» (СФ или СФК), который также описывает окружающее «белый ящик» пространство в виде компьютерной системы, реализующее криптопреобразование и связанные процессы обработки, передачи и хранения информации. В этом случае криптографическое преобразование осуществляется в подсистеме некоторой большей с теоретико-множественной точки зрения системы.

Одной из тенденций развития современной криптографии является квантовая криптография – когда ключи в системе распределяются с использованием физических процедур обмена отдельными пакетами фотонов, которые нельзя физически перехватить, не изменив их параметры.

Вторая тенденция – исключение человека и различных программных алгоритмов из процедур обеспечения безопасности, переход к криптофизической безопасности, когда человеческий фактор по возможности исключен, а система построена на простой, надежной и доверенной платформе. Она связана также с «технической сингулярностью», когда ключи криптографического алгоритма «неизвлекаемо» хранятся в рамках некоторого замкнутого и невскрываемого изделия [5].

ЗАКЛЮЧЕНИЕ

Четкое изложение понятийных основ криптографии позволит преподавателю донести до обучаемых комплексный характер современной криптографии, ее системность, а также зависимость предмета от установок, позиций и требований государственных регуляторов в рассматриваемой области.

СПИСОК ЛИТЕРАТУРЫ

1. А.Щербаков Перспективы современной криптографии Проектирование будущего. Проблемы цифровой реальности.- 2020. № 1 (3)- С. 227-233.
2. Hodges A. Alan Turing: The Enigma. Princeton University Press; Revised edition. 2014. Pp. 768.
3. Словарь криптографических терминов под редакцией Б. А. Погорелова и В. Н. Сачкова.- Москва: М.: МЦНМО, 2006.- 91 с.
4. ГОСТ Р 34.12–2015 «Информационная технология. Криптографическая защита информации. Блочные шифры». Утвержден приказом Федерального агентства по техническому регулированию и метрологии от 19 июня 2015 г. N 749-ст: дата введения 1 января 2016 г. – Москва: Стандартинформ, 2018.
5. Гриняев С.Н., Правиков Д.И., Разгуляев К.А., Рязанова А.А., Хан Д.В., Щербаков А.Ю. Основные методологические подходы к формированию и обоснованию архитектуры и протокола квантового распределенного реестра //Научно-техническая информация, сер. 2 Информационные процессы и системы.- 2020. №1. С. 11-18.

УДК: 336.221

Индустрия криптовалют России в мировом контексте: анализ актуального состояния

D.S. Machikhin

Russian Cryptocurrency Market in a Global Context: Analysis of the Current State

Abstract. *The article is devoted to the analysis of the current state of the cryptocurrency industry in the world and in Russia. The dynamics of the indicators of the global Bitcoin cryptocurrency market and changes in investment subjects are considered, the growth of involvement and acceptance of cryptocurrencies and related projects and technologies by institutional investors is shown. The indicators of projects related to the blockchain technology of crypto-currencies, non-fungible tokens, metaverses, decentralized finance, and the play-to-earn concept were studied. The viewpoints of the main regulators of Russia regarding the inclusion of cryptocurrencies in the existing regulatory framework, the impact of a potential ban on cryptocurrencies on the country's economy, the speed of technical development, and the investment climate are given. The analysis of the global market volume and Russia's share in it, as well es the estimated increase in the number of cryptocurrency users are presented, the prospects for mining in Russia are described. The potential income from these types of activities for the Russian budget has been calculated.*

Keywords: *cryptocurrency, regulation of the cryptocurrency market, taxation of cryptocurrencies, bitcoin, blockchain, token, digital asset, metaverse, decentralized finance, mining, cryptocurrency exchange.*

Д.С. Мачихин
Инвестор и IT предприниматель, основатель сервиса для легализации и налогообложения криптовалют.
E-mail: dm@bitnalog.com

Аннотация. *Статья посвящена анализу актуального состояния индустрии криптовалют в мире и в России. Рассмотрена динамика показателей мирового рынка криптовалюты Биткоин и изменения субъектов инвестирования, показан рост вовлеченности и принятия криптовалют и смежных проектов и технологий со стороны институциональных инвесторов. Изучены показатели проектов, связанных с технологией блокчейн криптовалют и смежными технологиями невзаимозаменяемых токенов, метавселенных, децентрализованных финансов, концепцией play-to-earn. Приведены позиции главных регуляторов России касательно включения криптовалют в существующую нормативную базу, влияния потенциального запрета криптовалют на экономику страны, скорость технического развития, инвестиционный климат. Представлен подробный анализ мирового объема рынка и доли России в нем, а также прогноз увеличения числа пользователей криптовалют, описаны перспективы майнинга в России. Рассчитан потенциальный доход от указанных видов деятельности для российского бюджета.*

Ключевые слова: *криптовалюта, регулирование рынка криптовалют, налогообложение криптовалют, биткоин, блокчейн, токен, цифровой актив, метавселенная, децентрализованные финансы, майнинг, биржа криптовалют.*

ВВЕДЕНИЕ

На сегодняшний день мировая индустрия криптовалют и связанные с ней технологии образуют значительный пласт мировой экономики, в котором Россия занимает одну из лидирующих позиций. Об этом свидетельствуют всевозможные факты и показатели по числу криптовалют, их пользователей и инвесторов, примеров использования криптовалютных сетей в частности и технологий распределенных реестров в целом. Несмотря на очевидную тенденцию к интеграции криптовалют в круг инструментов инвестирования и финансовую сферу, представителями государственной власти отрицается необходимость регулирования рынка криптовалют, уже практически сформированного в отсутствии соответствующего законодательства, а также достигшего показателей, приведенных в настоящей статье.

Феномен криптовалют, их сильное влияние на сферу финансов и инвестиционный климат при недостаточной исследованности приводит к появлению противоречивых подходов к политике регулирования. При этом разработка разумных мер требует анализа эмпирического опыта использования и подходов к регулированию криптовалют за рубежом и в России [1]. Необходимо учитывать и технические особенности майнинга и обмена, а также потенциальные преимущества от регулирования рынка

для государственного бюджета, основываясь на мнениях представителей всего сообщества в этой области.

Об отсутствии в действиях регулирующих органов определенного курса на формирование системного подхода к политике в области цифровых технологий, применяемых в финансовой сфере, неоднократно упоминалось, в том числе в научных изданиях [2-4]. При этом в соответствии с поручением Президента РФ (октябрь 2017 г.) [5] Правительством совместно с Банком России до 1 июля 2018 г. должно было быть обеспечено внесение изменений в законодательство, определяющих понятия и статус цифровых технологий, применяемых в финансовой сфере, и установлены требования к организациям, осуществляющим производство на основе принципов криптографии в среде распределённых реестров.

Однако, по мнению профессиональных представителей криптоиндустрии в России, значимое продвижение в регулировании индустрии криптовалют до сих пор отсутствует, более того, такие ключевые термины, как «криптовалюта» и «смарт-контракт», законодательно не определены, не установлены правила выпуска и обращения цифровых валют. Также отсутствие конкретных процедур и сроков включения операторов цифровых финансовых активов в реестр Банка России наряду с разрешительными процедурами Минсвязи делают почти невозможной работу оператора.

Необходимо отметить, что подобная правовая неопределенность в сочетании с запретительным характером поправок, вносимых в законодательные акты, препятствует развитию легального оборота и майнинга криптовалют в России. Кроме того, проекты в области публичного блокчейна, поданные на тестирование в регулятивную «песочницу», сформированную в 2018 г, не получили однозначного одобрения со стороны Банка России как главного финансового регулятора страны [6], что также свидетельствует об отсутствии развития в сторону легализации криптовалют.

Опубликованные в начале 2022 г. тезисы доклада Банка России, посвященного тенденциям в области криптовалют, угрозам, связанным с развитием криптоиндустрии, и возможным мерам по ее регулированию [7], повторно закрепили позицию главного финансового регулятора страны о недопустимости разрешительных мер. Однако, учитывая аргументы в пользу легализации и регулирования криптовалют, которые, в частности, были приведены в работе [8], нетрудно сделать вывод, что при нахождении криптовалют в “серой” зоне практически невозможно будет направить преимущества отрасли на пользу государству, а также минимизировать реальные и потенциальные угрозы, связанные с их использованием.

Одной из основных задач настоящей статьи является описание и анализ структуры и количественных показателей рынка криптовалют. Основные цели - наиболее объективно и полно оценить имеющийся потенциал индустрии криптовалют для дальнейшего формирования системного подхода к вопросам их законодательного регулирования, упростить процесс оценки различных релевантных показателей представителями органов власти и бизнеса.

Для решения указанной задачи используются данные международных аналитических порталов, социологических обзоров, инсайдерской информации, собственных баз данных, данных открытых блокчейн-систем (“он-чейн” информации), а также мнения экспертов.

Достигнутые результаты позволят объективно оценить потенциал развития и значение данной отрасли для экономики страны, а также сформировать стратегически верный подход к ее регулированию. Меры по регулированию рынка криптовалют, принятые в соответствии с результатами, смогут обеспечить не только скорейший приток дополнительных доходов в бюджет, но и большую прозрачность и предсказуемость рынка, создание гарантий защиты капитала любых категорий граждан. Кроме того, данные меры будут способствовать минимизации негативных последствий от бесконтрольных трансграничных переводов криптовалют в другие страны и сохранению капитала внутри страны.

ДИНАМИКА ПОКАЗАТЕЛЕЙ РЫНКА КРИПТОВАЛЮТЫ БИТКОИН В 2020-2022 ГГ., ОСНОВНЫЕ ИНВЕСТОРЫ

Кризис мировых финансовых рынков в начале 2020 года, вызванный пандемией коронавируса, отразился и на рынке криптовалют. Однако курс Биткойна за несколько месяцев вырос до значений начала года, а к концу 2020 года достиг отметки 29000 $. В ноябре 2021 года цена за 1 биткоин превысила отметку в 67000 $. Таким образом, в 2021-м году биткоин стал безусловным лидером рынка, показав к ноябрю почти 100% роста в сравнении с золотом: -2.5%, индексом S&P500: +26%, индексом Nasdaq: +31%, индексом RTSI: +23% за тот же временной период. В результате импульса, созданного Биткоином, цены на многие криптовалюты продолжали стремительно расти, а общая капитализация рынка криптовалют выросла в 4 раза: с 735 млрд. долл. на начало 2021 года до пикового значения в 3 трлн. долл. в ноябре того же года (рис. 1).

Рис. 1. Общая рыночная капитализация криптовалют за 2021 год[1]

Стоимость как важнейший фактор, влияющий на рост интереса со стороны мирового сообщества, определила не только увеличение спроса на криптовалюты, но и ускорение процесса их принятия. В 2021 году рынок криптовалют привлек значительный интерес розничных и институциональных инвесторов, крупнейших публичных компаний, государственных регулирующих органов.

Крупнейшим институциональным инвестором криптовалюты Bitcoin является компания MicroStrategy, которой принадлежит приблизительно 0,6% биткоинов, или около 125000 BTC. Крупными долями биткоинов владеют компании Tesla (≈0,2%), Block (≈0,04%), Marathon Digital Holdings (≈0,04%), Voyager Digital, Galaxy Digital Holdings Ltd. и другие [9]. Суммарный объем биткоинов на счетах публичных компаний по курсу на март 2022 года составлял $8,8 млрд [10].

В результате роста вовлеченности со стороны крупных компаний рынок криптовалют весьма гибко стал реагировать на действия крупнейших институциональных инвесторов, направленные на использование криптовалюты, например, в качестве платежного средства. Так, при введении Илоном Маском оплаты автомобилей биткоинами был зафиксирован рост курса биткоина и, наоборот, при отмене из соображений энергетической безопасности – падение курса.

В свою очередь, принятие криптовалют со

[1] Источник: https://www.coingecko.com/ru/global_charts

стороны крупных инвесторов априорно повышает их статус, в отдельных случаях приравнивая его к статусу традиционных фондов. Так в феврале 2022 года стало известно, что крупнейшая в мире компания по управлению финансовыми активами BlackRock готовится не только стартовать платформу для торговли криптовалютами [11] с клиентской поддержкой, но и создать программу, по которой клиенты смогут брать кредиты у BlackRock, используя криптоактивы в качестве залога. Под управлением фонда находятся активы на сумму более чем $10 трлн [12].

Таким образом, выраженной тенденцией последних лет является заметный рост вовлеченности институциональных инвесторов в основные проекты, связанные с криптовалютами и сопряженными технологиями. Аналитики рынка криптовалют из сферы традиционных финансов, ранее выступавшие с критикой криптовалют, в настоящее время признают их как неизбежный этап в развитии экономики. Другие значимые проекты на основе технологии блокчейн представлены в следующем разделе.

СОВРЕМЕННЫЕ ЗНАЧИМЫЕ ПРОЕКТЫ НА ОСНОВЕ ТЕХНОЛОГИИ БЛОКЧЕЙН

Индустрия криптовалют привлекла глобальную аудиторию вследствие развития инновационных идей на основе блокчейна, таких как невзаимозаменяемые токены, Play-To-Earn («играй и зарабатывай»), Метавселенные, децентрализованные финансы и других решений. На рисунках 2-6 представлены графики динамики поисковых запросов «NFT», «Play-To-Earn», «Metaverse», «Децентрализованные финансовые сервисы», а также поисковых запросов “Buy cryptocurrency” в Google.

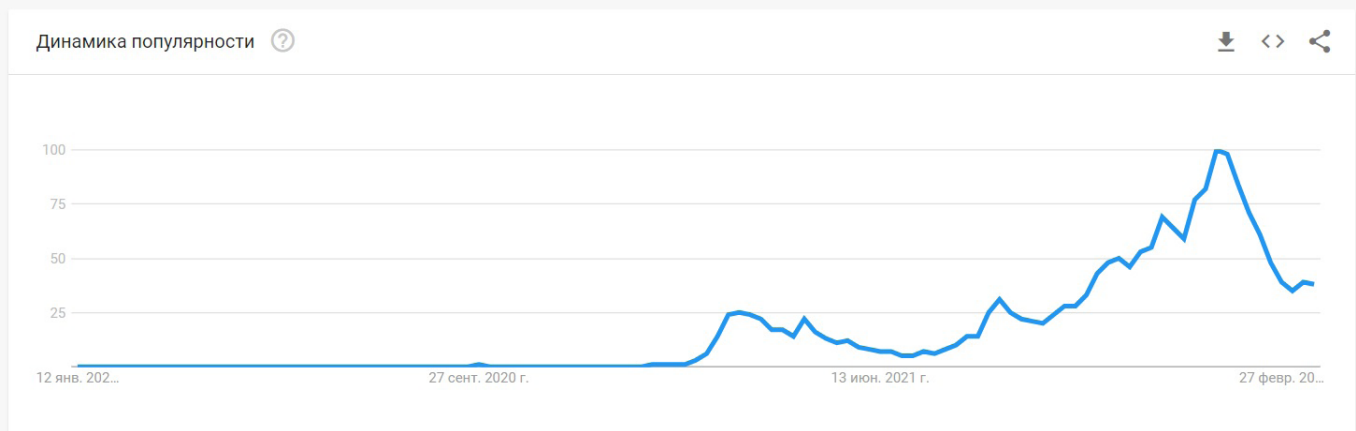

Рис. 2. Динамика поисковых запросов “NFT” в Google[2]

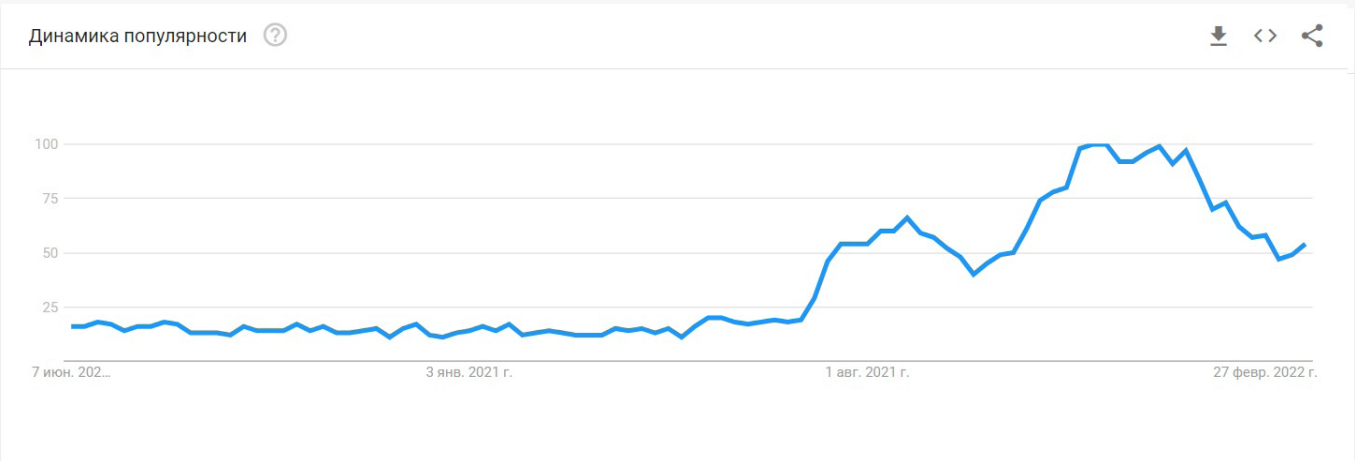

Рис. 3. Динамика поисковых запросов “Play to earn” в Google[3]

[2]Источник: https://trends.google.com/trends/explore?date=2020-01-06%202022-03-28&q=nft

[3]Источник: https://trends.google.com/trends/explore?date=2020-06-01%202022-03-28&q=play%20to%20earn

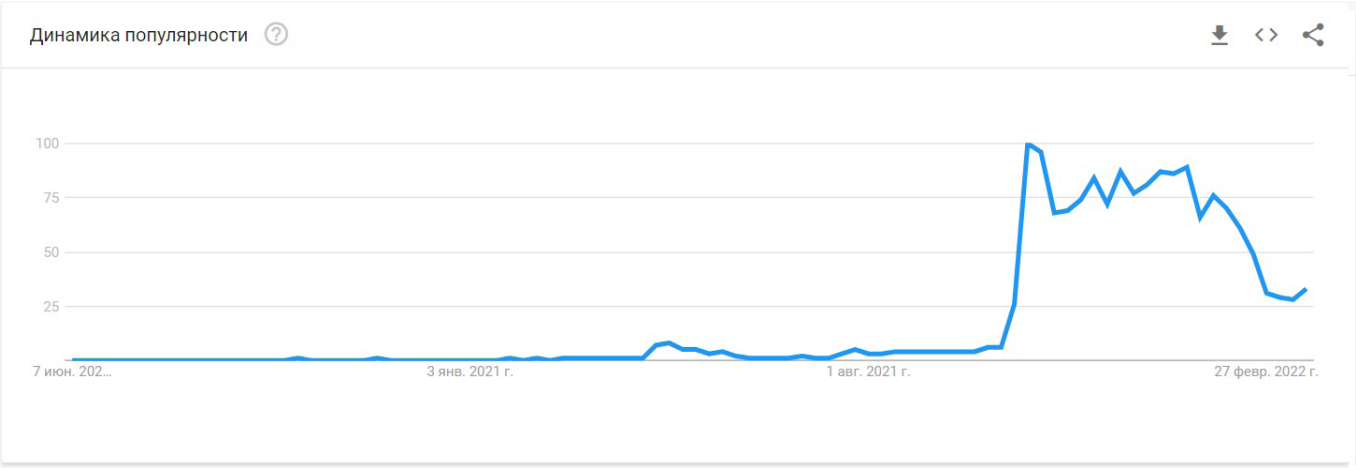

Рис. 4. Динамика поисковых запросов “Metaverse” в Google[4]

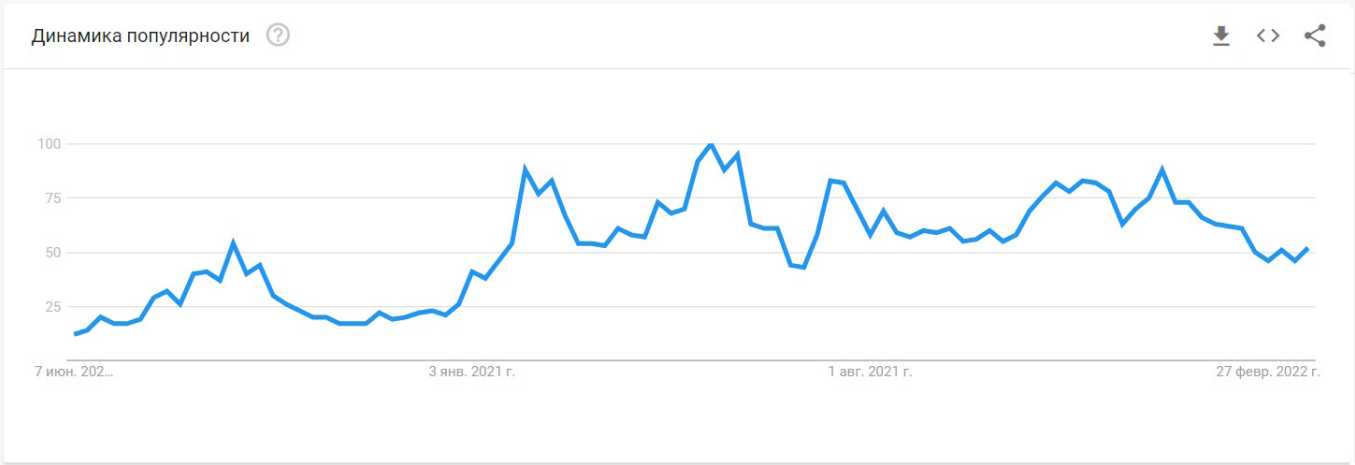

Рис. 5. Динамика поисковых запросов по теме “Децентрализованные финансовые сервисы” в Google[5]

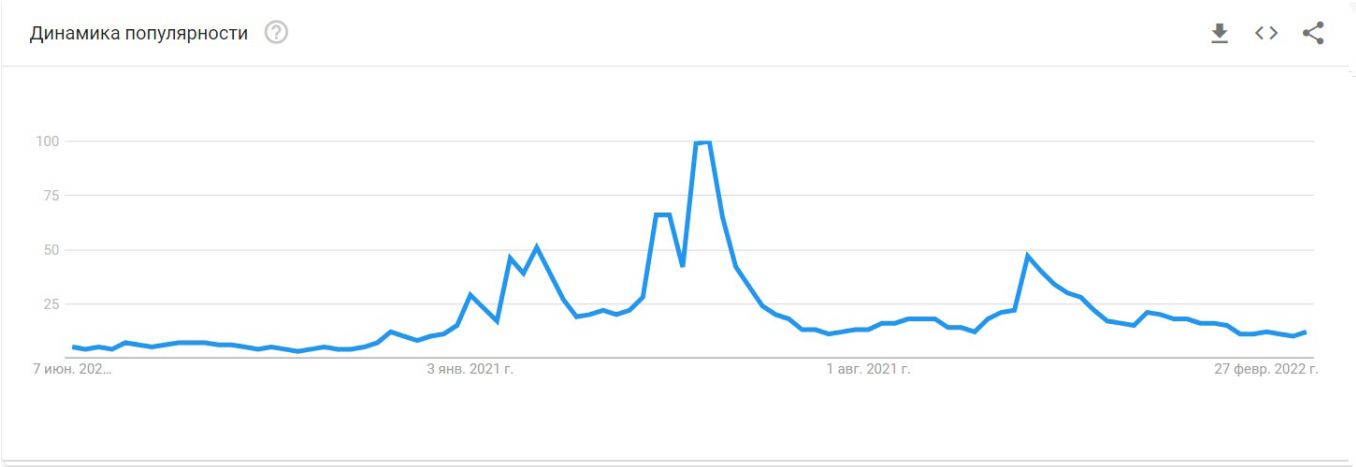

Рис. 6. Динамика поисковых запросов по теме “Buy cryptocurrency” в Google[6]

[4]Источник: https://trends.google.com/trends/explore?date=2020-06-01%202022-03-28&q=metaverse
[5]Источник: https://trends.google.com/trends/explore?date=2020-06-01%202022-03-28&q=%2Fg%2F11jp19xcvr
[6]Источник: https://trends.google.com/trends/explore?date=2020-06-01%202022-03-28&q=buy%20cryptocurrency

На графиках рисунков 2-6 заметна тенденция к скачкообразному росту поисковых запросов, который объясняется особенностями поведения инвесторов до и после принятия инвестиционных решений в рамках указанных проектов. При этом рост поисковых запросов «NFT» (рис. 2), вероятно, связан с беспрецедентным ростом капитализации рынка NFT к концу 2021 г., а растущая популярность концепции «Play-To-Earn» обусловлена интеграцией технологии блокчейн и игровой индустрии, которая и позволяет в процессе игр обмениваться и покупать цифровые активы, в том числе в виде NFT.

Рассмотрим подробно указанные проекты и технологии.

Невзаимозаменяемые токены (англ. non-fungible token, NFT)

Покупка произведения искусства в виде NFT за 69,34 млн долл. на аукционе Christie's [13] в начале прошлого года стала значимым событием не только с точки зрения развития криптовалют (самая крупная сделка на рынке NFT), но и в масштабе арт-рынка (необычная для аукционного дома Christie’s сделка по продаже предмета искусства в виде NFT) [14]. Автор проданной работы, цифровой художник, графический дизайнер и аниматор Бипл (Майк Винкельманн), вошел в тройку самых дорогих из ныне живущих художников мира. Этот прецедент вовлек новую аудиторию из креативных индустрий в развитие рынка NFT и активное использование криптовалют.

Напомним, что NFT (невзаимозаменяемый, уникальный токен) является новым средством хранения и реализации объектов, в т.ч. предметов искусства в цифровом виде, предметов цифрового искусства, и создается в NFT-мастерских, таких как OpenSea, Rarible, Mintable. Файлы с названием и описанием добавляются пользователем в его коллекцию, платформа создает токен, который отправляются на верификацию (на некоторых платформах токен создается с отсрочкой) [15]. Токены NFT можно хранить в кошельке и совершать операции с ними, как и с любой криптовалютой, однако NFT в силу индивидуальности наполнения, поскольку он обладает свойствами уникального предмета, невозможно разделить на части или обменять на аналогичный токен.

Таким образом, NFT является реестровой записью, содержащей цифровое произведение, как и информацию, связанную с ним (об авторе произведения, его владельце и т.д.), которая подтверждает права на реальный, как правило, уникальный объект.

По данным биржи криптовалют CEX.io, общая капитализация рынка NFT в 2021 г. превысила показатели 2020 года в 56 раз и составила 8$ млрд. К середине ноября 2021 г. объем торгов NFT составил $8.8 млрд [16], из которых 60% пришлось на торговлю предметами искусства и коллекционирования, а остальные 40% - на игровые NFT. Из методики цитируемого исследования следует, что к середине марта 2022 года общий объем торгов NFT составлял $11.7 млрд.

Показателен и тот факт, что общее количество активных кошельков на NFT-маркетплейсах за 2021 год выросло более чем в шесть раз [16].[7]

Концепция Play-To-Earn («Играй, чтобы заработать»)

Игры в концепции Play-To-Earn открыли новые экономические и бизнес-модели, позволив пользователям получать криптовалюты и ценные NFT, проводя время в игре. Игры на блокчейне позволят новому поколению геймеров по-настоящему владеть и распоряжаться внутриигровыми активами.

Согласно опросу, проведенному в конце 2021 г. популярной платформой для финансирования крипто-проектов Coinlist, 56,5% респондентов хотят видеть на платформе игровые проекты. Это подтверждает высокий спрос со стороны сообщества и, как утверждает Coinlist, убежденность в том, что игры станут поворотной точкой для массового внедрения блокчейна [17]. По состоянию на март 2022 года общий объем торгов игровыми NFT составил $4.4 млрд.

Крупнейшая игровая компания Ubisoft рассматривает блокчейн в качестве одного из перспективных направлений [18]. В исследовании, проведенном в конце 2021 года, Google оцени-

[7]Источник: https://www.theblockcrypto.com/data/nft-non-fungible-tokens/gaming

вал размер игровой индустрии в 3 миллиарда игроков, оборот за 21-ый год - приблизительно $175.8 млрд. [19]. Таким образом, игры play-to-earn обладают большим потенциалом роста, привлекая аудиторию глобальной быстрорастущей индустрии гейминга.

Метавселенные

В июле 2021 года основатель Facebook Марк Цукерберг объявил о планах по созданию метавселенной, после чего Facebook сменил название на Meta. [20]. Разработку собственных метавселенных анонсировали такие гиганты, как Epic Games [21] (с привлечением стратегических инвестиций многих компаний-партнеров, в том числе Sony Group Corporation) и Microsoft [22]. Развитие метавселенных не происходит без участия технологии блокчейн, поскольку именно она позволяет формировать в них цифровую экономику с различными типами токенов и NFT.

Метавселенные, хоть и находятся на ранней стадии своего развития, уже сегодня позволяют пользователям покупать землю, виртуальные объекты недвижимости, строить здания и организовывать виртуальные мероприятия. Так в 2021 году цифровую недвижимость в крупнейших метавселенных продали на $500 млн [23], а список компаний, открывших виртуальный офис или представительство внутри метавселенных, включает компании, относящиеся не только к криптоиндустрии, но и к другим секторам экономики, например, аукционный дом Sotheby's [24] и банк JP Morgan Chase [25].

Токены NFT, игры Play-To-Earn и Метавселенные стали катализаторами широкого распространения цифровых активов в 2021 году, вовлекая миллионы людей в процесс их массового использования.

Децентрализованные финансы (DeFi)

Прошедший год также характеризуется стремительным ростом рынка децентрализованных финансов. Стоимость средств в сфере DeFi выросла с $18 млрд на начало 2021 года до более чем $240 млрд в конце года. По состоянию на март 2022 года около $215 млрд. инвестировано в DeFi[8].

Годовой рост объема торгов на децентрализованных биржах (DEX) в ноябре 2021 года составил 522%. Своего максимума он достиг в мае 2021 года - по итогам месяца этот показатель преодолел отметку в $163 млрд [16].

Экосистема финансовых сервисов, называемая также dApps (decentralized applications), создана на основе смарт-контрактов блокчейна Ethereum и других блокчейнов. В настоящее время из-за низкой пропускной способности и перегруженности сети блокчейна Ethereum (несколько десятков операций в секунду) значительно выросла стоимость транзакций (транзакция может стоить сотни долларов). Большое количество альтернативных блокчейнов, таких, как Solana, Terra, Avalanche, появились как решение этой проблемы и способны поддерживать до нескольких тысяч транзакций в секунду, что снижает их стоимость.

Анализ трендов в области криптовалют и других проектов на основе технологии блокчейн подтверждает существование достаточно большого количества возможностей, которые реализуются либо потенциально могут быть реализованы в децентрализованных финансах в ответ на возникающие проблемы, задачи, требования и вызовы. Это, в свою очередь, создает технические предпосылки для формирования механизмов и инструментов влияния как на индустрию криптовалют, так и развитие и применение связанных с ней технологий, что также является одним из положительных факторов развития функциональной деятельности по регулированию криптовалют.

РЕГУЛИРОВАНИЕ РЫНКА КРИПТОВАЛЮТ

Политика регулирования в странах мира

Рынок криптовалют на протяжении многих лет находится в центре внимания регуляторов во всем мире. В некоторых странах отмечаются потенциальные изменения, связанные с характером взаимодействия акторов финансового криптовалютного рынка, с ростом возможных инноваций в различных секторах экономики. Правовой режим криптовалют по странам

[8]Источник: https://defillama.com/

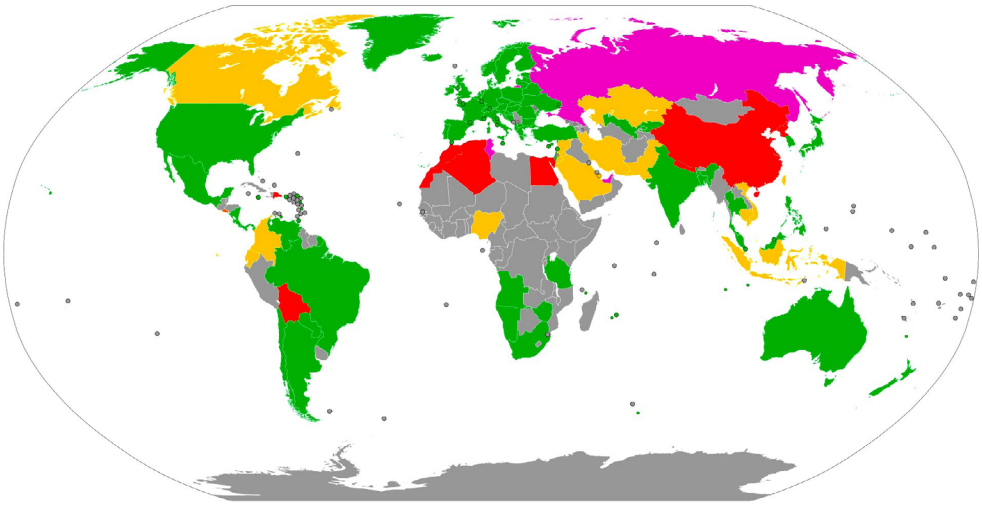

Рис. 7. Актуальный правовой режим криптовалют в странах мира[9]
(1.Законное платежное средство; 2.Разрешен (законно использование биткоина); 3. Спорный (есть ограничения использования биткоина, установленные законодательством); 4. Спорный (толкование старых законов, нет прямого запрета на использование биткоина); 5. Запретительный (полный или частичный запрет); 6. Отсутствуют данные.)

представлен на рис. 7.

Латиноамериканский Сальвадор стал первой страной в мире, в которой биткоин был объявлен законным платежным средством [26]. Но пока одни регуляторы разрабатывают методы включения криптовалют в существующую нормативную базу, есть и те юрисдикции, в которых деятельность, связанная с криптовалютами, запрещена. Так, например, власти Китая вслед за запретом майнинга вывели из легального поля любые транзакций с криптовалютой. Детальный анализ зарубежных подходов к регулированию криптовалют приведен в статье [1].

Регулирование рынка криптовалют в России

История регулирования криптовалют в России, включая дискуссии об их природе и влиянии на общество и экономику, берет свое начало в 2013 году. До 2018 года риторика со стороны регуляторов была исключительно запретительной. В 2019 году был принят Федеральный закон № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты РФ» [27], впервые закрепивший понятие цифровых финансовых активов, которое, однако, не соответствует реалиям рынка криптовалют в России. В законе не даются четкие определения статуса цифровых технологий и ключевые понятия, применяемые в области криптовалют, такие, как «криптовалюта» и «смарт-контракт», но содержатся противоречия, в том числе касательно базовых механизмов, связанных с работой криптовалютных сетей.

Так, условием выпуска ЦФА является положительное решение оператора ИС, включенного ЦБ РФ в реестр операторов информационных систем, включенного Банком России в реестр операторов ИС, но сроки включения не указаны. Выполнение этого требования становится практически невозможным, поскольку оператором на базе платформы, как правило, реализуется комплексный набор услуг. Вопросы корректности терминов в области ЦФА рассматриваются в работе [3].

В 2022 году Центральный Банк РФ и Министерство финансов РФ предложили различные концепции регулирования криптовалют. Доклад Центрального Банка РФ о регулировании криптовалют в России [7] вызвал широкий резонанс в сообществе. Позиция ЦБ была воспринята как предложение полного запрета

[9]Источник: https://en.wikipedia.org/wiki/Legality_of_cryptocurrency_by_country_or_territory

криптовалют. Очевидная необоснованность и бессмысленность потенциального запрета была отмечена ведущими представителями криптоиндустрии, что отражено в работе [8].

По мнению Минфина, такой запрет может привести к оттоку специалистов из страны, препятствованию техническому развитию, а также к потере потенциальных денежных средств от налоговых поступлений [28].

В настоящее время Министерство финансов работает над двумя новыми законопроектами в сфере криптовалют. Законопроект «О цифровой валюте» направлен на формирование правовой базы обращения и выпуска криптовалют[10]. Второй законопроект будет вносить изменения в уже существующие нормативные правовые акты в связи с принятием закона «О цифровой валюте»[11]. Правительство также продуктивно обсуждает варианты развития рынка криптовалют в России [29].

МИРОВОЙ ОБЪЕМ РЫНКА И ДОЛЯ РОССИИ В НЕМ

Число пользователей криптовалют в мире и России

Согласно исследованию, проведенному Crypto.com, за 2021 год число пользователей криптовалют во всем мире почти утроилось: с 106 миллионов в январе до 295 миллионов пользователей в декабре 2021 года [30]. Платежная платформа Triple A, по состоянию на 2021 год насчитывает в мире 300 миллионов пользователей криптовалют [31].

По состоянию на март 2022 года общемировой объем рынка криптовалют оценивается в 330 миллионов пользователей[12]. Россия является одним из ключевых игроков на рынке криптовалют. Доля пользователей из России в глобальном рынке криптовалют, по нашим расчетам, составляет не менее 4%. Таким образом, как минимум 13,2 миллиона пользователей криптовалют имеют отношение к России, что может составлять около 9% населения страны.

Методика производимых в настоящей работе расчетов приведена в разделе «Методологические подходы к проведению исследования».

Если экстраполировать скорость роста пользователей криптовалют на 2022 год, к началу 2026 года общемировое количество пользователей криптовалют может достигнуть предположительно 0,8-1 миллиарда человек, а количество пользователей в России вырастет приблизительно до 30 миллионов человек (26-33 млн. человек в зависимости от сценария) за этот же промежуток времени.

Количество криптовалютных кошельков у пользователей из России

Одной из ключевых особенностей экономики криптовалют является отсутствие ограничений на создание множества кошельков, каждому из которых присвоен один или более блокчейн-адресов. Максимальное количество криптокошельков является условно неограниченным благодаря технологиям хэширования, поэтому владение одним лицом десятками разных счетов является нормой.

Наряду с ростом интереса к сфере криптовалют, количество новых кошельков в системах крупнейших блокчейнов также неуклонно увеличивается. Так, по данным сервисов Glassnode[13] и Cryptoquant[14], в 2021-ом пользователи криптовалют создавали до 439000 новых кошельков Bitcoin и до 118000 новых кошельков Ethereum ежедневно. Напомним, что доля российских пользователей в сфере криптовалют составляет около 4%. Предположим, что на граждан РФ приходится столько же новых кошельков в процентном соотношении, следовательно, 17600 новых адресов в системе BTC и 4700 адресов ETH регистрировали россияне каждый день 2021-го года.

Также, по данным сервиса Glassnode, количество кошельков, которые успешно получали

[10]Официальный сайт для размещения информации о подготовке нормативных правовых актов https://regulation.gov.ru/projects#npa=125083
[11]Официальный сайт для размещения информации о подготовке нормативных правовых актов https://regulation.gov.ru/projects#npa=125084
[12]Источник: https://triple-a.io/crypto-ownership/.
[13]Источник: https://studio.glassnode.com/metrics?a=BTC&m=addresses.ActiveCount
[14]Источник: http://Cryptoquant.com

или отправляли хотя бы одну транзакцию сети, для сети Bitcoin в среднем за 2021-ый составило 985000 кошельков и 524000 кошельков Ethereum. При соразмерной доле российских пользователей среди таких активных кошельков почти 39400 и 21000 кошельков Биткоина и Эфира соответственно находятся в распоряжении у граждан РФ.

Количество активных пользователей криптовалют в России

Под активными пользователями криптовалют подразумеваются пользователи, которые за месяц хотя бы раз произвели транзакцию в криптовалютных сетях BTC, ETH, BSC, Polygon или операцию по покупке или продаже криптовалюты.

При расчете учитывалось количество транзакций и активных кошельков в крупнейших блокчейнах, количество активных пользователей децентрализованных приложений, предполагаемое количество активных пользователей крупных централизованных криптовалютных бирж и средневзвешенная доля российских пользователей в этих операциях. Было также учтено возможное дублирование аудитории среди областей.

По нашей оценке, приблизительно 1 миллион человек из России являются активными пользователями криптовалют с более чем одной транзакцией в месяц на блокчейне или операцией по покупке или продаже криптовалюты.

Доход иностранных криптобирж в России

Глава крупнейшей криптовалютной биржи Binance Чанпэн Чжао заявил, что по итогам 2020 года компания должна была получить прибыль в размере от $800 млн до $1 млрд. В 2021 году Binance реализовала приблизительно $3,3 млрд. чистой прибыли, из которых $195 млн. биржа заработала на операциях пользователей из России.

Binance получает прибыль от своей деятельности по всему миру и не является налоговым резидентом РФ, а платит налог на прибыль только по месту регистрации бизнеса. Если бы Binance отчисляла налоги в России, то в 2021 году бюджет РФ мог бы получить дополнительные $40 млн (3 млрд рублей) налога только от Binance (из расчета 20% налога на прибыль).

Принимая в расчет, что Binance принадлежит 23,7% объема торгов среди других криптовалютных бирж[15], можно экстраполировать полученные результаты на оставшиеся объемы, чтобы предположить общую реализованную чистую прибыль среди всех бирж. По нашей оценке, порядка $13,9 млрд. чистой выручки принесли пользователи криптовалютных бирж со всего мира в 2021 году. Учитывая средневзвешенную долю пользователей из России, криптовалютные биржи суммарно могут зарабатывать около $695 млн. чистой прибыли на операциях российских пользователей (из расчета 5% от общего количества пользователей). Таким образом, только за 2021 год бюджет России мог бы получить около $140 млн.

Количество майнеров в России

Напомним, что добыча цифровых валют или майнинг - это процесс создания новых информационных блоков криптовалюты с помощью специализированного оборудования. В процессе майнинга происходит валидация поступающей в блокчейн информации и распределение наград за проделанную работу между всеми участниками криптовалютной сети.

По результатам исследования всего крипторынка за 2021-ый год от ForkLog [32], чистая выручка всех мировых майнинговых предприятий по добыче биткоина составила $16,7млрд., а добыча Эфира принесла $23,4млрд. в 2021-ом году [33]. Следовательно, майнеры из РФ по результатам года выручили $1,84млрд. (по данным Кэмбриджского университета) и $2,57млрд. при работе с данными криптовалютами соответственно, поэтому регулирование этой сферы представляется сейчас особенно актуальным.

Главным событием майнинговой сферы в 2021-ом году стал стремительный отток добытчиков криптовалюты из Китая [34]. В результате такого изменения расстановки сил майнинговые компании и частные лица были вынуждены покинуть данную юрисдикцию и

[15]На основе данных с https://nomics.com/exchanges по состоянию на 31 марта 2022 г.

переместить операции по добыче криптовалюты в ближайшие страны с более подходящими условиями для ведения бизнеса, которыми, согласно нашим исследованиям интернет-трафика на Similarweb и аналогичных инструментах, в основном стали Россия и Казахстан.

Правительство КНР несколько лет двигалось в сторону жесткого регулирования сферы криптовалют и смежных с ними областей. В итоге в первой половине 2021-го года в Китае появилось несколько критических статей [35] по данному вопросу, после чего вышли в свет официальные заявления о принятии «определенных мер» в отношении майнинга, которые уже к концу года были полностью реализованы: все без исключения майнинговые компании на территории Китая должны были немедленно приостановить свою деятельность.

Еще за несколько месяцев до введения запретов в Китае трафик и поисковые запросы россиян по теме крупнейших майнинговых пулов Евразии и сайтов-обозревателей этих пулов начали резко набирать обороты по данным Google trends и похожих инструментов.

Подавляющее количество поисковых запросов по данной тематике в 2021-ом году приходило из Иркутской области, и к концу года эта тенденция только усилилась. Это объясняется уже имеющимися в Иркутской области необходимыми коммуникациями для развертывания бизнеса, а также привлекательными тарифами на электроэнергию, находящимися в диапазоне 3-4 руб. за 1 Квт/час.

Наш тезис о релокации бизнеса по добыче биткоина подтверждается данными исследования Statista [36], которые показывают, что по состоянию на 2020-й год Россия является страной с одним из самых низких показателей стоимости электричества в USD/kWh. Цена электричества является ключевым фактором в принятии решений о смене месте деятельности майнингового бизнеса.

Таким образом, размещение нового вычислительного оборудования в России на данный момент весьма востребовано. Это также подтверждают данные исследования Кэмбриджского университета по потреблению электроэнергии майнерами в 2021-ом году[16], в котором на Россию приходится 11.23% от майнинговых мощностей во всем мире.

На основании данных наших опросов можно предположить, что в среднем частный майнер владеет одним вычислительным устройством из верхнего модельного ряда. В таком случае расчеты показывают почти 153 тыс. майнеров, которым будет потенциально необходимо зарегистрировать свою деятельность как самозанятость или создать ИП и начать платить налоги, а также отчитываться по операциям в соответствии с 115 ФЗ.

Прибыли и убытки граждан РФ за 2021 год в сфере криптовалют

В работе с криптовалютами существует такое понятие как “он-чейн активность”. Это такой вид деятельности, при котором участники рынка взаимодействуют с распределенными базами данных (блокчейнами криптовалют) напрямую и без посредников, оставляя после себя записи обо всех совершенных действиях. Деятельность такого рода очень важно изучить, т.к. именно с нее начиналось развитие всей сферы криптовалют в целом еще до появления централизованных бирж.

По результатам анализа данных об он-чейн активности российских граждан можно сделать выводы о том, сколько получили прибыли или понесли убытков жители России за определенный период времени, сколько новых кошельков они создают, какой процент пользователей продолжает удерживать прибыльные или убыточные позиции, среднее время удержания активов и многое другое.

Для данной работы релевантны самые базовые виды взаимодействия пользователей с сетями блокчейн, которые могут стать предметом регулирования и повлекут налоговые последствия- это покупки и продажи криптовалют.

Для начала рассмотрим потенциальную извлеченную прибыль российских граждан при работе с биткоинами в прошлом году.

В соответствии с результатами исследования на основе данных аналитических лабораторий Glassnode и Cryptoquant, совокупная реализованная прибыль при прямом взаимодействия с блокчейном Bitcoin за весь 2021-ый год составила $303млрд. или $831млн. в день, из ко-

[16]Источник: https://ccaf.io/cbeci/mining_map

торых доля РФ составляет около 4%, как было обозначено ранее. Таким образом, пользователи из России суммарно достигли $12,12млрд. чистой прибыли за тот же период. Совокупный убыток за 2021-ый составил $104млрд. или $284млн. в среднем ежедневно, что соответствует $4,16млрд. понесенных российскими инвесторами убытков за тот же период. Таким образом, очевидна высокая средняя доходность при операциях с биткоином.

Настоящий анализ включает только базовые потенциально налогооблагаемые действия в сети Биткоина, но уже сейчас полученные результаты позволяют сделать однозначные выводы. При этом затруднительно провести быстрый и эффективный анализ данных, касающихся других популярных криптовалют, которые пользуются высоким спросом со стороны инвесторов из России. Работа с ними также нуждается в правовом урегулировании, контроле и защите прав инвесторов.

Рассмотренные показатели свидетельствуют об очень высокой доходности от операций с криптовалютой Биткоин. Полученные данные о числе пользователей, количестве криптовалютных кошельков в России, сумме чистых прибылей от операций российских пользователей и объеме майнинга, а также о доходе иностранных криптобирж в России дают возможность обоснованно утверждать, что российский рынок криптовалют сформирован, развивается последовательно, поддается анализу, мониторингу, регулированию и налогообложению.

МЕТОДОЛОГИЧЕСКИЕ ПОДХОДЫ К ПРОВЕДЕНИЮ ИССЛЕДОВАНИЯ

Для исследования состояния индустрии криптовалют в России использованы следующие методы анализа и связанные с ними ресурсы:

- анализ веб-трафика;
- выборочный анализ данных, содержащихся в блокчейнах, связанных с криптовалютами и цифровыми активами;
- он-чейн аналитика;
- внутренние данные компании Bitnalog;
- аналитические данные от партнеров;
- ранее проведенные исследования и опросы.

Для расчета доли России в мировом объеме криптовалютных операций были использованы данные по трафику в разных странах сервиса веб-аналитики SimilarWeb. На основе данных по посещениям российскими пользователями глобальных криптовалютных сайтов в различных категориях была вычислена средневзвешенная доля России в мировом количестве пользователей криптовалют.

Был проведен анализ веб-трафика более 100 ресурсов по тематике криптовалют в следующих категориях:

- CEX, DEX, P2P биржи и обменники;
- кошельки: веб-кошельки, десктопные, горячие;
- невзаимозаменяемые токены (NFT);
- блокчейн-игры;
- сектор децентрализованных финансов (DeFi);
- майнинг;
- трекеры и графики криптовалют;
- информационные и новостные ресурсы;
- форумы.

Для уточнения оценки учитывались внутренние данные компании, данные от партнеров, активность пользователей в различных часовых поясах, популярность валютных пар, объемы торгов, языковые параметры веб-сайта и другие данные. Также были приняты во внимание проведенные ранее исследования и отчеты на тему географии распространения криптовалют.

По нашим оценкам доля пользователей из России в глобальной криптоэкономике составляет около 4,03%, при этом для упрощения расчетов использовалось округленное значение - 4%.

Для расчета количества потенциальных майнеров на территории РФ были использованы следующие инструменты:

- открытые исторические данные изменения хэшрейта BTC;
- данные других исследований по смежным вопросам;
- открытые данные блокчейнов;
- опросы в социальных сетях;
- тематические форумы.

Формула расчета прибыли/убытков в результате он-чейн активности

Анализ он-чейн активности был произведен на основе опыта лаборатории Glassnode. При этом извлеченной прибылью в результате он-чейн деятельности целесообразно считать разницу между предыдущим и последующим перемещением актива на момент совершения такого перемещения при условии, что цена актива стала выше в момент второго перемещения. Этот метод подсчета уже прошел проверку временем и применяется при анализе такого рода данных о пользователях блокчейна BTC.

Извлеченные убытки рассматриваются как разница между предыдущим и последующим перемещением актива на момент совершения такого перемещения при условии, что цена актива стала ниже в момент второго перемещения.

Для получения данных в разрезе на каждый день 2021-ого года была использована 365 Moving median для всех метрик.

ЗАКЛЮЧЕНИЕ

Анализ показателей развития криптоиндустрии с применением описанных выше методологических подходов позволил рассчитать долю России в мировом объеме криптовалютного рынка. Полученные результаты свидетельствуют о высоком потенциале и значимости для российской экономики как криптовалют, так и технологий, лежащих в их основе и применимых в рамках обеспечения цифровой трансформации и цифровизации страны. Кроме того, результаты подтверждают тезис о необходимости регулирования криптовалют и закрепления их в российском законодательстве.

Феномен криптовалют все еще недостаточно изучен, что можно объяснить их децентрализованным характером, накладывающим определенные ограничения на исследования. Среди них – сложности в установлении принадлежности криптовалютных адресов к определенным странам и точной суммы, отправленной и полученной в сети по адресам в конкретной стране. Многие данные закрыты для доступа или предоставляются только институциональным инвесторам, а некоторые методы исследования еще не прошли проверку временем.

В целом положительная динамика показателей индустрии криптовалют, развитие технологий в сторону метавселенных и децентрализованных финансов, а также изменение состава субъектов инвестирования (рост инвестиций со стороны институциональных инвесторов) свидетельствуют о том, что индустрия достаточно успешно и стремительно развивается при отсутствии государственного регулирования. Дальнейшая легализация криптовалют может обеспечить прозрачный процесс оборота криптовалют на территории РФ, и, в конечном счете, создать новый источник налогов на доход с криптовалютных операций.

СПИСОК ЛИТЕРАТУРЫ

1. Мачихин Д.С. Современные подходы к налогообложению криптовалюты // Вестник современных цифровых технологий. 2021. №. 8. С. 23-29.

2. Криптовалюта в России: законодательное недорегулирование. URL: https://www.garant.ru/news/1448450/ (Дата обращения: 21.04.2022)

3. Рязанова А.А., Черкашин П.А., Щербаков А.Ю. Современные тенденции и актуальные вопросы развития институциональных основ технологий распределенных реестров и цифровых финансовых активов // Вестник современных цифровых технологий. 2021. №. 9. С. 19-25.

4. Агеев В. Н., Власов А. В. Потенциал применения цифровых финансовых активов // Финансовый журнал. 2020. Т. 12. № 6. С. 100–112. DOI: 10.31107/2075-1990-2020-6-100-112.

5. Перечень поручений по итогам совещания по вопросу использования цифровых технологий в финансовой сфере. URL: http://www.kremlin.ru/acts/assignments/orders/55899 (Дата обращения:

29.04.2022)
6. Мы хотели быть ледоколом, который ломает лед между регулятором и индустрией»: как ЦБ тестировал криптопроекты и что из этого вышло. URL: https://www.forbes.ru/finansy-i-investicii/430777-my-hoteli-byt-ledokolom-kotoryy-lomaet-led-mezhdu-regulyatorom-i (Дата обращения: 29.04.2022)
7. Криптовалюты: тренды, риски, меры. Доклад для общественных консультаций. URL: https://cbr.ru/Content/Document/File/132241/Consultation_Paper_20012022.pdf (Дата обращения: 27.04.2022)
8. Мачихин Д.С. О подходах к регулированию индустрии криптовалют в России // Вестник современных цифровых технологий. 2021. №. 10. С. 11-18.
9. Публичные компании, которые инвестируют в криптовалюту: топ-11. URL: https://ru.beincrypto.com/learn/publichnye-kompanii-kotorye-investiruyut-v-kriptovalyutu/ (Дата обращения: 27.04.2022)
10. Bitcoin Holdings by Public Companies. URL: https://www.coingecko.com/en/public-companies-bitcoin (Дата обращения: 29.03.2022)
11. BlackRock Planning to Offer Crypto Trading, Sources Say. URL: https://www.coindesk.com/business/2022/02/09/blackrock-planning-to-offer-crypto-trading-sources-say/ (Дата обращения: 27.04.2022)
12. BlackRock Now Manages Over $10 Trillion in Assets. URL: https://www.wsj.com/articles/blackrock-now-manages-over-10-trillion-in-assets-11642162013 (Дата обращения: 29.04.2022)
13. Beeple's opus. URL: https://www.christies.com/features/Monumental-collage-by-Beeple-is-first-purely-digital-artwork-NFT-to-come-to-auction-11510-7.aspx (Дата обращения: 21.04.2022)
14. Created over 5,000 days by the groundbreaking artist, this monumental collage was the first purely digital artwork (NFT) ever offered at Christie's https://www.christies.com/features/Monumental-collage-by-Beeple-is-first-purely-digital-artwork-NFT-to-come-to-auction-11510-7.aspx (Дата обращения: 29.04.2022)
15. Что такое NFT и почему они приносят миллионы. URL: https://trends.rbc.ru/trends/industry/604f3f139a794797b44b7a70 (Дата обращения: 29.04.2022)
16. The Block Research. https://www.tbstat.com/wp/uploads/2021/12/The-Block-Research-2022-Digital-Asset-Outlook.v2.pdf (Дата обращения: 29.04.2022)
17. Five Crypto Trends To Watch in 2022. URL: https://blog.coinlist.co/five-crypto-trends-to-watch-in-2022/ (Дата обращения: 29.04.2022)
18. Ubisoft Reports First-Half 2021-22 Earnings Figures https://staticctf.akamaized.net/8aefmxkxpxwl/667U3sKCZltRVFBUMN0jM8/c9dbc2fd1ddbf14c9def4cfb5fe90fd2/Ubisoft_FY22_H1_Earnings_PR_English.pdf (Дата обращения: 21.04.2022)
19. Global Frontier Report. URL: https://games.withgoogle.com/reports/#section_blue-island (Дата обращения: 29.04.2022)
20. Facebook's CEO on why the social network is becoming 'a metaverse company. URL: https://www.theverge.com/22588022/mark-zuckerberg-facebook-ceo-metaverse-interview (Дата обращения: 29.04.2022)
21. Announcing a $1 Billion Funding Round to Support Epic's Long-Term Vision for the Metaverse. URL: https://www.epicgames.com/site/en-US/news/announcing-a-1-billion-funding-round-to-support-epics-long-term-vision-for-the-metaverse (Дата обращения: 29.04.2022)
22. Converging the physical and digital with digital twins, mixed reality, and metaverse apps. URL: https://azure.microsoft.com/en-us/blog/converging-the-physical-and-digital-with-digital-twins-mixed-reality-and-metaverse-apps/ (Дата обращения: 21.04.2022)
23. Sales of Virtual Real Estate Reached $500 Million in 2021 and Are Expected to Double in 2022. URL: https://www.investing.com/news/cryptocurrency-news/sales-of-virtual-real-estate-reached-500-million-in-2021-and-are-expected-to-double-in-2022-2755919 (Дата обращения: 21.04.2022)
24. Sotheby's Opens Virtual Replica of Its London Galleries in Decentraland. URL:

https://www.coindesk.com/markets/2021/06/04/sothebys-opens-virtual-replica-of-its-london-galleries-in-decentraland/ (Дата обращения: 21.04.2022)

25. There's a Portrait of Jamie Dimon Hanging in JPMorgan's Metaverse Lounge. URL:
https://www.bloomberg.com/news/articles/2022-02-15/dimon-s-portrait-roaming-tiger-jpmorgan-opens-metaverse-lounge?sref=i4qXzk6d (Дата обращения: 21.04.2022)

26. In a world first, El Salvador makes bitcoin legal tender. URL:
https://www.reuters.com/world/americas/el-salvador-approves-first-law-bitcoin-legal-tender-2021-06-09 (Дата обращения: 21.04.2022)

27. Федеральный закон от 31.07.2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации». URL: http://www.kremlin.ru/acts/bank/45766 (Дата обращения: 21.04.2022)

28. В Минфине считают, что его концепция по криптовалютам отвечает на все вопросы ЦБ. URL: https://www.interfax.ru/business/821905 (Дата обращения: 21.04.2022)

29. В Минфине ждут решения по криптовалютам в течение месяца
https://www.interfax.ru/business/819516 (Дата обращения: 21.04.2022)

30. Crypto Market Sizing. URL: https://assets.ctfassets.net/hfgyig42jimx/5i8TeN1QYJDjn82pSuZB5S/85c7c9393f3ee67e456ec780f9bf11e3/Cryptodotcom_Crypto_Market_Sizing_Jan2022.pdf (Дата обращения: 21.04.2022)

31. Cryptocurrency across the world. URL: https://triple-a.io/crypto-ownership/ (Дата обращения: 21.04.2022)

32. Большое исследование рынка криптовалют за 2021-ый год от Forklog. URL:
https://forklog.com/2021-god-v-tsifrah-rekordy-bitkoina-bum-nft-gamefi-i-rastsvet-l2-reshenij-dlya-ethereum/ (Дата обращения: 21.04.2022)

33. Отчет: за 2021 год биткоин-майнеры заработали $16,7 млрд. URL: https://forklog.com/otchet-za-2021-god-bitkoin-majnery-zarabotali-16-7-mlrd/ (Дата обращения: 21.04.2022)

34. Китайский запрет майнинга. URL: https://forklog.com/majning-bitkoina-v-2021-godu-kitajskij-zapret-izmenil-rasstanovku-sil/ (Дата обращения: 21.04.2022)

35. Биткоин упал ниже $37 000 на фоне новостей о запрете майнинга в Китае. URL:
https://cryptofans.ru/news/novosti_majninga/bitkoin_upal_nizhe_37_000_na_fone_novostej_o_zaprete_majninga_v_kitae.html (Дата обращения: 21.04.2022)

36. Household electricity prices worldwide in december 2020, by select country. URL:
https://www.statista.com/statistics/263492/electricity-prices-in-selected-countries/ (Дата обращения: 21.04.2022)

УДК: 004.056

О подходах к обеспечению информационной безопасности цифровых двойников

D.S. Lazorin, D.I. Pravikov, A.Yu. Shcherbakov

On Approaches to the Ensuring Information Security of Digital Twins

Abstract. *The article is devoted to the consideration of existing approaches to ensuring the information security of digital twins and the formulation of proposals for the choice of means to counter various threats, primarily the threat of distortion of the digital twin. It is shown that none of the existing approaches and methods provides the full security of digital twins. The implementation of an integrated approach to ensure the security of digital twins within the framework of specific threat and intruder models that are relevant to them is proposed.*

Keywords: *digital twin, digitalization, information security, threat and intruder model, computer model, multi-level system, digital certificate, data encryption, cryptographic algorithms, machine learning, tokenization.*

Д.С. Лазорин[1]
Д.И. Правиков[2]
А.Ю. Щербаков[3]
[1]Студент РГУ нефти и газа (НИУ) имени И.М. Губкина.
E-mail: lazorindanya@yandex.ru
[2]Кандидат технических наук, заведующий кафедрой комплексной безопасности критически важных объектов, РГУ нефти и газа (НИУ) имени И.М. Губкина.
E-mail: d_pravikov@mail.ru
[3]Доктор технических наук, профессор кафедры комплексной безопасности критически важных объектов РГУ нефти и газа (НИУ) имени И.М. Губкина, ведущий научный сотрудник Государственного университета управления.
E-mail: x509@ras.ru

Аннотация. *Статья посвящена рассмотрению существующих подходов к обеспечению информационной безопасности цифровых двойников и формулированию предложений по выбору средств противодействия различным угрозам, прежде всего угрозе искажения цифрового двойника. Показано, что ни один из существующих подходов и методов не обеспечивает полноценной безопасности цифровых двойников. Предложена реализация комплексного подхода для обеспечения безопасности цифровых двойников в рамках актуальных для них специфических моделей угроз и нарушителя.*

Ключевые слова: *цифровой двойник, цифровизация, информационная безопасность, модель угроз и нарушителя, компьютерная модель, многоуровневая система, цифровой сертификат, шифрование данных, криптографические алгоритмы, машинное обучение, токенизация.*

ВВЕДЕНИЕ

Понятие «цифровой двойник» в настоящее время прочно заняло позиции в современных цифровых технологиях. Данный термин достаточно широк и в первом приближении описывает математическую или компьютерную имитационную модель, связанную с физическим объектом потоками передачи информации, которая может быть отчуждена или отделена от исходного объекта в целях воспроизведения его функционирования или выполнения действий с указанным объектом.

Термин «цифровой» подразумевает под собой набор алгоритмов, которые описывают сам объект и протекающие в нём процессы. Цифровой двойник связан с процессами цифровизации - внедрения в определенные области деятельности и компетенции компаний современных информационных технологий, которые позволяют реформировать её деятельность. Цифровизация является основой современного подхода в том числе и к развитию промышленности, который позволил переосмыслить многие действующие бизнес-процессы корпораций [1].

Программные компоненты систем и физические процессы взаимосвязаны. Цифровой двойник выступает в роли объединяющей цепочки между «настоящим» миром и цифровой реальностью. Например, для того чтобы на предприятии эта цепочка находилось в рабочем состоянии, необходимо непрерывно получать информацию от технологического оборудования. Этим процессам помогают датчики

и сенсоры физического объекта, конструкции или технологической системы. Применение цифрового двойника необходимо для анализа и обновления в реальном времени большого количества данных, получаемых от физического объекта и требующих значительных вычислительных мощностей для их обработки, а также для моделирования и расчёта того, как будет вести себя та или иная конструкция или установка [2].

Актуальность цифровых двойников сегодня общепризнана. Об этом свидетельствуют, в частности, документы Министерства Энергетики [3].

Одной из наиболее острых является проблема информационной безопасности цифровых двойников. Вместе с имитацией процессов объектов физического мира при помощи данной технологии появляется возможность их контролировать, следовательно, не допускать наступления негативных событий. Приоритетной задачей становится обеспечение информационной безопасности организаций и технологических процессов, использующих технологию цифровых двойников.

Специфика обеспечения информационной безопасности в условиях применения технологий цифровых двойников связана с необходимостью применения имитационного моделирования, основанного на использовании характеристик каждого элемента системы и разработке логической цепочки процессов на базе реального объекта.

Также одной из актуальных проблем безопасности цифрового двойника является целенаправленное внесение искажений нарушителем таким образом, что управление объектом становится не оптимальным или невозможным.

ЭЛЕМЕНТЫ СИСТЕМЫ «ФИЗИЧЕСКИЙ ОБЪЕКТ – ЦИФРОВОЙ ДВОЙНИК» (ФОЦД)

Рассмотрим основные компоненты системной целостности, включающей физический объект и виртуальный объект.

1. Физический объект (ФО).
2. Виртуальный объект или специальная модель, соответствующая физическому объекту (цифровой двойник, ЦД).
3. Взаимосвязи в системе, включающей виртуальный объект и физический объект.

Собственно цифровым двойником в этой целостности является второй компонент, который может иметь связи с физическим объектом для его мониторинга и управления (третий компонент системной целостности).

Для объединения в ФОЦД вышеперечисленных частей используются различные, как принято говорить в современной информатике, интеграции, обеспечивающие получение реальных данных от модели ФО, которая может строиться на основе технологий «Интернет вещей» (Internet of Things, сокращённо IoT), а также различных математических моделях. К ним могут относиться, например, CAE-системы (Computer-aided engineering. автоматизированное проектирование), предназначенные для решения инженерных задач [4].

Стоит отметить, что вопрос обеспечения информационной безопасности ЦД конструктивно решается в том случае, если учитываются следующие априорные требования: контроль получаемых от ФО параметров, обеспечение целостности и конфиденциальности при обмене данными, обеспечение доступности и, самое главное, соответствие модели реальному объекту.

Кроме того, в одной из «проекций» цифровой двойник — это симбиоз технологий PLM (Product Lifecycle Management — управление жизненным циклом программных продуктов) и IIoT (Industrial Internet of Things, промышленный интернет вещей). Непосредственно на данный объект могут возникать несанкционированные воздействия, которые тем или иным способом могут повлиять на работу цифрового двойника и привести, как минимум, к неоптимальной его работе или же отказу всей системы, в которой он применяется.

СПЕЦИФИЧЕСКИЕ СВОЙСТВА ЦИФРОВЫХ ДВОЙНИКОВ

С точки зрения системного анализа необходимо выявить специфические свойства и об-

щие требования, которые можно предъявить к ФОЦД.

В первую очередь, это целостность, понимаемая как неразрывная взаимосвязь всех трех компонентов, их актуальность (в смысле соответствия текущему состоянию параметрам), наличие исчерпывающих связей между элементами системной целостности ФОЦД и их полнота.

В этом смысле весьма конструктивным представляется подход к описанию ФОЦД как некоторой платформы или ее части, данный подход будет проанализирован ниже.

С точки зрения реализации угроз ЦД может не соответствовать ФО, который управляется или мониторируется с его помощью.

Проверка соответствия ЦД ФО может проводиться через оценку качества управления. Цифровой двойник должен представлять собой адекватную модель существующего физического продукта или целостного процесса.

При необходимости можно зафиксировать и другие требования: актуальность цифрового двойника, защита канала связи двойника и объекта и т.д.

ОТЛИЧИЕ СТАНДАРТНОЙ МАТЕМАТИЧЕСКОЙ МОДЕЛИ И ЦИФРОВОГО ДВОЙНИКА

Попробуем прояснить весьма важный вопрос, касающийся различия общепринятой математической модели и ЦД.

Математическая модель — комплекс аналитических или вероятностных зависимостей параметров ФО, благодаря которым можно отразить характеристики рассматриваемого объекта или явления, построенных на основе физической модели и взаимодействиях её с окружающей средой. Она необходима для прогнозирования поведения реального объекта, однако всегда демонстрирует различную степень его идеализации.

Модель цифрового двойника — объект, который можно представить в виде физической и виртуальной системы, которая в свою очередь также включает стандартную математическую модель, так что виртуальная система отображает физическую, и наоборот.

Ключевое отличие от математической модели состоит в том, что модель цифрового двойника основывается не на идеализации, а на реальном поведении самого объекта.

ОПИСАНИЕ ОСНОВНЫХ ПОДХОДОВ К БЕЗОПАСНОСТИ ЦИФРОВЫХ ДВОЙНИКОВ

Ниже проанализированы актуальные источники и определены основные подходы и методы обеспечения информационной безопасности, которые могут быть применены к технологии цифровых двойников. Для каждого из них проведено краткое описание, изложена конструктивная критика данных подходов и методов.

Блокчейн-структура

В цифровом двойнике в процессе непрерывного обмена данными отражаются все стадии жизненного цикла физического объекта. Технологии распределенных реестров и, в частности, блокчейн позволяют фиксировать в режиме реального времени и в неизменяемом виде все состояния физического объекта и действия над ним, что является одним из основных условий обеспечения прозрачности, отслеживаемости, целостности и неизменности данных [5]. Блокчейн позволяет обмениваться событиями и уведомлениями, которые хранятся в защищенном виде. В целом интеграция с технологией блокчейн обеспечивает безопасное, эффективное, децентрализованное и надежное хранение данных виртуальных моделей [6, 7, 8].

Использование данной технологии позволяет противодействовать угрозе изменения созданных записей, однако недостаточно для обеспечения комплексной безопасности цифровых двойников. В частности, блокчейн-структура не защищает от ложных команд управления и не обеспечивает защиту канала связи ФО и ЦД.

Подход к организации информационного взаимодействия в многоуровневой системе

Единицей межуровневого информационного обмена выступает программная структура особого типа — пакет, построенный по принципу организации сообщений в HTTP(s)-протоколах. Непосредственно метаданные (средства классификации, упорядочивания и характери-

стики данных) источника размещаются в заголовке пакета и позволяют выполнять распознавание соответствующих ресурсов по мере поступления данных. Данные цифрового двойника или его физического прототипа размещаются в теле пакета. Использование в заголовке пакета блока метаданных должно быть компактным и доступным для анализа программными средствами обработки данных.

Токен — специальный ключ, идентифицирующий поступающий запрос. Существует подход к кодированию заголовка с метаданными на основе комбинирования форматов DTDL (Digital Twins Definition Language — язык определения цифровых двойников), предназначенного для семантического описания промышленных цифровых двойников, и JWT (JSON Web Token), обеспечивающего процедуру поддержания сеанса связи между клиентом и сервером в веб-ориентированной архитектуре приложений. Непосредственно метаданные задаются в формате DTDL, а их размещение в заголовке пакета представляет собой программную «свертку» данных в формате токена JWT, заменяющего громоздкое JSON-описание источника данных легковесным текстовым кодом [9].

Согласно открытому стандарту RFC7519 (стандарт для создания токенов доступа, основанный на формате JSON), JWT представляет собой безопасный способ передачи данных между парой участников информационного взаимодействия [10-12].

Данный подход предпочтителен тем, что в его основе лежит обеспечение безопасности в системе взаимодействия между программным продуктом или приложением и сервером, но не затрагиваются другие внутрисистемные процессы цифровых двойников, на которые могут быть направлены потенциальные атаки и взломы.

Система иерархической токенизации элементов системы

Токенизация в одном из определений — процесс замены конфиденциальной информации на равнозначные не конфиденциальные данные с использованием специальных значений (токенов). Для повышения эффективности процессов обмена, обработки данных и безопасности между уровнями системы цифровых двойников предлагается подход, основанный на принципе токенизации информационных ресурсов. Данная технология активно используется для защиты и шифрования в современных системах информационной безопасности, а также для реализации систем блокчейн.

Использование токенизации для разметки источников данных и их физических прототипов, а также результатов их агрегирования на основании пространственной кластеризации (процедуре сбора данных) по заданным признакам обеспечивает безопасность использования цифровых двойников. В соответствии с предлагаемой концепцией информационного взаимодействия элементов системы предполагается маркировка соответствующих наборов данных для идентификации их источника в процессе обработки и анализа данных в составе единого информационного пространства. Так как идентификация является одним из основополагающих факторов обеспечения информационной безопасности, это позволит избежать изменения данных, исходящих от внесистемных источников [13, 14].

Данный метод обеспечивает неизменность данных и идентификацию поступающих к цифровому двойнику запросов, однако не позволяет осуществлять комплексную защиту от угроз, направленных на цифровой двойник, как и технология блокчейн (см.выше).

Digital ID или цифровой сертификат

Эта технология представляет собой относительно новый подход к безопасности и доверию, в рамках которого идентифицируются запросы от верифицированных источников, например, внутрисистемные запросы для управления продуктом, в которых используется цифровой двойник. Благодаря цифровому сертификату можно защититься от более широкого круга действий нарушителя.

Программные приложения, сети и компьютеры могут использовать Digital ID в шифровании, как путь защиты информации перед отправкой его с одной компьютерной системы на другую [15].

Этот метод обеспечивает проверку поступающих запросов, но не рассматривает другие возможные способы нарушения работы цифровых двойников, например, замену посторон-

него ID на истинный.

Методика многоуровневого шифрования команд для управления удалёнными компьютерными системами

Процесс криптографических преобразований сообщений на конечных клиентских устройствах и их передача через сервер в зашифрованном виде называется сквозным шифрованием [16]. На сегодняшний день такой подход к защите данных является одним из наиболее эффективных и приобретает всё большее распространение. Однако применение сквозного шифрования не исключает необходимости защиты данных, которыми обмениваются компоненты информационной системы с сервером, так как часть из них предназначены непосредственно самому серверу, а значит, не могут быть подвергнуты сквозному шифрованию [17]. Это касается команд для администрирования сервера и страниц с информацией о текущем состоянии процесса мониторинга.

Для всех перечисленных данных необходимо применять транспортное шифрование, то есть шифрование, выполняемое только при передаче через интернет, при котором данные расшифровываются каждым компонентом информационной системы, а при необходимости дальнейшей передачи зашифровываются заново. Таким образом, для обеспечения безопасной передачи данных в системе удалённого мониторинга и управления компьютерами должно быть реализовано многоуровневое шифрование, объединяющее в себе сквозное симметричное шифрование команд между управляющим компьютером и компьютерами пользователей и транспортное шифрование между сервером и управляющим компьютером, а также сервером и компьютерами пользователей.

Безопасность сквозного шифрования основана на том, что ключи для шифрования и расшифрования сообщений доступны только непосредственным участникам взаимодействия. При этом главная проблема реализации сквозного шифрования заключается в безопасной передаче ключей от отправителя к получателю. Для обмена ключами используется один из распространённых видов алгоритмов: симметричный или асимметричный, а также, в некоторых случаях, дополнительно используется разделение секрета или иные протоколы, позволяющие разделить ключи.

Использование асимметричных криптографических алгоритмов в сквозном шифровании порождает несколько дополнительных проблем, таких как аутентификация ключей, проверка личности отправителя, управление цифровыми сертификатами и их подтверждением. Асимметричное шифрование в первую очередь направлено на использование участниками взаимодействия через Интернет, когда нет никаких возможностей отдельной передачи симметричных ключей.

Преимуществом такого метода является следующее: если в системе таких ограничений нет, то все её компоненты находятся под единым административным управлением, разрабатываются и конфигурируются централизованно, к тому же администратор в любой момент имеет доступ к каждому компьютеру, на котором установлено клиентское программное обеспечение. В связи с этим при разработке системы удалённого управления компьютерами целесообразно применение симметричных алгоритмов с использованием предварительного общего ключа PSK (Pre-Shared Key — предварительно опубликованный ключ для шифрования данных перед отправкой, который разделён между двумя сторонами системы взаимодействия).

Использование удалённого управления и мониторинга оборудования в этом случае значительно упростит работу администратора и снизит расходы на поддержание работы информационной системы, а описанные методы защиты не приведут к появлению дополнительных уязвимостей и позволят избежать снижения уровня информационной безопасности цифровых двойников.

В данной методике рассматривается взаимодействие через сеть Интернет, но не предоставляются различные варианты безопасной работы систем при ситуациях, когда доступ к сети может быть нарушен, либо же специально ограничен.

Комплексный подход с использованием машинного обучения и искусственного интеллекта

Существуют решения на основе искусственного интеллекта, способные обнаружить отклонения в технологическом процессе на ранней стадии. Принцип защиты системы основан на выстраивании модели таким образом, чтобы она была готова к попытке «скормить» ей искаженную информацию и могла справиться с атакой. Использование машинного обучения позволит исправлять возникающие искажения, которые обнаруживает искусственный интеллект.

Стоит отметить, что для цифровых двойников, базирующихся на машинном обучении (Machine Learning), основную опасность несут враждебные атаки (Adversarial attacks), основанные на внесении минимальных изменений в данные, которые поступают в цифровую модель. Применительно к заводам и фабрикам это могут быть показания датчиков, интегрированных в производственное оборудование. Изменения, как правило, заключаются в добавлении данных, которые подбираются таким образом, чтобы максимально исказить предсказания, которые формирует модель.

Подобная атака может привести к простоям оборудования, лишним расходам на сырье и другим незапланированным издержкам, которые плохо сказываются на экономической политике предприятия. Следовательно, данный метод привлекает нарушителя возможностью «скармливания искажённой информации».

Использование таких решений на сегодняшний день возможно в качестве дополнительных, потому что они требуют определенного количества времени для обучения работе в самой системе.

Обеспечение безопасности ЦД в рамках концепции многоуровневой платформы

Многоуровневая система (платформа) имеет различные уровни организации, в которых происходят определенные процессы. Верхние уровни обеспечивают бизнес-взаимодействия, а нижние уровни поддерживают информационную безопасность самой платформы. Авторами данного подхода вводится понятие «стек технологий», в котором работа верхних уровней поддерживается нижними уровнями, и предлагается использование интеграционной модели защищенной цифровой платформы, включающей вертикальное разделение по уровням абстракций представления данных и уровням обеспечения информационной безопасности [18].

На основе проанализированных подходов к безопасности цифровых двойников построена таблица 1 «Некоторые способы обеспечения комплексной безопасности цифровых двойников».

Таблица 1

Некоторые способы обеспечения комплексной безопасности цифровых двойников

Информационное взаимодействие в многоуровневой системе	✓
Проверка подлинности поступаемых запросов к модели	✓
Шифрование данных при передаче по каналам связи	✓
Решения на основе машинного обучения и искусственного интеллекта	✓
Соответствие модели реальному объекту	**X**

ЗАКЛЮЧЕНИЕ

Проведенный анализ существующих подходов к обеспечению информационной безопасности цифровых двойников позволяет сделать вывод, что практически ни один из предложенных способов в отдельности не обеспечивает комплексной безопасности в рамках актуальных для цифровых двойников моделей угроз и нарушителя. Использование технологий распределенных реестров, метода иерархической токенизации, цифровых сертификатов, многоуровневого шифрования, машинного обучения и искусственного интеллекта на современном уровне весьма оправдано, но направлено на решение частных задач.

В связи с этим целесообразно развивать методологию обеспечения информационной безопасности цифровых двойников в соответствии с концепцией многоуровневой платформы, поскольку в понятие платформы уже включен комплексный подход и иерархия решений от низкоуровневых способов защиты канала связи ФОЦД при помощи криптографических алгоритмов до высокуровневых задач, связанных с проверкой соответствия моделей функционирования ЦД и обеспечения корректности бизнес-процессов, отражаемых цифровым двойником.

При этом отдельные способы обеспечения информационной безопасности могут включать уже готовые решения (например, средства шифрования данных при передаче по каналам связи), а для части методов (направленных, например, на обеспечение соответствия виртуальной модели реальному объекту) необходимо использовать другие средства и подходы, которые будут сформулированы в следующих работах.

СПИСОК ЛИТЕРАТУРЫ

1. Намиот Д. Е., Покусаев О. Н., Куприяновский В. П., Жабицкий М. Г. Цифровые двойники и системы дискретно-событийного моделирования // International Journal of Open Information Technologies. 2021. №9. С. 70-75.

2. Цифровое зеркало. URL: https://www.gazprom-neft.ru/press-center/sibneft-online/archive/2018-september-projects/1863687/ (Дата обращения: 12.01.2022)

3. Паспорт: «Программы инновационного развития» ПАО «Газпром» до 2025 года. URL: https://in.minenergo.gov.ru/knowledge-base/programmy-razvitiya/programmy-innovatsionnogo-razvitiya/pasport-programmy-innovatsionnogo-razvitiya-pao-gazprom-do-2025-goda (Дата обращения: 13.01.2022)

4. Перспективы использования цифровых двойников на производстве и технологии для их создания. URL: https://controleng.ru/innovatsii/cifrovye-dvojniki/chto/ (Дата обращения: 27.02.2022)

5. Дроговоз П.А., Кошкин М.В. Проекты внедрения технологий блокчейн и интернета вещей в трансграничных цепочках поставок // Управление научно-техническими проектами: сб. материалов III междунар. науч.-техн. конференции. М.: Изд-во МГТУ им. Н.Э. Баумана, 2019. С. 153–156.

6. Гарина И. О. Методический подход к разработке блокчейн-структуры цифрового двойника изделия в машиностроении // Современные наукоемкие технологии. 2020. № 11-1. – С. 15-20. – DOI 10.17513/snt.38331.

7. Mandolla C., Petruzzelli A.M., Percoco G., Urbinati A. Building a digital twin for additive manufacturing through the exploitation of blockchain. Comput. Ind. 2019. Vol. 109. P. 134–152.

8. Freni P., Ferro E., Moncada R. Tokenization and Blockchain Tokens Classification: a morphological framework // IEEE Symposium on Computers and Communications (ISCC), Rennes, France, 2020. P. 1-6, DOI: 10.1109/ISCC50000.2020.9219709.

9. Воробьев А. В. Концепция информационного пакетного взаимодействия в многоуровневой системе цифровых двойников // Известия Саратовского университета. Новая серия. Серия: Математика. Механика. Информатика. 2021. Т. 21, вып. 4. С. 532-543. DOI: 10.18500/1816-9791-2021-21-4-532-

543.
10. Janoky L., Levendovszky J., Ekler P. An analysis on the revoking mechanisms for JSON Web Tokens // International Journal of Distributed Sensor Networks. 2018. Vol. 14, iss. 9. P. 1–10. https://doi.org/10.1177/2F1550147718801535
11. Aldya A. P., Rahmatullo A., Arifin M. N. Stateless Authentication with JSON Web Tokens using RSA-512 Algorithm // Journal INFOTEL. 2019. Vol. 11, № 2. P. 36–42. https://doi.org/10.20895/infotel.v11i2.427
12. Rahmatulloh A., Gunawan R., Nursuwars F. Performance comparison of signed algorithms on JSON Web Token // IOP Conference Series: Materials Science and Engineering. 2019. Vol. 550. P. 012023. https://doi.org/10.1088/1757-899X/550/1/012023
13. Marchewka-Bartkowiak K., Nowak K. Get Tokenized... The Specificity of Personal Tokens in the Context of Tokenization and Axiological Categorization // Proceedings of the 3rd International Conference on Economics and Social Sciences. 2020. P. 823-831. DOI:10.2478/9788395815072-081.
14. Cassimon T., de Hoog J., Anwar A., Mercelis S., Hellinckx P. Intelligent data sharing in digital twins: Positioning paper. In: L. Barolli, M. Takizawa, T. Yoshihisa, F. Amato, M. Ikeda, eds. Advances on P2P, Parallel, Grid, Cloud and Internet Computing. 3PGCIC 2020 (Lecture Notes in Networks and Systems, vol. 158). Springer, Cham, 2021, P. 282– 290. https://doi.org/10.1007/978-3-030-61105-7_28
15. Tang S., Wei G. ID-based digital Multisignature scheme // Journal of Circuits, Systems, and Computers. 1999. Vol. 9. No 3-4. P. 223-227. – DOI 10.1142/S0218126699000189.
16. Бытый Д.Э. Методика многоуровневого шифрования команд для системы управления удалёнными компьютерами // Наукосфера. 2021. № 10-1. С. 92-95.
17. Лапонина О.Р. Основы сетевой безопасности : учеб. Пособие / Национальный Открытый Университет «ИНТУИТ». Москва, 2014, 374 с.
18. Правиков Д.И., Глейм А.В., Егоров В.И., Рязанова А.А., Щербаков А.Ю. К вопросу о формулировании системного подхода к исследованиям в области цифровых платформ, распределенных реестров и цифровых активов // Вестник современных цифровых технологий. 2021. № 9. С. 5-14.

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.