

**МЕЖДУНАРОДНЫЙ ЦЕНТР НАУЧНОГО СОТРУДНИЧЕСТВА
«НАУКА И ПРОСВЕЩЕНИЕ»**



НОВЫЕ НАУЧНЫЕ ИССЛЕДОВАНИЯ И ТЕХНОЛОГИИ:

АКТУАЛЬНЫЕ ВОПРОСЫ, ДОСТИЖЕНИЯ И ИННОВАЦИИ:

МОНОГРАФИЯ

**ПЕНЗА
МЦНС «НАУКА И ПРОСВЕЩЕНИЕ»
2024**

УДК 001.1
ББК 60
Н76

Рецензенты:

Бабанова Юлия Владимировна – доктор экономических наук, доцент, заведующий кафедрой «Управление инновациями в бизнесе» Высшей школы экономики и управления ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)»

Колесников Геннадий Николаевич – доктор технических наук, профессор, заведующий кафедрой ФГБОУ ВО «Петрозаводский государственный университет»

Кунц Елена Владимировна – доктор юридических наук, профессор, зав. кафедрой уголовного права и криминологии ФГБОУ ВО «Челябинский государственный университет»

Авторский коллектив

Азарян Е.М., Аменицкая Л.А., Аменицкий А.В., Аменицкий Д.А., Блиничкина Н.Ю., Бузни А.Н., Воликов В.В., Гаврилов В.А., Грабков Ю.П., Дерябин Н.И., Зайналов Ж.Р., Кудрявцева Н.А., Матевосова Е.К., Маторина О.С., Рухович И.В., Тарасов А.В., Удавцова Е.Ю., Халаимова В.И., Хачатурян Э.В., Четкин А.В.

Н76

НОВЫЕ НАУЧНЫЕ ИССЛЕДОВАНИЯ И ТЕХНОЛОГИИ: АКТУАЛЬНЫЕ ВОПРОСЫ, ДОСТИЖЕНИЯ И ИННОВАЦИИ: монография / Под общ. ред. Г. Ю. Гуляева — Пенза: МЦНС «Наука и Просвещение». — 2024. — 208 с.

ISBN 978-5-00236-641-5

В монографии представлены теоретические подходы и концепции, аналитические обзоры, практические решения в конкретных сферах науки и общества.

Издание может быть интересно российским и зарубежным ученым, руководителям и служащим государственного аппарата, руководителям и специалистам учреждений и хозяйственных организаций, педагогам, аспирантам и студентам высших учебных заведений.

Ответственность за аутентичность и точность цитат, имен, названий и иных сведений, а также за соблюдение законодательства об интеллектуальной собственности несут авторы публикуемых материалов.

УДК 001.1
ББК 60

© МЦНС «Наука и Просвещение» (ИП Гуляев Г. Ю.), 2024
© Коллектив авторов, 2024

ISBN 978-5-00236-641-5

ОГЛАВЛЕНИЕ

| | |
|---|-----|
| РАЗДЕЛ I. АКТУАЛЬНЫЕ ВОПРОСЫ СОЦИАЛЬНО-ЭКОНОМИЧЕСКОГО РАЗВИТИЯ | 5 |
| ГЛАВА 1. РАЗВИТИЕ ПРАВОВОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ МИРОПОРЯДКА..... | 6 |
| ГЛАВА 2. КРИПТОВОЛЮТА КАК ПРЕДМЕТ МОШЕННИЧЕСТВА | 17 |
| ГЛАВА 3. СТРАТЕГИЧЕСКИЙ АСПЕКТ РАЗВИТИЯ УГОЛОВНОГО РОССИЙСКОГО ЗАКОНОДАТЕЛЬСТВА В ОБЛАСТИ ОХРАНЫ ЗДОРОВЬЯ | 28 |
| ГЛАВА 4. ПРОБЛЕМЫ ЭФФЕКТИВНОСТИ УПРАВЛЕНИЯ ФИНАНСОВОЙ СИСТЕМОЙ В УСЛОВИЯХ ИННОВАЦИОННОГО РАЗВИТИЯ ЭКОНОМИКИ | 40 |
| ГЛАВА 5. ПЕРСПЕКТИВЫ РАЗВИТИЯ ЕВРАЗИЙСКОЙ ИНТЕГРАЦИИ В КОНТЕКСТЕ ВСТУПЛЕНИЯ ТАДЖИКИСТАНА В ЕАЭС | 53 |
| ГЛАВА 6. КРЕАТИВНЫЙ МАРКЕТИНГ КАК ИННОВАЦИОННЫЙ ИНСТРУМЕНТ РАЗВИТИЯ ОТРАСЛЕЙ И СФЕР ДЕЯТЕЛЬНОСТИ..... | 65 |
| ГЛАВА 7. ГЕЙМИФИКАЦИЯ В МЕНЕДЖМЕНТЕ – «ЗА» И «ПРОТИВ»..... | 75 |
| РАЗДЕЛ II. СОВРЕМЕННАЯ МЕДИЦИНА: АКТУАЛЬНЫЕ ВОПРОСЫ, ДОСТИЖЕНИЯ И ИННОВАЦИИ | 88 |
| ГЛАВА 8. РАЗРАБОТКА МЕДИЦИНСКИХ ИЗДЕЛИЙ ДЛЯ КРИОКОНСЕРВИРОВАНИЯ ЭРИТРОЦИТОВ ДОНОРСКОЙ КРОВИ | 89 |
| ГЛАВА 9. НАДО ЛИ УЧИТЫВАТЬ ОСОБЕННОСТИ КРОВООБРАЩЕНИЕ ПРОТЕЗНОГО ЛОЖА У ПАЦИЕНТОВ ДОНБАССА ПРИ ПОЛНОМ СЪЕМНОМ ПРОТЕЗИРОВАНИИ? | 100 |
| ГЛАВА 10. СИЛЬНЫЙ ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ КАК ГОЛОГРАММА ТЕМНОЙ ИНФОРМАЦИИ | 110 |
| РАЗДЕЛ III. СОВРЕМЕННЫЕ ТЕХНОЛОГИИ КАК ФАКТОР И РЕЗУЛЬТАТ ИННОВАЦИОННОГО РАЗВИТИЯ | 121 |
| ГЛАВА 11. ПОТЕНЦИОМЕТРИЧЕСКИЕ СЕНСОРНЫЕ СИСТЕМЫ ДЛЯ ОЦЕНКИ АНТИОКСИДАНТНОЙ АКТИВНОСТИ | 122 |
| ГЛАВА 12. КИБЕРБЕЗОПАСНОСТЬ. ОСНОВНЫЕ ТЕНДЕНЦИИ ПРЕСТУПНОСТИ В СФЕРЕ КРИПТОВАЛЮТ | 145 |

| | |
|--|-----|
| ГЛАВА 13. КИБЕРБЕЗОПАСНОСТЬ ВЕБ-САЙТОВ | 164 |
| ГЛАВА 14. КИБЕРБЕЗОПАСНОСТЬ. DARK WEB VS. DEEP WEB VS. SHADOW WEB | 176 |
| ГЛАВА 15. КИБЕРБЕЗОПАСНОСТЬ. ХААС ПРЕОБРАЗОВАНИЕ ЦИФРОВОГО ЛАНДШАФТА..... | 193 |

РАЗДЕЛ I. АКТУАЛЬНЫЕ ВОПРОСЫ СОЦИАЛЬНО- ЭКОНОМИЧЕСКОГО РАЗВИТИЯ

УДК 34

ГЛАВА 1. РАЗВИТИЕ ПРАВОВОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ МИРОПОРЯДКА

Матевосова Елена Константиновна

к.ю.н., доцент, доцент кафедры теории государства и права,
Московский государственный юридический университет имени О.Е. Кутафина (МГЮА)

Аннотация: в настоящей главе автором обосновывается, что формы, характер и степень влияния цифровых технологий на развитие различных сфер жизни современного российского общества требует от юридической науки и практики выработки инновационных парадигм к осмыслению новой правовой реальности и созданию нормативных и организационных механизмов реагирования на вызовы, угрозы и риски в условиях формирования многополярного мира, а также усиления и распространения всеохватывающих процессов цифровизации, а также формулируются авторские предложения по совершенствованию правовых подходов в реализации государственной политики в данной области.

Ключевые слова: правовая система, цифровые технологии, цифровизация, многополярность, полицентричность, законодательство, правоприменение, научно-технологическое развитие, искусственный интеллект

DEVELOPMENT OF THE LEGAL SYSTEM OF THE RUSSIAN FEDERATION IN THE CONDITIONS OF DIGITAL TRANSFORMATION OF THE WORLD ORDER

Matevosova Elena Konstantionovna

Abstract: in this chapter, the author substantiates that the forms, nature and degree of influence of digital technologies on the development of various spheres of life of modern Russian society require legal science and practice to develop innovative paradigms for understanding the new legal reality and creating normative and organizational mechanisms for responding to challenges, threats and risks in the context of the formation of a multipolar world, as well as the strengthening and spread of all-encompassing digitalization processes, and also formulates the author's proposals for improving legal approaches in the implementation of state policy in this area.

Key words: legal system, digital technologies, digitalization, multipolarity, polycentricity, legislation, law enforcement, scientific and technological development, artificial intelligence

Определяя приоритетные направления реализуемой Российской Федерацией внутренней и внешней политики в условиях происходящих уже в настоящем и прогнозируемых в ближайшем будущем трансформаций миропорядка, Пре-

зидент Российской Федерации в своём ежегодном Послании к Федеральному Собранию Российской Федерации от 29 февраля 2024 года [1], обращая особое внимание на необходимость качественного достижения целей проектов обеспечения технологического суверенитета государства, которые «должны стать мотором обновления нашей промышленности, помочь всей экономике выйти на передовой уровень эффективности и конкурентоспособности», указывает на следующие наиболее важные задачи государственного масштаба, связанные с всеохватывающими процессами цифровизации современного российского общества, в частности:

- внедрение цифровых технологий в управление;
- использование искусственного интеллекта в промышленности, в сельском хозяйстве, в строительстве, в транспорте, в социальной сфере;
- модернизация сети научно-технических библиотек в вузах и научных организациях в цифровые центры знаний и информации;
- цифровизация (с использованием технологий искусственного интеллекта) всех сфер производительности труда;
- создание цифровых платформ, которые позволяют оптимально выстроить взаимодействие граждан, бизнеса и государства между собой;
- создание цифровых платформ для сферы здравоохранения, обеспечивающих получение дистанционной медицинской помощи на основе данных цифрового профиля гражданина;
- формирование к 2030 году цифровых платформ во всех ключевых отраслях экономики и социальной сферы;
- использование алгоритмов искусственного интеллекта на создаваемых цифровых платформах;
- создание условий для использования цифровых систем не только в мегаполисах, но и в малых городах, в сельских территориях и в отдаленных районах, вдоль федеральных и региональных трасс, местных дорог.

В настоящее время возникает потребность в комплексном правовом обеспечении реализации новых национальных проектов технологического суверенитета («Средства производства и автоматизации», «Новые материалы и химия», «Промышленное обеспечение транспортной мобильности», «Новые технологии сбережения здоровья», «Технологическое обеспечение продовольственной безопасности», «Новые атомные и энергетические технологии», «Биоэкономика», «Беспилотные авиационные системы»), сформированных во исполнении поручений Президента Российской Федерации [2] и с учётом актуализации официальных взглядов на будущее научно-технологического развития России.

Новые реалии стремительного и масштабного внедрения цифровых технологий во все сферы жизни российского общества потребовали внесения следующих изменений в Национальную стратегию развития искусственного интеллекта на период до 2030 года [3; 4]:

1) корректировка понятий «технологии искусственного интеллекта» и «набор данных»;

Так, согласно актуальной редакции документа, технологиями искусственного интеллекта является «совокупность технологий», а не «технологии, основанные на использовании искусственного интеллекта», как это было определено в документе до 15 февраля 2024 года. А набор данных в настоящее время понимается не как «совокупность данных», а как «состав данных», которые структурированы или сгруппированы по определенным признакам, соответствуют требованиям законодательства Российской Федерации (не ограничиваясь требованиями законодательства Российской Федерации об информации, информационных технологиях и о защите информации) и необходимы не для «для разработки программного обеспечения на основе искусственного интеллекта», а непосредственно «для разработки программ для электронных вычислительных машин на основе искусственного интеллекта».

2) введение в нормативный оборот таких новых понятий, как «большие генеративные модели», «большие фундаментальные модели», «исходные данные», «модель искусственного интеллекта», «отказоустойчивость», «параметры модели искусственного интеллекта», «промышленные данные», «решение в области искусственного интеллекта», «сильный искусственный интеллект», «доверенные технологии искусственного интеллекта»;



Рис. 1. Основные принципы развития и использования технологий искусственного интеллекта в Российской Федерации



Рис. 2 Модель комплексной системы нормативно-правового регулирования

3) дополнение положениями о роли технологий искусственного интеллекта для современного человека в решении экономических, социальных, научных, медицинских, трудовых задачах общественного развития, положениями о международной конкуренции в данной области, содержащими экскурс в анализ прошлого, оценку настоящего и прогнозы [5] будущего использования указанных технологий, учитывая достигнутое и планируемое различными странами мира, в особенности лидирующими в области искусственного интеллекта;

4) замена такого принципа развития и использования технологий искусственного интеллекта, как «разумная бережливость» на принцип «наиболее эффективное использование технологий искусственного интеллекта», не изменяя общего содержания соответствующего подпункта «е)» пункта 19 и не придавая ему большей ясности;

5) дополнение принципов развития и использования технологий искусственного интеллекта (рис. 1) такими, как «открытость и доступность», «преемственность», «защищенность», «достоверность исходных данных»;

6) моделирование общей системы нормативно-правового регулирования общественных отношений в соответствующей области (рис. 2);

7) дополнение (с заменой отдельных пунктов) основных задач развития искусственного интеллекта в Российской Федерации такими задачами, как «повышение доступности инфраструктуры», «поддержка организаций», «повышение уровня компетенций» и повышение «уровня информированности граждан», «стимулирование внедрения технологий искусственного интеллекта», «обязательное внедрение доверенных технологий», а также «укрепление международного сотрудничества», предусматривая по каждой из задач комплекс мер-направлений;

8) установление конкретных показателей в сочетании количественных и качественных характеристик достижения целей развития искусственного интеллекта в Российской Федерации, измеряемых в максимальной мощности, приросте, объёме, численности, долях и уровнях;

9) определение конкретных задач международного сотрудничества в области использования технологий искусственного интеллекта;

10) определение основных направлений экспертно-аналитического и методологического сопровождения реализации задач развития искусственного интеллекта в Российской Федерации.

Примечательно, что в ранее действующей Национальной стратегии развития искусственного интеллекта на период до 2030 не содержалось ни одного положения об ответственности за разработку и использования технологий искусственного интеллекта, однако с внесением в неё ряда изменений и дополнений реализуемая сегодня стратегия предусматривает отдельные положения об ответственности, споры о которой сохраняют свою актуальность, приобретая ещё большую остроту, среди представителей юридического сообщества, научно мыслящих и практически созидających, и теми специалистами, которые, имея технические знания, непосредственно разрабатывают эти технологии и обес-

печивают их функциональное использование. Так, закрепленный принцип «защищенность» (подпункт «к» пункта 19) предполагает «разграничение ответственности организаций - разработчиков и пользователей технологий искусственного интеллекта исходя из характера и степени причиненного вреда». Однако, следует отметить, что данный подход к разграничению ответственности указанных субъектов может иметь существенные недостатки в его практической реализации, поскольку в таком случае демаркационные линии будут проводиться "знаками", описывающими последствия нарушений, а не обстоятельства, при которых они совершались, в то время как именно последние, раскрывая причинно-следственную связь, имеют первостепенное значение. Как принцип нормативно-правового регулирования общественных отношений принцип «ответственность» (подпункт «е» пункта 51(10) сводится к запрету делегирования системам искусственного интеллекта «ответственного нравственного выбора (в том числе принятие любых решений, способных оказать влияние на жизнь или здоровье человека)», а также делегирования «ответственности за последствия принятия решений». Системы искусственного интеллекта не обладают правосубъектностью, а потому любые решения, принимаемые данными системами, должны рассматриваться как производные от действий или бездействий физических или юридических лиц, которые их разрабатывают, тестируют, внедряют и эксплуатируют, и такой подход является обоснованным, что подтверждает правовой опыт большинства стран. Однако как в данном пункте, так и в иных нормах действующего российского законодательства отсутствует конкретизация используемого понятия «ответственный нравственный выбор», что создаёт неопределенность в его интерпретировании, поскольку нравственный выбор, рассматриваемый как процесс и результат, требует учёта философских, психологических и социокультурных аспектов в их единстве, и, соответственно, оперирования не формальными юридическими, а морально-этическими критериями в рамках нравственной, а не юридической ответственности, а потому не имеет достаточной степени определенности смысловая нагрузка слова «ответственного» в соответствующем положении нормативного характера. Надо признать, что конструкция «ответственного нравственного выбора» универсальна в своём применении к любым решениям, а не только к тем, которые, как закрепляется в рассматриваемом подпункте, «в том числе» способны оказать влияние на жизнь или здоровье человека.

Действующая Стратегия научно-технологического развития Российской Федерации [6] в числе т.н. «больших вызовов» для общества, государства и науки одним из наиболее значимых для научно-технологического развития Российской Федерации вызовов определяет такой, как «а) трансформация миропорядка, сопровождающаяся перестройкой глобальных финансовых, логистических и производственных систем, ростом геополитической и экономической нестабильности, международной конкуренции и конфликтности, системного неравенства на фоне ослабления национальных государственных институтов, снижения уровня и повышения сложности участия в международной ко-

операции в рамках научной, научно-технической и инновационной деятельности».

Несмотря на многомерную сложность понятия «большие вызовы», лишаящую правотворца возможности всеобъемлюще и статично его определить, в общих положениях Стратегии научно-технологического развития Российской Федерации данное понятие определяется как «объективно требующая реакции со стороны государства совокупность проблем, угроз и возможностей, сложность и масштаб которых таковы, что они не могут быть решены, устранены или реализованы исключительно за счет увеличения объема используемых ресурсов». Следует отметить, что в ранее действующей Стратегии научно-технологического развития Российской Федерации [7] содержалось аналогичное определение понятия «большие вызовы», однако такое явление, как «трансформация миропорядка» официально в этом документе стратегического характера не рассматривалось как большой вызов до 28 февраля 2024 года, знаменующего провозглашение Указом Президента Российской Федерации от 28.02.2024 № 145 нового курса государственной политики в соответствующей области.

Детальный анализ определения «большие вызовы» в синтезе прежде всего герменевтического, дискурсивного и догматического подходов с целью деконструкции и интерпретации его концептуальной матрицы, позволяет утверждать, что такими вызовами являются не отдельные проблемы, угрозы и возможности, а именно их совокупность, которая создаёт качественно новое состояние, выходящее за рамки простой суммы отдельных элементов, оказывая системное влияние на глобальное сообщество. По формулировке легального определения такая совокупность объективно требует «реакции со стороны государства» под которой применительно к исследуемой проблематике можно понимать феноменологическое проявление государственной власти, имплицитное реализацию комплекса мер для обеспечения и защиты национальных интересов при условии оптимизации ресурсного планирования с учётом закономерностей социальной динамики и в условиях нелинейности и неопределенности развития современного мира.

В контексте проблематики совершенствования правотворческих [8; 9] и правоприменительных подходов к обеспечению технологического суверенитета важно проводить различия между такими понятиями, как «вызовы», «угрозы» и «риски», учитывая, что «вызов» есть совокупность условий и факторов, создающих новые стимулы для развития, но также способных привести к возникновению угрозы, что требует адаптивных изменений и инновационных политических и правовых решений, «угроза» — это совокупность условий и факторов, создающих возможность наступления неблагоприятных событий, а «риск» — это реальная и вероятная возможность реализации угрозы.

Трансформация миропорядка в его цифровом измерении, являясь катализатором масштабных структурно-системных изменений в социальной, экономической, политической и культурной сферах жизни общества, есть

вызов, который, при политически выверенном и юридически продуманном подходе, может не создавать препятствия, а наоборот способствовать достижению государственных задач и целей устойчивого развития, общих для международного сообщества в целом. Однако следует признать, что такая цифровая трансформация способна привести и к возникновению ряда угроз, к примеру, такой, как повышение уровня уязвимости систем безопасности на национальном уровне (в том числе объектов критической информационной инфраструктуры) и в международном пространстве (в том числе международных организаций). Вместе с тем цифровая трансформация миропорядка вызывает значительные риски, связанные с неравномерным распределением ресурсов, формирующих цифровой потенциал государств, усиливая цифровое неравенство между ними, и, следовательно, конфликтность в международных отношениях.

Характер и направленность трансформационных изменений миропорядка сегодня во многом осмысливается в рамках концепции многополярности (полицентричности), которую последовательно отстаивает Российская Федерация, рассматривая такое мироустройство как результат воздействия тех объективных процессов, что уже наблюдаются в существующей мирополитической системе. Системный анализ действующих основополагающих, стратегических и прогнозных документов позволяет утверждать, что данная идея в течение многих лет отражается в официальных политических взглядах, согласно которым «система международных отношений должна быть многополярной» и основываться на определенных принципах [10], «процесс перехода к многополярности сопровождается нарастанием геополитической нестабильности и неустойчивости развития мировой экономики, резким обострением глобальной конкуренции» [11], «инновационное развитие характеризуется многополярностью распределения региональных точек роста» [12], новые вызовы начала XXI века и масштабные задачи в сфере международных отношений в условиях глобализации придают культурно-гуманитарным связям возрастающую значимость, что, «в первую очередь, связано с утверждением в мире многополярности» [13], современный мир претерпевает изменения, обусловленные переходом к полицентричной системе международных отношений [14]. Надо признать, что сегодня в условиях расширения цивилизационного влияния Российской Федерации на процесс формирования многополярного мира возникает объективная потребность в отражении политических приоритетов в действующем законодательстве, а именно введении в нормативные правовые акты различного уровня, особенно в системе стратегического планирования, всё больше положений, характеризующих многополярный мир, его преимущества, подчёркивая важность многополярного устройства в цифровизирующемся мире, и определяющих проектные задачи строительства нового стабильного и устойчивого миропорядка, объединяющего интересы большинства государств, как и Россия выступающих за многополюсность.

Современная наука находится ещё в состоянии поиска единообразного представления о многополярности (полицентричности), и задача вывести нечто

общее из того множества мнений, что высказываются представителями политической и правовой теории и практики, ещё не решена, однако уже в настоящее время цифровая трансформация общества и государства рассматривается как неотъемлемая часть сложного процесса «тектонических изменений» миропорядка, в том числе и в особенности формирования цифровой многополярности. Цифровая многополярность есть вызов для политической и правовой системы любого государства, которое должно оптимизировать институты публичной власти, систему законодательства и практику его применения, в целом правореализацию к новым условиям: совершенствовать систему государственного управления, находя новые формы взаимодействия и даже коллаборации с частным сектором как основным источником и двигателем цифровых инноваций, внедрять новые механизмы обеспечения кибербезопасности государства, учитывая, что в многополярном мире число киберугроз и рисков может не только не сокращаться, но и возрастать, разрабатывать новые правила, требования, стандарты, вводя цифровое пространство в правовые рамки, но не возводя границ, которые бы препятствовали инновациям.

Идея цифровой многополярности возникла как ответ на растущую несправедливость и неравенство в глобальном цифровом пространстве, в котором основные рычаги управления находятся преимущественно у нескольких крупных технологических компаний и государств. Но этот ответ в определенной степени есть часть более широкого стремления человечества к справедливости и равенству в глобальном масштабе, что наблюдается и на примере многих других «нецифровых» вопросов мировой повестки дня, и невозможно однозначно ответить на вопрос о том, является ли это следствием утраты инструментальной роли социальных ценностей фундаментального характера, что может представлять собой серьёзную угрозу, или это есть следствие научно-технологического прогресса, который меняет архитектуру международных отношений, выступая не как угроза, а как вызов для каждого государства.

Несмотря на нерешенность многих научных и политических споров в осмыслении цифрового настоящего и будущего государства как особой организации общества, практическую значимость сегодня имеет задача определения тенденций развития правовой системы [15] государства и их приоритизирующего «калибрования». В классификации данных тенденций необходимо руководствоваться различными критериями, которые обеспечивали бы релевантность и обоснованность выявления соответствующих тенденций, в частности учитывая формы и степень проявления тех или иных тенденций, сферы общественных отношений, в которых они возникают и развиваются, отрасли (подотрасли) или институты (подинституты) в системе права, подверженной цифровому влиянию. Как представляется, в современных условиях цифровых трансформаций общества, при которых цифровизация рассматривается не как результат преобразований общества, а как условие их достижения, необходима разработка нормативного правового акта как концептуальной основы обеспечения системного подхода к совершенствованию правовой системы Российской

Федерации, её нормативного, организационного, функционального и культурно-ценностного компонентов, в новой и стремительно изменяющейся цифровой реальности (к примеру, с таким наименованием, как Концепция правовой политики Российской Федерации в сфере цифрового развития общества) с постановкой конкретных целей и задач правовой политики в данном направлении, с обозначением принципов и ценностных ориентиров, с обозначением тех цифровых вызовов, угроз и рисков, которые оказывают влияние на саму правовую систему государства и которые требуют от права создавать новые эффективные модели регулирования изменчивых и возникающих общественных отношений, а также с указанием на субъектный состав участников и с описанием конкретных рабочих механизмов реализации такой политики. Нормативная обеспеченность внутренней и внешней политики Российской Федерации в условиях цифровизации общества государства должна иметь не только отраслевой, специализированный характер, как это прослеживается сегодня, но и своим целеполагаемо-программированным и планируемо-прогнозируемым основанием иметь единую общую правовую основу, формирование которой есть ключевая задача российского юридического сообщества.

Примечание к главе: данный монографический материал подготовлен автором в рамках выполнения работ по государственному заданию на тему: «Российская правовая система в реалиях цифровой трансформации общества и государства: адаптация и перспективы реагирования на современные вызовы и угрозы (FSMW-2023-0006)». Регистрационный номер ЕГИСУ НИОКТР: 124012000079-6.

Список источников

1. Послание Президента Российской Федерации Федеральному Собранию Российской Федерации от 29.02.2024 «Послание Президента Федеральному Собранию» // Российская газета. № 46. 01.03.2024.
2. Официальный сайт Президента Российской Федерации. URL: <http://www.kremlin.ru/events/president/news/75604> (дата обращения: 21.11.2024).
3. Указ Президента Российской Федерации от 10.10.2019 № 490 (ред. от 15.02.2024) «О развитии искусственного интеллекта в Российской Федерации» (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года») // Собрание законодательства Российской Федерации. 14.10.2019. № 41. Ст. 5700.
4. Перечень поручений по итогам конференции «Путешествие в мир искусственного интеллекта» (утв. Президентом Российской Федерации 17.01.2024 № Пр-83) // СПС «КонсультантПлюс».
5. Агамиров К.В. Юридическое прогнозирование как фактор совершенствования российской правовой системы. М., 2021. 528 с.

6. Указ Президента Российской Федерации от 28.02.2024 № 145 «О Стратегии научно-технологического развития Российской Федерации» // Собрание законодательства Российской Федерации. 04.03.2024. № 10. Ст. 1373.

7. Указ Президента Российской Федерации от 01.12.2016 № 642 «О Стратегии научно-технологического развития Российской Федерации» // Собрание законодательства Российской Федерации. 05.12.2016. № 49. Ст. 6887.

8. Правотворчество: аксиологические основания и стратегические приоритеты : монография; под общ. ред. О. Ю. Рыбакова. М., 2024. 298 с.

9. Амелин Р.В., Чаннов С.Е. Эволюция права под воздействием цифровых технологий. Москва: НОРМА, 2023. 280 с.

10. Указ Президента Российской Федерации от 31.03.2023 № 229 «Об утверждении Концепции внешней политики Российской Федерации» // Собрание законодательства Российской Федерации. 03.04.2023. № 14. Ст. 2406.

11. Указ Президента Российской Федерации от 13.05.2017 № 208 «О Стратегии экономической безопасности Российской Федерации на период до 2030 года» // Собрание законодательства Российской Федерации. 15.05.2017. № 20. Ст. 2902.

12. Прогноз долгосрочного социально-экономического развития Российской Федерации на период до 2030 года (разработан Минэкономразвития России) // СПС «КонсультантПлюс».

13. Основные направления политики Российской Федерации в сфере международного культурно-гуманитарного сотрудничества (утв. Президентом Российской Федерации 18.12.2010) // СПС «КонсультантПлюс».

14. Распоряжение Правительства Российской Федерации от 23.05.2020 № 1388-р (ред. от 12.07.2024) «Стратегия развития таможенной службы Российской Федерации до 2030 года» // Собрание законодательства Российской Федерации. 01.06.2020. № 22. Ст. 3572.

15. Марченко М. Н. Тенденции развития права в современном мире. М., 2015. 369 с.

УДК 0043

ГЛАВА 2. КРИПТОВОЛЮТА КАК ПРЕДМЕТ МОШЕННИЧЕСТВА

Хачатурян Эмиль Витальевич

студент 2 курса магистратуры юридического факультета
Дальневосточного филиала ФГБОУ ВО «Всероссийская академия внешней торговли
Министерства экономического развития Российской Федерации»

Кудрявцева Надежда Алексеевна

к.ю.н., доцент кафедры Юриспруденция
Дальневосточного филиала ФГБОУ ВО «Всероссийская академия внешней торговли
Министерства экономического развития Российской Федерации»,
судья Камчатского краевого суда в почетной отставке

Аннотация: в данной главе раскрываются основные характеристики криптовалюты как предмета мошенничества, рассматриваются основные схемы совершения указанных преступлений, рассматриваются основные виды криптовалют, анализируется судебная практика применительно к поставленному вопросу.

Ключевые слова: мошенничество, предмет преступления, криптовалюта, майнинг, цифровая валюта, цифровые финансовые активы, денежный суррогат.

CRYPTOCURRENCIES AS A SUBJECT OF FRAUD.

Khachaturian Emil Vitalievich*Scientific supervisor: Kudryavtseva Nadezhda Alekseevna*

Abstract: the article reveals the main characteristics of cryptocurrencies as a subject of fraud, examines the main schemes for committing these crimes, examines the main types of cryptocurrencies, analyzes judicial practice in relation to the issue raised.

Keywords: fraud, subject of crime, cryptocurrency, mining, digital currency, digital financial assets, monetary surrogate.

Несмотря на то, что в последние годы возросло количество судебных дел, в которых в той или иной мере фигурирует криптовалюта, на законодательном уровне её правовой статус не определен.

В доктринальных разработках так же отсутствует единый подход относительно того, что понимать под «криптовалютой», какова её правовая сущность и как следует квалифицировать действия, связанные с её оборотом.

Вместе с тем, 2022 год ознаменовался рядом громких скандалов, связанных с криптовалютами, включая банкротства и обвинения в мошеннических действиях FTX, Celsius, Three Arrows Capital и прочие.

Так, Министерство юстиции США выступило с заявлением о задержании главы криптовалютной компании-маркетмейкера «Gotbit» Алексея Андрюнина

на территории Португалии. Его арест произошел 8 октября 2024 года в Португалии, и в настоящее время он ожидает экстрадиции. Обвинения, предъявленные «Gotbit», «ZM Quant», «CLS Global» и «MyTrade», касаются манипулирования рынком и фиктивных сделок. Предполагается, что эти компании искусственно увеличивали торговые объемы для токенов, совершали мошенничество на рынке криптовалют. Помимо гражданина России, обвинения были предъявлены еще 17 физическим и юридическим лицам, включая граждан США. Восемнадцати лицам предъявлены обвинения в рамках международной операции, направленной на противодействие широко распространенным мошенническим действиям и манипуляциям на криптовалютных рынках. Обвиняемые создавали криптовалютные компании, делали ложные заявления о токенах и заключали фиктивные сделки. Эти действия привлекали новых инвесторов, что способствовало росту цен на токены, после чего обвиняемые продавали их по искусственно завышенным ценам. Сервис «MyTrade» позволял совершать миллионы сделок «wash» в день для каждой клиентской криптовалюты. Один из обвиняемых охарактеризовал «MyTrade» как превосходящую «CLS» и «Gotbit», поскольку они контролировали перекачку и сброс цифровой валюты, а цели wash-трейдинга включали демонстрацию непрерывной торговой активности и создание больших объемов торгов для бирж.

Если криминальную активность с криптовалютой оценивать в денежном эквиваленте то, по некоторым подсчетам в мире эта сумма на 2022 год составляла 20,6 млрд. долларов [4]. В России криминализация действий с криптовалютами также занимает существенное место, о чем свидетельствует тот факт, что за 2022 год было вынесено 463 судебных актов по уголовным делам о мошенничестве, присвоении, растрате и иных преступлениях в которых криптовалюта являлась либо предметом преступления, либо способ его совершения был связан с использованием криптовалюты (чаще всего с легализацией (отмыванием) доходов, полученных преступным путем) [7].

В 2024 году совокупный веб-трафик российских пользователей на крупнейших криптовалютных площадках, таких как биржи, P2P-платформы и обменники, увеличился на 16,4% по сравнению со вторым и третьим кварталами 2023 года и составил 104,6 миллиона посещений. Также на 15,1% выросло среднемесячное количество уникальных пользователей (IP-адресов) этих площадок. Доля россиян в общем количестве посещений также увеличилась до 7% в первом квартале 2024 года.

И если судебная практика по уголовным делам, связанным с легализацией (отмываем) доходов, полученных преступным путем, является более - менее устоявшейся, то в вопросе о том, может ли криптовалюта являться предметом преступлений против собственности, в частности, мошенничества, единого мнения как в научной литературе, так и в правоприменительной практике не наблюдается.

Первая точка зрения основывается на том, что криптовалюту нельзя признавать предметом преступлений против собственности поскольку она не явля-

ется объектом гражданских прав (Аджиев Н.Б., Э.Л. Сидоренко [1]), подобное обоснование послужило основанием исключения действий с криптовалютой из объема обвинения в уголовном деле о вымогательстве (ст. 163 УК РФ) в приговоре Петроградского районного суда г. Санкт – Петербурга. По обстоятельствам дела подсудимые обвинялись в том, что представившись сотрудниками ФСБ, инцинировали группу захвата и предъявили потерпевшему требования о передаче 5 миллионов рублей и направлении на названные ими электронные адреса 99.7035 биткоинов, стоимость которых составляла на момент совершения преступления 48 млн. руб., 2072150.73446889 дигибайтов, стоимость которых составляла 4 млн. руб. и 198700.17928287 битшейресов, стоимостью 3 млн. руб. Исключая из объема обвинения эпизод с завладением криптовалютой, суд указал, что криптовалюта не может выступать предметом хищения, поскольку не является объектом гражданских прав и не может быть отнесена к деньгам, ценным бумагам, вещам или иному имуществу, данный вид денежных средств не подпадает ни под одну из категорий, не признается в качестве средства платежа на территории Российской Федерации и отнесен к суррогатам денежных средств (приговор был в последующем отменен вышестоящей инстанцией по протесту прокурора с направлением уголовного дела на новое судебное рассмотрение) [10].

Противоположенную позицию занимают А.Е. Русскевич и И.И. Малыгин, А.Н. Ляскало, М.А. Простосердов, указывая на наличие у криптовалюты таких признаков как экономическая стоимость и материальная ценность [7, 12]. Имеется и судебная практика подтверждающая указанный подход, так Восьмой Кассационный суд общей юрисдикции, рассматривая уголовное дело по ч. 4 ст. 159 УК РФ, определил криптовалюту предметом хищения, указав, что «.. криптовалюта - биткоины, по своей сути, являются разновидностью цифровой валюты, имеет способность к конвертации в денежные средства, в том числе в валюту иностранных государств, а также может быть принята в качестве средства инвестиций и платежа, не являясь денежной единицей или расчетной единицей, в связи с чем, имеет материальную ценность, стоимость которой необходимо определять как актуальную на момент совершения преступления [4].

Определением Первого кассационного суда общей юрисдикции от 4 июня 2024 года признан законным приговор по обвинению М. по п. “б” ч. 3 ст. 163 УК РФ, при этом суд, расценил требование в адрес потерпевшего о передаче 5 биткоинов как требование о передаче иного имущества, поскольку, как указал в определении суд, “биткоин обладал рыночной стоимостью в рублевом эквиваленте” на момент [5].

Аналогичным образом обоснована и позиция о признании Н. виновным в совершении преступления, предусмотренного п. “б” ч. 3 ст. 161 УК РФ в определении Третьего кассационного суда общей юрисдикции от 6 июня 2023 года, к котором указано, что отсутствие законодательного регулирования криптовалюты и оценки их стоимости в законодательстве Российской Федерации не исключает квалификации действий по их безвозмездному изъятию и обращению

в свою пользу как хищения, поскольку она имеет определенную имущественную ценность [6].

Для разрешения этого вопроса, прежде всего, следует определиться с понятием «криптовалюта», учитывая, что оно не раскрывается ни в Гражданском кодексе РФ, ни в Федеральном законе РФ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации».

В ч. 3 ст. 1 указанного закона дано определение *цифровой валюты* как совокупности электронных данных (цифрового кода или обозначения), содержащихся в информационной системе которые предлагаются и (или) могут быть приняты в качестве средства платежа, не являющегося денежной единицей. То есть, другими словами, это единица ценности воплощенная в электронную форму (в виде алгоритмов или кодов), цифровой актив для выпуска которого используются особые алгоритмы и операции шифрования данных.

Следует учитывать, что криптовалюта не является денежными средствами в Российской Федерации, поскольку в соответствии с ч. 7 ст. 14 Федерального закона РФ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» она не может выступать в качестве оплаты товаров, работ или услуг. Также запрещено распространение любой информации о ресурсах, где можно расплатиться криптовалютой. Требования граждан и юридических лиц, связанные с цифровыми валютами, подлежат судебной защите только в том случае, если они предоставили информацию об активах в налоговые органы. [9].

Интересно отметить, что на территории Евросоюза пятой директивой AMLD было введено определение «виртуальной валюты», под которой понимается цифровое представление стоимости, которое не выдается и не гарантируется центральным банком или государственным органом, не обязательно привязано к установленной законом валюте и не имеет юридического статуса валюты или денег, но принимается физическими или юридическими лицами в качестве средства обмена и которое может передаваться, храниться и продаваться в электронном виде [3].

В Гражданском кодексе РФ закрепления определения криптовалюты также не имеется. Статья 128 ГК РФ к объектам гражданского права относит «цифровые права», понятие которых раскрывается в ст. 141.1 ГК РФ. Но сопоставление ст. ст. 128 и 141.1 ГК РФ не дает возможности установить, какие конкретно объекты гражданских прав отнесены к цифровым правам. То есть вопрос о том, можно ли криптовалюты относить к объектам гражданских прав остался открытым.

Кроме того, необходимо разводить понятие криптовалюты, цифровой валюты и цифровых финансовых активов, поскольку достаточно часто эти понятия рассматриваются как аналогичные, коими не являются.

Цифровая валюта - это цифровой аналог фиатной валюты, который существует в виртуальном мире, не имеет физического облачения и эквивалента. То

есть, являясь более общим понятием, оно охватывает любую электронную версию валюты. Криптовалюта - лишь одна из разновидностей цифровой валюты, наряду с стейблкоинами (курс которых привязан к определенной фиатной валюте (централизованные стейблкоины) или активу из реального мира (децентрализованные), игровыми деньгами и цифровой валютой центрального банка (CBDCs).

Эмиссией стейблкоинов занимаются специальные компании, например, Tether Limited, после поступления на банковский аккаунт компании фиатных денег в пропорциональном соотношении создаются токены (один Tether равен одному доллару), которые таким образом поступают в обращение.

Цифровая валюта центрального банка (CBDCs) - это цифровая валюта, которая выпускается и контролируется центральным банком страны, например, Центральный банк Багамских островов (Send Dollar), Банк Ямайки (JemDex) и др.

Цифровые финансовые активы выпускаются через официальных операторов, включенных в реестр Центральным Банком РФ и являются цифровыми правами (ст. 1 Федерального закона РФ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации»). По своей сути – это цифровой аналог договора займа, векселя или облигации, которые существуют в определенной информационной системе [13].

В основе же криптовалют лежит технология блокчейн, которая, простыми словами, представляет собой реестр операций (платформа, хранящая информацию о сделках), то есть цепочка блоков о всех транзакциях и сделках, которая является последовательной и непрерывной. Каждый такой блок содержит ссылку на предыдущий и метку времени. Эта база формируется автономно, без внешних серверов и администраторов. В блокчейне прозрачна лишь история транзакций, но личность их совершивших не раскрывается. Для работы с криптовалютой нужна программа-кошелек, которая содержит два ключа - приватный и публичный. Публичный ключ - это как раз цифровая строка которую может увидеть каждый, а приватный или закрытый - это код из серии случайных чисел, который невозможно взломать и который обеспечивает безопасность.

Выпуск криптовалюты осуществляется посредством майнинга при отсутствии эмитента.

Таким образом, можно выделить следующие признаки криптовалюты:

- она не является денежными средствами, это цифровой код, результат функционирования соответствующей компьютерной программы;

- курс криптовалюты практически не оценим, поскольку все биржи имеют различные курсы, которые зачастую не прогнозируемы, а сама она ничем не обеспечена, специальный орган или порядок, установленный законом, который бы позволил определить стоимость конкретной криптовалюты на определенную дату, отсутствует;

- она децентрализована, оборот осуществляется с использованием пиринговых операционных систем, то есть никакого специального органа или механизма позволяющего отследить ее перемещение также не имеется, отсутствует внешний или внутренний администратор. В этом отличие криптовалюты от цифровой валюты, транзакции которой контролируется серверами, принадлежащими определенной группе людей. Вместе с тем, в настоящее время имеются некоторые механизмы позволяющие отслеживать операции с криптовалютами. Первый - с помощью информации, имеющейся на криптовалютных биржах, если им переданы открытые кошельки для трейдинга. То есть, если правоохранительные органы запросят подобную информацию, биржа обязана ее предоставить. Второй способ - с привлечением специалистов, способных отслеживать и анализировать информацию о транзакциях. В частности, правоохранительные органы США для раскрытия уголовных дел, связанных с криптовалютой, привлекают специалистов таких фирм;

- она анонимна – на бирже мы не сможем увидеть персональные данные владельца, IP-адрес напрямую с физическим лицом не связан, такое лицо является лишь владельцем пароля от криптокошелька, то есть «именем» является лишь логин от «кошелька». А отличие от цифровой валюты для пользования которой необходимо пройти идентификацию;

- это полностью виртуальное явление, она возникает только в Интернет-пространстве, не имеет физического воплощения;

- она трансгранична, не имеет национальной принадлежности;

- необратимость транзакции, то есть в отличие от банковской операции по переводу фиатных денег, которую в течении определенного срока можно отменить, транзакция криптовалюты необратима;

- не являясь денежной единицей, она представляет экономический интерес и имеет материальную ценность. В данном случае речь идет именно об экономической стоимости, которая формируется исходя из различных факторов, как политических или экономических, так и общественных событий. [13].

Фактически оборот криптовалюты построен на принципах добросовестности контрагента и доверии между сторонами транзакции. То есть, участники соответствующих отношений просто договариваются о том, что владелец соответствующего кода имеет определенное количество имущества, которое можно использовать как эквивалент стоимости товаров, это цифровое представление стоимости, оборот криптовалюты исключает участие каких-либо посредников.

Учитывая имеющиеся пробелы в законодательстве, а так же указанные выше особенности криптовалюты, в том числе её анонимность, децентрализованность, построение на принципе добросовестности контрагента, она достаточно часто используются при совершении преступлений, в том числе, мошеннических действий. Однако, в каждом конкретном деле необходимо устанавливать, что в действительности является предметом преступления: непосредственно сама криптовалюта или конкретная денежная сумма, которая передавалась, например, для “якобы ее приобретения”. Провести такое разграничение

возможно в зависимости от той мошеннической схемы, которая используется.

Рассмотрим несколько наиболее распространенных схем, в которых предмет преступления является криптовалюта.

1. Завладение криптовалютой под предлогом её обмена на эквивалент в рублях или иной валюте, когда субъект преступления не намереваясь производить оплату стоимости криптовалюты, вводит потерпевшего в заблуждение путем обещаний перечислить оговоренную сумму, а затем, получая доступ к принадлежащему потерпевшему «BTC-e» коду (который им передает сам потерпевший, находясь в заблуждении), зачисляет «BTC-e» код на свою учетную запись.

2. Предложение быстрого увеличения размера криптовалюты и получения дохода за счет временного предоставления доступа к «BTC-e» коду. В результате, после того, как потерпевший предоставляет доступ, «BTC-e» код зачисляется на учетную запись мошенников.

3. Фишинг - создание поддельных сайтов, чаще всего достаточно похожих на оригинальные, на которых можно проверить какую награду от проекта получил пользователь. Чаще всего создаются аккаунты, полностью идентичные какому-либо известному криптопроекту. Для проверки награды необходимо подключить свой криптокошелек (как правило всплывает окно с запросом о разрешении подключения криптокошелька), как только дано подтверждение, все содержимое криптокошелька списывается. Иногда под разрешением на подключение кошелька замаскировано согласие на списание имеющихся в нем средств.

4. Dust attack - с помощью специальных сервисов создается кошелек, адрес которого похож на адрес потанциальной жертвы, далее с поддельного адреса жертве пересылаются небольшие суммы в криптовалюте. Фейковый адрес отражается в истории операций. Потерпевший перепутав номера, может отправить на фейковый номер криптовалюту. Например, один из пользователей таким образом потерял 68 млн. долларов, которые в последующем были ему возвращены.

Второй вариант такого вида мошенничества, это создание монет, в которых содержится слово “эирдроп”, затем они направляются потерпевшим, в расчете на то, что они пройдут по указанному адресу, подключив к нему кошелек, в результате чего мошенники получают доступ к активам пользователя.

5. Вложение в новую криптовалюту, которая имеет большой рост, однако при последующей попытке обналичивания денежных средств, вложения обнуляются, поскольку в саму монету была зашита комиссия 100 % при продаже.

6. Предложение работы с получением зарплаты в криптовалюте, однако, чтобы вывести активы (потерпевший видит записи о наличии на своем счете криптовалюты), необходимо перевести определенную сумму или пополнить баланс, например на 50-100 \$.

7. Продажа за криптовалюту якобы популярного канала в “Телеграмме”, не говоря уже об организации финансовых пирамид под видом получения дохода

от операций с криптовалютой.

То есть все указанные варианты сводятся к тому, что лицо берет на себя определенное обязательство за определенную плату совершить какую-либо сделку или действие с криптовалютой, заведомо не собираясь этого совершать либо иным обманным путем получает доступ к криптовалюте потерпевшего.

Следует так же иметь ввиду, что в Российской Федерации отсутствует специальный орган или порядок, установленный законом, который бы позволил определить стоимость конкретной криптовалюты на определенную дату, то есть правоохранительным органам и суду проблематично установить точный размер хищения, и как следствие, причиненный ущерб, что в соответствии со ст. 73 УПК РФ входит в предмет доказывания.

Ответ на указанный вопрос на практике предлагается решать двумя способами:

- стоимость криптовалюты определяется исходя из средств, затраченных на её приобретение;
- стоимость устанавливается путем проведения соответствующих экспертных исследований, путем сопоставления среднерыночного курса с денежным эквивалентом на момент совершения преступления.

Вместе с тем, имеющийся пробел не должен являться основанием для отказа в возбуждении уголовных дел, поскольку в таком случае права потерпевших остались бы незащищенными, что только усугубит криминальную ситуацию в указанной сфере, поскольку, как известно, безнаказанность порождает вседозволенность.

С другой стороны, обман при мошеннических действиях может выражаться в предложениях «приобрести» криптовалюту в обмен на определенную сумму денег (когда после перевода денежных средств никакая криптовалюта не предоставляется), инвестировать денежные средства в проведение сделок с криптовалютой и таким образом получать доход. Достаточно часто для реализации таких схем используются и «раскручиваются» телеграмм-каналы об инвестициях в криптовалюту, после того, как потерпевший переводит определенную сумму денег, ему сообщают об многократном ее увеличении, но для ее обналичивания необходимо оплатить проценты, которые не могут сниматься с основной суммы, а требуется внести дополнительно и т.п., однако в этих случаях обещание приобретения криптовалюты - это лишь способ получить денежные средства потерпевшего, следовательно предметом преступления будут являться денежные средства.

Так, согласно приговору Йошкар-Олинского городского суда Республики Марий Эл от 23 января 2024 г., обвиняемый, находясь в неизвестном месте, зарегистрировался в мессенджере «Телеграм» и в своём аккаунте начал переписку с потерпевшим, с которым ранее был знаком. Они обсуждали куплю-продажу криптовалюты - биткоинов. В ходе переписки обвиняемый неоднократно менял условия сделки и её сумму. Сначала он хотел заключить сделку на 388 800 рублей, а затем увеличил сумму до 11 188 800, так как думал, что у

него будет такая сумма денег. Потерпевший рассчитывался с обвиняемым за биткойны на заявленные суммы. Потерпевший сообщил обвиняемому через мессенджер, что приготовил 10 800 000 рублей для покупки биткойнов, так как собирался приобрести их только на эту сумму. Они договорились о месте и времени встречи в городе Йошкар-Оле Республики Марий Эл для проведения сделки. В связи с этим у обвиняемого возник корыстный преступный умысел, направленный на хищение 10 800 000 рублей, принадлежащих потерпевшему, путём обмана и злоупотребления доверием, в особо крупном размере. Чтобы осуществить свой план, он решил назначить встречу в безлюдном месте. Затем, под предлогом проверки подлинности 10 800 000 рублей, он взял бы эти деньги и скрылся с ними с места преступления, не переводя биткойны [11].

Из данного примера видно, что в указанном случае криптовалюта не являлась непосредственным предметом преступления, коим являлись денежные средства. Виновные путем обещаний приобрести криптовалюту получили доступ к денежным средствам потерпевшего.

Естественно, это лишь малая часть всех мошеннических схем. Важно само понимание предмета мошенничества при этом, либо это непосредственно криптовалюта и тогда закономерно встает вопрос в ее оценке, либо это конкретная сумма денежных средств, переданная мошенникам под условием, например, «якобы» приобретения криптовалюты.

Специфичный предмет преступления предопределяет вопросы, которые возникают перед правоохранительными органами при расследовании указанной группы преступлений, это не только правильное определение предмета преступления и определение его стоимости, но и особенности в получении «цифровых доказательств», особенности изъятия криптовалюты и наложения ограничений на её оборот и ряд других.

Как видно из приведенных примеров, анализа законодательства, в данном случае для формирования судебной практики необходимо законодательное закрепления понятия криптовалюты, формирование единого подхода к определению ее признаков, поскольку это позволит осуществить возможность формирования единообразной судебной практики.

В заключении хотелось бы отметить, что мошенничество, предметом хищения которого является криптовалюта подлежит квалификации по ст. 159 УК РФ. В то же время в Уголовном кодексе РФ имеется статья 159.3 УК РФ - мошенничество с использованием электронных средств платежа. Однако предметом указанного преступления являются денежные средства как безналичные, так и электронные

Список источников

1. Аджиев Н.Б. Криптовалюта как предмет преступлений против собственности. Международный научно-исследовательский журнал № 8 (134) 2023

— URL: <https://research-journal.org/archive/8-134-2023-august/10.23670/IRJ.2023.134.149> (дата обращения 22.10.2024)

2. Апелляционное определение Санкт-Петербургского городского суда от 16 мая 2022 года по делу 1-257/21. — URL: https://sankt-peterburgsky--spb.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=57149965&delo_id=4&new=4&text_number=1 (дата обращения 23.04.2023)

3. Директива Европейского парламента и Совета от 16 сентября 2009 г. 2009/110/ЕС о допуске к деятельности организаций электронных денег и ее осуществлении, а также о пруденциальном надзоре за этими организациями, об изменении Директив 2005/60/ЕС и 2006/48/ЕС и об отмене Директивы 2000/46/ЕС. Журнал Европейского Союза L 267. С. 7—17.// URL: <http://eurlex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32009L0110&from=FR>.

4. Кассационное определение восьмого кассационного суда общей юрисдикции от 21.12.2023 № 77-5316/2023. Электронный ресурс. Режим доступа: https://8kas.sudrf.ru/modules.php?name=sud_delo&name_op=doc&number=27146451&delo_id=2450001&case_type=0&new=2450001&text_number=1&srv_num=1 (дата обращения: 24.10.2024)

5. Кассационное определение Первого кассационного суда общей юрисдикции от 04.06.2024 № 77-1995/2024 (УИД 50RS0028-01-2023-003168-98) Электронный ресурс. Режим доступа: <https://1kas.sudrf.ru/> (дата обращения: 24.10.2024)

6. Кассационное определение Третьего кассационного суда общей юрисдикции от 06.06.2023 по делу № 77-1296/2023 Электронный ресурс. Режим доступа: <https://3kas.sudrf.ru/> (дата обращения: 24.10.2024)

7. Ляско А.Н. Криптовалюта как предмет и средство преступления / Уголовное право: стратегия развития в XX I веке: материалы XVI Международной конференции. М.: РГ-Пресс, 2019. С. 87-89

8. Отчет о криптокриминале за 2023 год. BitNovosti.com — URL: <https://bitnovosti.io/2023/03/27/otchyot-o-kriptokriminala-2023/> (дата обращения 22.10.2024)

9. О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 31 июля 2020 г. № 259-ФЗ (в ред. 8 августа 2024 г. № 223-ФЗ) //Собрание законодательства Российской Федерации от 3 августа 2020 г. № 31 (часть I) ст. 5018

10. Приговор Петроградского районного суда г. Санкт-Петербурга от 30.06.2020 по делу № 1-95/2020. Электронный ресурс. Режим доступа: <http://pgr.spb.sudrf.ru/> (дата обращения: 24.10.2024)

11. Приговор Йошкар-Олинского городского суда Республики Марий Эл № 1-15/2024 1-838/2023 от 23 января 2024 г. по делу № 1-15/2024 Электронный ресурс. Режим доступа: <https://yoshkarolinsky-->

mari.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=case&case_id=8326963&case_uid=6ae5ee49-9984-45c8-8fac-aa0003399f5a&delo_id=1540006&new= (дата обращения: 24.10.2024)

12. Русскевич А.Е., Малыгин И.И. преступления, связанные с обращением криптовалют: особенности квалификации. Журнал Высшей школы экономики. 2021. № 3. С. 106-125

13. ЦФА – это не криптовалюта. — URL: <https://www.rbc.ru/crypto/news/631b2bf69a794796b75dd573?ysclid=m2mg1nty1b368455670> (дата обращения 23.10.2024)

14. Число связанных с криптовалютами судебных дел выросло в России на 15% : РБК.Крипто. 19.04.2023 — URL: <https://www.rbc.ru/crypto/news/643fb5629a79471d10b8bbc1> (дата обращения 22.10.2024)

УДК 343.61

ГЛАВА 3. СТРАТЕГИЧЕСКИЙ АСПЕКТ РАЗВИТИЯ УГОЛОВНОГО РОССИЙСКОГО ЗАКОНОДАТЕЛЬСТВА В ОБЛАСТИ ОХРАНЫ ЗДОРОВЬЯ

Маторина Ольга Сергеевна,
Удавцова Елена Юрьевна

кандидат технических наук
ФГБУ ВНИИПО МЧС России

Аннотация: приводится анализ законодательства с уклоном на стратегический аспект развития в области охраны здоровья. Рассмотрены и проанализированы документы ООН, отечественное уголовное законодательство, международно-правовые соглашения, стратегия национальной безопасности, приведены тезисы исследователей рассматриваемой области.

Ключевые слова: стратегический подход, уголовное законодательство, охрана здоровья.

THE STRATEGIC ASPECT OF THE DEVELOPMENT OF RUSSIAN CRIMINAL LEGISLATION IN THE FIELD OF HEALTH PROTECTION

Matorina Olga Sergeevna,
Udavtsova Elena Yuryevna

Abstract: the analysis of legislation with a focus on the strategic aspect of development in the field of health protection is presented. The UN documents, domestic criminal legislation, international legal agreements, national security strategy are considered and analyzed, and the theses of researchers in the field under consideration are presented.

Key words: strategic approach, criminal law, health protection.

Понятие «здоровье» впервые было обозначено в преамбуле Устава Всемирной организации здравоохранения ВОЗ [1] как состояние полного социального, физического и душевного благополучия, при отсутствии болезней, физических недугов. Нормы Устава ВОЗ ознаменовали начало регулирования социального права на здоровье в международных договорах, конвенциях.

В частности, в ст. 5 Всеобщей декларации прав человека [2] установлен всеобщий запрет на применение пыток, бесчеловечного, жестокого обращения, унижения достоинства, который непосредственно характеризует нарушение права человека на здоровье. Вместе с этим, нормы п. 1 ст. 25 Всеобщей декларации провозглашают право человека на жизненный уровень, обеспечивающий жилище, одежду, пищу, социальное обслуживание, медицинский уход, необходимые для поддержания его здоровья.

Для реализации указанных запрета и прав человека на здоровье были раз-

работаны другие документы ООН по множеству вопросов, связанных с охраной здоровья. Так в сфере здравоохранения было принято 4 декларации ООН, 9 конвенций и прочих соглашений о правах ребенка, 10 конвенций и др. международных соглашений о правах инвалидов, 8 конвенций и пр. соглашений в сфере предупреждения преступности, 2 конвенции по медико-санитарным правилам и т.д. [3].

Например, среди международных соглашений о правах ребенка стоит выделить Пекинские правила 1985 года [4], которые определяют ключевые основы системы правосудия при разрешении дел с участием несовершеннолетних:

1) система судопроизводства должна соответствовать основным интересам несовершеннолетних и функционировать на основе участия несовершеннолетнего с собственной точкой зрения без какого-либо принуждения и ограничений в сфере здоровья;

2) выбор мер уголовно-правового воздействия на несовершеннолетнего должен проводиться с учетом следующих принципов:

- при рассмотрении дела с участием несовершеннолетнего вопросы здоровья ребенка должны быть ключевым фактором;

- применение наказания должно соизмеряться с обстоятельствами, тяжестью правонарушения, потребностями, здоровьем и социальным положением несовершеннолетнего;

- наказание в виде ограничения свободы для несовершеннолетнего следует применять при условии тщательного анализа всех обстоятельств и присуждения возможного минимума;

- несовершеннолетнего лица не следует лишать свободы кроме случаев совершения серьезного насилия против человека или неоднократного другого серьезного правонарушения при условии отсутствия возможности применения иных мер воздействия.

Как видно на примере Пекинских правил, охрана здоровья в уголовно-правовых нормах международного права обеспечивает гуманное соблюдение права на здоровье разных сторон уголовного судопроизводства: несовершеннолетние могут быть лишены свободы за насильственное преступление против здоровья человека и в рамках судопроизводства должны учитываться особенности здоровья виновного подростка.

То есть, можно обобщить вывод о международно-правовом аспекте развития уголовного российского законодательства об охране здоровья, который характеризуется развитием с XIX века международно-правовых соглашений по множеству гуманных вопросов охраны здоровья человека в сферах санитарных, социальных, оздоровительных, уголовно-правовых и пр. отношений.

Представленные конституционные и международно-правовые особенности предполагают многоотраслевой характер российского законодательства в сфере охраны здоровья, что подтверждается множеством законодательных актов, регулирующих в той или иной мере вопросы уголовно-правовой ответственности за нарушение требований в сфере охраны здоровья.

В этой связи следует указать на общие нормы УК РФ о признаках преступлений, связанных с человеческим здоровьем. Так в ст. 20 УК РФ предусмотрены субъективные признаки наступления уголовной ответственности с 14 лет за более тяжкие преступления в сфере здоровья человека (ст. 105, 111, 112, 126, 131, 132). В нормах ст. 37 УК РФ обозначены объективные признаки необходимой обороны и отсутствия состава преступлений в случае причинения обороняющимся вреда здоровью человека в рамках защиты от посягательства при соблюдении условий необходимой обороны.

Вместе с этим, положения ст. 57 УК РФ определяют общие уголовно-исполнительные признаки установления наиболее строгой меры в виде пожизненного лишения свободы за особые категории преступление, связанных с посягательством на жизнь, здоровье населения, половой неприкосновенности несовершеннолетних.

Стоит привести тезисы М.П. Журавлева, С.И. Никулина [5], В.П. Кашепова [6] и др. российских исследователей [7], которые связывают государственную защиту конституционного права на охрану здоровья с уголовно-правовым обеспечением безопасности личности, которая согласно Федеральному закону «О безопасности» [8] и Стратегии национальной безопасности РФ (далее – Стратегия НБ [9]) представляется состоянием защищенности здоровья и личных прав от возможных угроз, обеспечивающим реализацию конституционных прав человека на охрану здоровья и личных прав.

Действительно, обеспечение охраны здоровья российских граждан установлено одной из государственных задач Стратегии НБ, поскольку государственная политика России направлена, в первую очередь, на создание комплекса условий укрепления здоровья, роста продолжительности жизни, уменьшения показателей смертности, улучшения других важных показателей качества жизни и развития человека [10].

По данному поводу в п. 33 Стратегии НБ определено 17 задач государственной политики России в сфере охраны здоровья, включающих:

- 1) имущественные задачи: роста реальных доходов россиян, снижения количества малообеспеченных и уровня неравенства доходов граждан;
- 2) социальные задачи: повышения доступности и качества услуг для граждан, обеспечения участия лиц старшего возраста и с ограниченным здоровьем в общественной жизни;
- 3) демографические задачи: повышения в российских семьях рождаемости, развития мотивации семей к многодетности;
- 4) оздоровительные задачи: роста продолжительности жизни, уменьшения уровня инвалидизации и смертности населения, предупреждения профзаболеваний; и пр.

Указанные задачи государственной политики России в сфере охраны здоровья, как видно, отличаются имущественным, социальным, демографическим и пр. содержанием, но не охватывают уголовно-правовые и др. правоохранные задачи обеспечения прав граждан на здоровье в рамках исполнения со-

ответствующего законодательства.

Поэтому предлагается дополнить п. 33 Стратегии НБ подпунктом 18, определяющим обеспечительную задачу в сфере охраны здоровья: «18) привлечение к установленной законом ответственности лиц, нарушающих права человека, провозглашенные Конституцией РФ».

Таким образом, можно выделить стратегический аспект развития уголовного российского законодательства об охране здоровья, который обусловлен регламентацией в Стратегии НБ [11] комплекса задач государственной политики России в сфере развития здоровья и человеческого потенциала, включающих многоотраслевые меры обеспечения здоровья человека без указания обеспечительных мер уголовно-правовой и прочей ответственности в сфере охраны человеческого здоровья.

Схожим негативным аспектом отсутствия необходимых правовых механизмов уголовной ответственности за нарушения прав граждан на здоровье отличается базовый закон в сфере охраны здоровья. Так в нормах Основ охраны здоровья российских граждан (далее – Основы [12]) предусмотрено семь видов норм отраслевых законов, образующих систему российского законодательства в сфере здоровья [13].

Первый вид включает положения законов сферы обеспечения прав на безопасную среду обитания (об охране воздуха, о радиационной безопасности, о санитарно-эпидемиологических требованиях, о безопасности пищи, о питьевой воде и пр.). Указанные нормы отличаются экологическим предназначением.

Второй вид определяет нормы законов профилактического содержания (об ограничениях табакокурения, о профилактике инфекционных болезней, о лечебных природных ресурсах, о предупреждении ВИЧ, о профилактике туберкулеза, о порядке обращения наркотиков, психотропных веществ, о спорте и физической культуре, о запретах рекламы табака, алкоголя и пр.). Положения этой группы характеризуются превентивной направленностью.

Третья категория законодательных предписаний сферы охраны здоровья, отраженные в Основах, – это нормы, которые определяют средства защиты прав граждан (о правах больных-пациентов, о защите потребительских прав, об особенностях рекламы оздоровительных услуг, лекарств и медицинских изделий и пр.). Обозначенная категория законодательных предписаний относится к правозащитным нормам.

Четвертый вид составляют статусные нормы о полномочиях, ответственности медицинских работников (соответствующие положения УК РФ, КоАП РФ, о страховании ответственности в профессиональной деятельности, о медицинской этике, о пенсиях медработников и т.д.).

Следующий вид образуют нормы законов, регулирующих формирование национальной системы российского здравоохранения, задачи ее элементов (о российском здравоохранении, о частной медицине, о подсистеме медицинских организаций, о подсистеме фармацевтики и пр.). Представленные положения можно обозначить как структурно-отраслевые нормы законов, образующих си-

стему российского законодательства в сфере здоровья.

Шестой вид формируют нормы законов о финансировании российской системы здравоохранения (о системе медицинского страхования, о соответствующем сегменте государственного бюджета, о тарифах системы обязательного страхования и т.д.). Указанные нормы отличаются финансово-обеспечительным характером.

Седьмая категория законодательных предписаний сферы охраны здоровья, отраженные в Основах, – это нормы российского законодательства об отдельных видах деятельности сферы здравоохранения (о психиатрии, о трансплантации человеческих органов, тканей, о донорстве, о Красном Кресте и пр.) [14]. Положения этой группы характеризуются специальным или классификационно-отраслевым содержанием.

Несмотря на объемный характер обозначенных семи категорий норм сферы охраны здоровья, в Основах установлены только три правовых механизма привлечения к уголовной ответственности, связанные с нарушениями в сфере медицинской, фармацевтической деятельности:

- в положениях ч. 8 ст. 56 Основ обозначено наступление уголовной ответственности за незаконное осуществление аборта;
- в нормах ч. 7 ст. 69 Основ предусмотрена уголовная ответственность за незаконную медицинскую, фармацевтическую деятельность;
- содержание ст. 98 Основ определяет общую конструкцию привлечения к ответственности за правонарушения в сфере здоровья только специальных субъектов (органов власти, муниципалитетов, должностных лиц, работников организаций в медицинской и фармацевтической сферах деятельности).

В контексте уголовно-правовой защиты прав на здоровье стоит добавить, что требования п. 9 ч. 1 ст. 79 Основ, детализированные приказом Минздрава России № 664н от 2021 года [15], определяют обязанность компетентных субъектов здравоохранения информировать соответствующие подразделения внутренних дел о трех видах фактов:

- 1) о фактах поступления пациента с признаками причинения вреда его здоровью противоправными действиями;
- 2) о фактах поступления пациента, личность которого не может быть установлена;
- 3) о фактах смерти пациента с неустановленной личностью.

Обозначенная обязанность компетентных субъектов здравоохранения представляется одним из ключевых источников информации о признаках преступления против здоровья человека, которые отражены в ст. 6.1, 40.1, 40.2, 144, 148, 226.5 УПК РФ в качестве сообщений о преступлении, а в ст. 37, 39 УПК РФ обозначены предметом контроля (надзора) за ходом рассмотрения информации о преступлении. Наличие в Основах трех правовых механизмов привлечения к уголовной ответственности специальных субъектов медицинской, фармацевтической деятельности и обязанностей медработников направлять в органы внутренних дел сведения о признаках преступлениях против здоровья

человека характеризует неопределенность в части применения уголовной ответственности за преступления против здоровья. Такая неопределенность обусловлена формальным указанием в ч. 8 ст. 56, ч. 7 ст. 69, ст. 98 Основ видов уголовной ответственности в сфере охраны здоровья только с участием специальных субъектов и предопределяет важность дополнения Основ другими видами уголовной ответственности и соответствующими субъектами.

В этой связи предлагается дополнить ст. 98 Основ частью 5 следующего содержания: «5. В случае нарушения прав, свобод человека, связанных с его здоровьем, виновное лицо привлекается к ответственности согласно федеральному закону».

Исходя из вышеизложенного, можно выделить комплексный аспект развития уголовного российского законодательства об охране здоровья, который характеризуется: установлением в Основах [16] семи видов норм отраслевых законов, образующих систему российского законодательства в сфере здоровья (экологического, превентивного, правозащитного, статусного, структурного, финансового, специального содержания); наличием в Основах только трех правовых механизмов привлечения к уголовной ответственности специальных субъектов медицинской, фармацевтической деятельности; целесообразностью дополнения Основ другими видами уголовной ответственности в сфере здоровья.

С учетом конституционно-правовой значимости уголовного законодательства об охране здоровья и его комплексного содержания следует обратить внимание на различные подходы российских правоведов к понятию здоровья.

В частности, Ю.П. Лисицын отмечает, что в биологическом контексте здоровье определяется отсутствием у человека болезней (психических, соматических), дефектов организма и других патологий, ведущих к нарушению: социальной адаптации субъекта, управления функциями организма, энергетического баланса человека и т.д. [17].

Зарубежные исследователи во главе с Б. Тобес считают, что здоровье характеризуется не только отсутствием у человека болезней, но и наличием у него позитивного отношения к жизни, активного восприятия индивидом ответственности человека. Поэтому здоровье следует воспринимать комплексом физических, душевных и социальных аспектов состояния человека [18].

Схожее мнение о физическом, духовном, социальном свойствах здоровья отмечено в работах российских исследователей [19] и обобщено, как отмечалось выше, в преамбуле Устава ВОЗ как совокупного состояния полного социального, физического и душевного благополучия.

В этой связи стоит обратить внимание легальные дефиниции здоровья, охраны здоровья, обозначенные в ст. 2 Основ:

1) в соответствии с п. 1 ч. 1 ст. 2 Основ здоровье определено состоянием благополучия человека, которое характеризуется физическим, психическим, социальным содержанием, отсутствием заболеваний, расстройств функций систем организма и органов человека; что также отражает ключевые элементы здоровья физического, психического, социального содержания, при этом пси-

хофизическое содержание определяется актуальными показателями болезней, организма человека;

2) согласно п. 2 ч. 1 ст. 2 Основ охрана здоровья российских граждан установлена в качестве системы мер правового, социального, политического, научного, экономического, медицинского, санитарно-противоэпидемического, предупредительного характера, которые исполняются органами власти и муниципалитетами, другими субъектами в целях: сохранения, укрепления психического, физического здоровья человека, профилактики заболеваний, поддержания активной долголетней жизнедеятельности человека, предоставления медицинской помощи каждому нуждающемуся.

Как видно, дефиниция охраны здоровья отличается системным, межотраслевым и многоцелевым характером.

Стоит обратить внимание на содержании целей системы мер по охране здоровья, которые упускают обеспечительно-правовые вопросы уголовной и пр. ответственности за нарушение прав человека на здоровье, что уже отмечалось при анализе ст. 56, ст. 69, ст. 98 Основ.

То есть, из содержания ст. 2, 56, ст. 69, ст. 98 Основ следует, что российская система охраны права на здоровье не включает задачи, инструменты уголовной и пр. ответственности за посягательства на здоровье человека, кроме совершения преступлений медработниками и фармацевтами.

Помимо предложенного ранее изменения ст. 98 Основ, это предполагает соответствующее включение в п. 2 ч. 1 ст. 2 Основ охрана цели правового обеспечения системы мер охраны здоровья.

В этом отношении рекомендуется дополнить п. 2 ст. 2 Основ словами «... привлечения к ответственности лиц, виновных в нарушении прав, свобод человека, связанных с его здоровьем...».

Таким образом, понятие здоровье человека определяется тремя его составными элементами физического, психического и социального содержания.

При этом дефиниция охраны здоровья, как отмечено выше, отличается системным, межотраслевым и многоцелевым характером.

Из представленных тезисов также следует, что право на здоровье включает право на получение человеком от компетентных субъектов системы мер охраны здоровья правового, социального, политического, научного, экономического, медицинского, санитарно-противоэпидемического, предупредительного, целевого и обеспечительного содержания.

По данному поводу А.А. Белоусова логично аргументирует, что право человека на здоровье включает совокупность:

1) прав на лечение, поддержание здоровья человека мероприятиями сферы здравоохранения;

2) прав на обеспечение здоровья человека способами, средствами, установленными законом [20], которые в числе прочих предусматривают уголовно-правовую защиту здоровья россиян.

Уголовно-правовая охрана права на здоровье в рамках соответствующей

ответственности согласно норм УК РФ дифференцирована по степени вредных последствий для здоровья потерпевшего. Так в составах статей 111, 112, 115 УК РФ установлено наказание за умышленное нанесение соответственно тяжкого, среднего и легкого вреда здоровью потерпевшего.

Общие критерии установления степени нанесенного вреда здоровью обозначены в соответствующих Правилах, утвержденных постановлением Правительства РФ № 522 от 2007 года (далее – Правила [21]). В положениях в п. 2, 3 Правил приводится понятие вреда здоровью человека – это нарушение физиологической функции, анатомической целостности тканей и органов человека от внешнего воздействия психических, биологических, химических и физических факторов, которое классифицируется на тяжкий, средний, легкий вред с учетом двух признаков:

- квалифицирующих признаков физического, психического, функционально-социального характера, которые регламентированы нормами п. 4 Правил;
- медицинских (физических, психических) критериев установления тяжести вреда здоровью, которые утверждены приказом Минздравсоцразвития РФ № 194н от 2008 года (далее – Приказ [22]).

Обобщая приведенные тезисы, можно отметить регламентацию уголовно-правовой охраны человеческого права на здоровье нормами УК РФ в виде обеспечительных механизмов защиты такого права с учетом трех признаков здоровья физического, психического, социального свойства и дифференциации уголовной ответственности.

Физические признаки уголовно-правовой охраны права на здоровье, которые регулируются и дифференцируются нормами УК РФ, означают соответствующую степень вредных физических последствий для потерпевшего.

В частности, установленные в п. 4 Правил квалифицирующие физические признаки нанесения здоровью тяжкого вреда включают:

- потерю человеком слуха, зрения, речи;
- потерю потерпевшим какого-либо органа;
- утрата органом человека его обычных функций;
- прерывание у женщины беременности;
- заболевание потерпевшего токсикоманией, наркоманией;
- неисправимое обезображивание лица человека.

Согласно пп. 6.10 Приказа неисправимость обезображивания лица должна определяться судом, для этого эксперты подтверждают неисправимость полученного повреждения и формулируют его последствия по медицинским критериям, поскольку неисправимость повреждения лица человека отличается невозможностью их самостоятельного исчезновения без хирургического вмешательства.

Обозначенные в п. 4 Правил квалифицирующие физические признаки нанесения здоровью среднего и легкого вреда определяются: длительным и кратковременным расстройством человеческого здоровья.

Психические признаки уголовно-правовой охраны права на здоровье, ко-

торые регулируются и дифференцируются нормами УК РФ, означают соответствующую степень вредных психиатрических последствий для потерпевшего.

Предусмотренный п. 4 Правил квалифицирующие психический признак нанесения здоровью тяжкого вреда определяется наступлением у потерпевшего психического расстройства. В дополнение этой нормы в пп. 6.8 Приказа установлено, что возникновение у потерпевшего психического расстройства должно быть последствием причинения физического вреда его здоровью, что отражает объективную связь физических и психических признаков уголовно-правовой охраны права на здоровье.

Социальные критерии охраны права на здоровье, которые регулируются нормами УК РФ, означают высокий уровень вредных социальных последствий для потерпевшего, которые также классифицируются с учетом нанесения здоровью потерпевшего тяжкого, среднего, легкого вреда.

В этой связи, установленные в п. 4 Правил [21] квалифицирующие социальные признаки нанесения здоровью тяжкого вреда, составляют:

- признак стойкой значительной утраты общей трудоспособности человека на одну треть и более;
- признак полной утраты, имеющейся у потерпевшего профессиональной трудоспособности.

Согласно пп. 6.11 Приказа [22] признак стойкой значительной утраты общей трудоспособности человека на одну треть и более объективно связан с медицинскими (физическими) критериями, поскольку тяжкий вред человеческому здоровью имеет место при отдельных повреждениях:

- 1) закрытый, открытый перелом кости плеча: головки плеча (внутрисуставной перелом), анатомической шейки плеча (околосуставной перелом), диафиза или хирургической шейки кости плеч;
- 2) закрытый, открытый перелом кости, образующей локтевой сустав;
- 3) закрытый, открытый вывих-перелом кости предплечья;
- 4) компрессионный перелом от двух смежных позвонков поясничного либо грудного отдела позвоночника, который не нарушил функции тазовых органов, спинного мозга; и т.д.

В соответствии с пп. 6.12 Приказа [22] квалифицирующие социальные признаки полной утраты работником профессиональной трудоспособности определяются возможностью исполнения работы конкретного качества и объема в рамках определенной специальности (профессии), по условиям которой работник проводил основную для себя трудовую деятельность. При этом критерии степени утраты работником профессиональной трудоспособности устанавливаются по Правилам определения степени утраты работником трудоспособности [23].

В отношении взаимодействия рассматриваемых квалифицирующих признаков уголовно-правовой охраны здоровья человека стоит добавить, что тесная взаимосвязь трех квалифицирующих признаков здоровья физического, психического, социального свойства и соответствующей уголовной ответственно-

сти за нарушение права на здоровье отражена в нормах УК РФ.

Например, в диспозиции ч. 1 ст. 111 УК РФ в качестве элементов объективной стороны умышленного нанесения тяжкого вреда здоровью обозначены следующие признаки здоровья:

1) физические признаки: наступление опасности для жизни; потеря речи, зрения, слуха; потеря органа; утрата органом своих функций; прерывание беременности; неисправимое обезображивание лица человека;

2) психические признаки: приобретение психического расстройства, заболевание токсикоманией или наркоманией, поскольку эти болезни отличаются стойкой психической зависимостью от соответствующих препаратов [24];

3) социальные признаки: стойкая значительная утрата потерпевшим общей трудоспособности на треть или более; полная утрата работником профессиональной трудоспособности.

Приведенные тезисы позволяют сформулировать понятие уголовно-правовой охраны права человека на здоровье в России – это регламентированная нормами УК РФ система обеспечительных механизмов защиты права на здоровье, которые классифицируются с учетом трех взаимосвязанных признаков вреда здоровью физического, психического, социального свойства, детализируются медицинскими показателями и позволяют дифференцировать степень уголовной ответственности виновного по объему вредных последствий, наступивших для здоровья потерпевшего и другими критериям соответствующих составов преступлений.

Список источников

1. Устав (Конституция) Всемирной организации здравоохранения (ВОЗ) (принят в г. Нью-Йорке 22.07.1946, с изм. от 24.05.1973, вступил в силу для СССР 7 апреля 1948 года). [Электронный ресурс], URL: <https://docs.cntd.ru/document/901977493> (дата обращения 25.11.2024).

2. Всеобщая декларация прав человека (принята Генеральной Ассамблеей ООН 10.12.1948) // Российская газета. 10 дек. 1998 года.

3. Сведения сайта ООН о темах деклараций, конвенций. [Электронный ресурс], URL: https://www.un.org/ru/documents/decl_conv/convtheme.shtml (дата обращения 24.11.2024).

4. Минимальные стандартные правила Организации Объединенных Наций, касающиеся отправления правосудия в отношении несовершеннолетних (Пекинские правила) (приняты 29.11.1985 Резолюцией 40/33 на 96-ом пленарном заседании Генеральной Ассамблеи ООН), [Электронный ресурс], URL: http://www.un.org/ru/documents/decl_conv/conventions/beijing_rules.shtml (дата обращения 25.11.2024).

5. Российское уголовное право. Особенная часть / Под ред. М. П. Журавлева, С. И. Никулина. 3-е изд. М., 2014. С. 20.

6. Кашепов В.П. О гарантиях уголовно-правовой защиты безопасности

личности // Журнал российского права. 2005. № 12. С. 105-118.

7. Бимбинов А.А. Некоторые проблемы квалификации насильственных преступлений против сексуальной свободы личности (статьи 131-132 УК РФ) / А.А. Бимбинов, В.Н. Воронин // Вопросы безопасности. 2018. № 6. С. 9-16; Лопатин В.А. Проблемы квалификации насильственных преступлений / В.А. Лопатин, С.А. Дробот // Фундаментальные и прикладные аспекты развития современной науки. Сборник научных статей по материалам III Международной научно-практической конференции. Уфа, 2020. С. 83-88; Мартыненко Н.Э. Уголовно-правовое обеспечение безопасности личности в Российской Федерации // Публичное и частное право. 2010. № 2 (6). С. 75-79; Шикун И.Р. Уголовно-правовые средства обеспечения безопасности личности потерпевшего от преступного посягательства против жизни и здоровья // Преступность и общество. Москва, 2010. С. 174-178; и др.

8. Федеральный закон от 28.12.2010 № 390-ФЗ (ред. от 28.04.2023) «О безопасности» // Собрание законодательства РФ. 2011. № 1. Ст. 2.

9. Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» // Собрание законодательства РФ. 2021. № 27 (часть II). Ст. 5351.

10. Винокуров В.А. Проблемы реализации правовых норм при вакцинации в условиях чрезвычайной ситуации или повышенной готовности // Медицинское право. 2021. № 5. С. 3 - 10.

11. Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» // Собрание законодательства РФ. 2021. № 27 (часть II). Ст. 5351.

12. Федеральный закон от 21.11.2011 № 323-ФЗ (ред. от 28.04.2023) «Об основах охраны здоровья граждан в Российской Федерации» // Собрание законодательства РФ. 2011. № 48. Ст. 6724.

13. Герасименко Н.Ф. Законодательное обеспечение охраны здоровья граждан Российской Федерации // Ремедиум. Журнал о российском рынке лекарств и медицинской технике. № 7-8, 2003. С. 44-48.

14. Герасименко Н.Ф. Законодательное обеспечение охраны здоровья граждан Российской Федерации // Ремедиум. Журнал о российском рынке лекарств и медицинской технике. № 7-8, 2003. С. 44-48.

15. Приказ Минздрава России от 24.06.2021 № 664н «Об утверждении Порядка информирования медицинскими организациями органов внутренних дел в случаях, установленных пунктом 5 части 4 статьи 13 Федерального закона «Об основах охраны здоровья граждан в Российской Федерации» [Электронный ресурс], URL: <https://www.consultant.ru/cons/cgi/online> (дата обращения 24.11.2024).

16. Федеральный закон от 21.11.2011 № 323-ФЗ (ред. от 28.04.2023) «Об основах охраны здоровья граждан в Российской Федерации» // Собрание законодательства РФ. 2011. № 48. Ст. 6724.

17. Лисицын, Ю.П. Общественное здоровье и здравоохранение: учебник /

Ю.П. Лисицын. - 2-е изд. -М.: ГЭОТАР-Медиа, 2010. С. 29.

18. Тобес Б. Право на здоровье: Теория и практика / Б. Тобес, А. Кэмпбэлл, Г. Джиллет, Г. Джонс. Пер.: М. Кротов, Я. Кротов, Л. Корнелиус. М.: Устойчивый мир, 2001. С. 56.

19. Дорина В.В. Понятие и структура права на охрану здоровья в международном праве // Вестник Полоцкого государственного университета. Серия D. Экономические и юридические науки. № 5, 2019. С. 149-156; Капралова Е.В. Конституционное право на охрану здоровья: его содержание и законодательное обеспечение / Е.В. Капралова, Е.С. Сергеева // Вестн. Нижегород. гос. ун-та им. Лобачевского. 2011. № 1. С. 295-302; Комарова В.В. Социальная государственность России и право на охрану здоровья, медицинскую помощь // Право и государство: теория и практика. - М.: Право и государство пресс, 2014, № 2 (110). С. 32-38.

20. Белоусова, А.А. Право на здоровье в современном международном праве: автореф. дис. ... канд. юрид. наук: 12.00.10 / Белоусова Анастасия Александровна. Москва, 2015. 25 с.

21. Постановление Правительства РФ от 17.08.2007 № 522 (ред. от 17.11.2011) "Об утверждении Правил определения степени тяжести вреда, причиненного здоровью человека" // Собрание законодательства РФ. 2007. № 35. Ст. 4308.

22. Приказ Минздравсоцразвития РФ от 24.04.2008 № 194н (ред. от 18.01.2012) «Об утверждении Медицинских критериев определения степени тяжести вреда, причиненного здоровью человека» // Российская газета. №188, 5 сент. 2008 года.

23. Постановление Правительства РФ от 16.10.2000 № 789 (ред. от 24.03.2023) «Об утверждении Правил установления степени утраты профессиональной трудоспособности в результате несчастных случаев на производстве и профессиональных заболеваний» // Собрание законодательства РФ. № 43. 2000. Ст. 4247.

24. Божченко А.П. К вопросу о правилах и медицинских критериях определения тяжести вреда, причиненного здоровью человека // Медицинское право. 2022. N 2. С. 32 - 38; N 3. С. 3 – 8; Мохов А.А. Психическое здоровье как феномен // Медицинское право. 2019. № 1. С. 3 – 9.

УДК: 336.025

ГЛАВА 4. ПРОБЛЕМЫ ЭФФЕКТИВНОСТИ УПРАВЛЕНИЯ ФИНАНСОВОЙ СИСТЕМОЙ В УСЛОВИЯХ ИННОВАЦИОННОГО РАЗВИТИЯ ЭКОНОМИКИ

Зайналов Жахонгир Расулович

д.э.н., профессор,
Самаркандский институт экономики и сервиса

Аннотация: в данной главе рассматривается эффективность управления финансовой системой в условиях инновационного развития экономики Узбекистана, дается развитие сферы финансов Узбекистана на различных этапах и рассматриваются эти этапы с позиции огромных перемен вследствие проведенных реформ в сфере банков, денежной системы, налогов, бюджета, инноваций и т.д., которые в целом полностью вывели финансовую систему Республики на новую основу, связанную с новыми рыночными преобразованиями.

Даются конкретные предложения по улучшению финансового состояния предприятий, в этом ракурсе выявляется, что результат этих хозяйствующих субъектов является определяющим в обеспечении стабильности роста финансового потенциала административно-экономической территории Узбекистана.

Ключевые слова: финансовый механизм, эффективность, финансовая политика, ситуация, мобилизация бюджетных средств, малые предприятия, налоговая нагрузка, задолженность, финансовые ресурсы, денежные средства населения, источник оборотного капитала.

EFFICIENCY CHALLENGES IN MANAGING THE FINANCIAL SYSTEM AMID INNOVATIVE ECONOMIC DEVELOPMENT

Zaynalov Jahongir Rasulovich

Abstract: The article examines the efficiency of managing the financial system amid the innovative economic development of Uzbekistan. It explores the evolution of Uzbekistan's financial sector at various stages, analysing these stages from the perspective of significant changes driven by reforms in banking, monetary systems, taxation, budgeting, and innovations. These reforms have fundamentally restructured the country's financial system, aligning it with new market transformations.

Specific proposals are provided to improve the financial performance of enterprises, highlighting that the outcomes of these economic entities are crucial in ensuring stable growth in the financial potential of Uzbekistan's administrative-economic regions.

Keywords: financial mechanism, efficiency, financial policy, situation, mobilization of budgetary funds, small enterprises, tax burden, debt, financial resources, household funds, working capital sources.

Актуальность темы исследования. Социально-экономическая жизнь общества в условиях инновационного развития зависима от множества факторов, степень их влияния и смягчения во многом опирается на методы государственного регулирования (МГР). Подобные методы в течение 2010-2016 годов были положены в основу финансовой политики. В этот период в значительной степени, если акцент был сделан на финансовые инструменты регулирования финансовой политики, то, начиная с 2017 года до 2022 года, опираясь на это, приоритетным направлением стало бюджетно-целевое, денежно-кредитное регулирование. Министерством финансов и Центральным Банком Республики Узбекистан, как субъектами финансового оздоровления экономики, начиная с 2022 года субъектам финансовой, денежно-кредитной политики было оглашено обеспечение стабильности развития хозяйствующих субъектов экономики. Как следует из сказанного, можно сказать, что произошла смена акцентов на финансовые механизмы регулирования не только бюджетно-налоговых, денежно-кредитных отношений, но и формирования и распределения финансовых ресурсов хозяйствующих субъектов. Итак, ныне в условиях Нового Узбекистана сложилась развитая система регулирования финансовых отношений. Отсюда вывод – существовавшие до 2021 года механизмы регулирования финансовых отношений подвергались сильному изменению, потому что применявшиеся методы государственного финансового регулирования до 2017 года могли бы привести к обострению и без того рискованных (т.е. безнадежных) явлений в хозяйстве. На основе изучения правительственных документов и материалов отечественной литературы и печати легко можно прийти к выводу о том, что скоропалительные решения в рамках смягчения размеров налоговой ставки привели к формированию научно необоснованных границ всех видов налогов с сиюминутным изменением цен во всем, беспочвенному ограничению размеров кредитов, предоставляемых на льготных условиях малым предприятиям, что означало трудности при принятии эффективных бюджетно-налоговых решений, что оказало сильное влияние на финансовые отношения хозяйствующих субъектов, падение производства, экспорта, торможение падения инфляции и многое другое. Все это не столько определило ход стратегии реформ, как привело к непрозрачной финансовой ситуации, характеризующейся отходом от рыночных рецептов регулирования финансовой системы в целом, ослаблением активного участия государства в управлении и широким внедрением форм эффективной системы управления финансами с элементами теории предложения и рациональных ожиданий.

Непоследовательность действий в принятии решений, косвенные ошибки в формировании инновационных механизмов формирования финансовых ресурсов до принятия государственной программы стратегии развития перехода к новой системе хозяйствования были обусловлены отсутствием программы «оживления» и «инновационного обновления» рыночного хозяйства, направленной на определение развития финансовых отношений в Республике Узбекистан, особенно в условиях выбора пути Нового Узбекистана. В связи с этим

вполне обоснованным является то, что общество в значительной степени не было подготовленным к восприятию самого термина «новой» системы, также произошло существенное снижение регулирующей роли государства, ограниченной только незначительными решениями в целях сдерживания роста цен и инфляции в сочетании с созданием дополнительных рабочих мест.

Исходя из принятых в экономической литературе концепций в рамках многофакторной природы развития сферы финансов Узбекистана, можно столкнуться с факториально-аналитическими материалами достаточно многих экономистов, таких как Т.С.Маликов [8], О.О.Олимжонов [8], Ш.А.Тошматов [14], и др., специалистов, работающих в государственных органах управления. В их научных трудах даны реформенные этапы и отмечается, что на каждом реформенном этапе решались, якобы, задачи в рамках отечественной экономики. При этом особое внимание ими уделялось факторам, приводящим или способствующим проведению реформы, в частности, налогово-бюджетной системы. При этом они упускали из виду, что важным реформенным фактором, приводящим к развитию финансовой системы и механизмов эффективности управления ими, являлось создание эффективных механизмов управления финансовыми ресурсами, находившихся долгие годы под влиянием «импортируемой» извне инфляции, которая представляет собой одну из самых сложных проблем проведения эффективной политики.

Несмотря на частые упоминания о количестве этапов развития финансовой науки в широком смысле слова в различной научной литературе, необходимость проведения преобразования финансовых отношений, его сущностные аспекты, роль и место в инновационном развитии экономики почти не раскрыты. Ряд ученых – А.Маршалл [9], П.Друкер [7], Б. Твисс [13], Р.А.Фатхудинов [15], С. Воронин [5], Т.С.Маликов [8], И.А.Майбурова [11], Ш.Тошматов [8], А.Мусагалиев [10], С.С.Алиева [4] и др. в контексте инновационного развития экономики делают правильные выводы, что сочетание финансовых механизмов финансовых отношений и эффективности управления ими оказывает благоприятное воздействие на величину производства, но не в состоянии решать острейшие проблемы выхода из критических ситуаций по преодолению инфляции, безработицы и др.

Отдельные экономисты как, напр., С.Воронин [5], напротив, ограничивают или сужают роль инструментов финансово-экономического механизма в рамках микроэкономики. В конечном итоге в своих научных трудах они приходят к выводу, что в целом регулирующие механизмы эффективности управления финансовой системой предполагают, что развитие любого процесса, напр. инвестиционного, модернизационного, реструктуризационного и т.п., на предприятиях ведет к их развитию и росту, что в перспективе обеспечит рост ВВП при помощи налоговых выплат, сокращение безработицы, улучшение инвестиционной привлекательности административно-экономических территорий в целом.

Ряд вышеуказанных экономистов считают, что каждый процесс (т.е. инвестиционный, производственный, модернизационный и т.п.) способен влиять

при помощи налоговых льгот на развитие как финансовых отношений, так и на развитие финансово-хозяйственной деятельности предприятий. Однако право-подобный подход (или взгляды) значительно сужает социально-экономическую природу финансовых отношений и элементов финансового механизма управления, и последний не отражает ту среду, в которой происходит взаимосвязь между ресурсодателями и ресурсополучателями.

Финансовый ресурс и механизм его формирования и распределения в рамках взаимодействия предприятий, имеющих свободные ресурсы, и предприятий в них нуждающихся. Наряду с этим следует, что многие подходы к определению финансовых отношений имеют схожие взгляды, а, следовательно, имеют схожие недостатки, которые заключаются в сужении экономических границ финансово-денежных ресурсов в рамках этапов экономического развития. Каждый этап развития финансовых отношений и принимаемых решений будет подвергаться риску.

Значит, необходимость применения действенных способов эффективного управления финансовой системой должна быть обусловлена развитием масштабов производства инновационной продукции, укреплением хозяйственных структур и процессов и процессов на основе модернизации экономики и расширения инновационной деятельности предприятий, или инновационное развитие предприятия в рамках эффективного управления финансовыми отношениями должно рассматриваться как средство сглаживания и предотвращения рисков явлений, так как его расширение или сужение способно не только обеспечить потребность предприятий в финансовых ресурсах в ходе воспроизводственного цикла, но и оказывать активное воздействие на обеспечение стабильности и эффективности управления финансовой системой в целом в условиях инновационного развития отечественной экономики.

Наряду с этим уместно отметить значение реформистских этапов и, соответственно, принятых решений правительством с учетом каждого реформенного периода в единых рамках. Напр., этапы и принятые законодательные акты можно представить в рамках, то есть: 1991-1993; 1994-1996; 1997-2000 годами, а можно выделить этап от 1991 до 1995 года и после (1996-2000 годы), 2001-2007; 2008-2016 и 2017 и по настоящий период. А в некоторых законодательных актах эти периоды приводятся в другом формате. Напр., выделяются три этапа, т.е. 1997-2001 гг.; 2001-2006 гг. и 2005 г. и последующие годы [1].

Ныне новая методология построения финансовых отношений стала опираться на новые или на модернизированные финансовые отношения. Это объясняется изменениями принимаемых мер, позволяющих в полной мере ликвидировать финансовую несбалансированность госбюджета, более четко распределить финансовые ресурсы в пользу развития социальной сферы страны. При этом требуется новый подход, имеющий характер всеобщности, то есть применение ряда мер для критического анализа состояния дореформенной финансовой системы и использование достижений современной системы финансовых отношений. Разумеется, пользуясь лишь одним подходом, опираясь на зару-

бежный опыт регулирования финансовых отношений, нельзя будет устранить все причины, могущие тормозить развитие финансовых отношений. Но – это уже другая проблема, и ее решение зависит от эффективности использования иных элементов регулирования финансовых механизмов управления финансовой системой, включая и ее оценку. Но это еще не говорит о том, что до 2017 года правительственные решения по обеспечению стабильности были пущены на самотек. Здесь нет того, что часто заформализовывает многие начинания: стремление получения возможности отчитаться, подстегнуть события, происходившие в указанные периоды. Но те процессы, которые происходили в управлении финансами, четко были фиксированы, особенно менялась качественная характеристика финансовых отношений в рамках формирования и использования финансовых ресурсов, прежде всего, не только не только увеличилось количество предприятий вневедомственного статуса, не входящих в систему республиканских министерств и ведомств. Это – совместные предприятия с иностранными фирмами, ассоциации предприятий, предприятия, расположенные в экономической зоне. Однако перемены, которые произошли в структуре законодательных актов, привели к огромным переменам в сфере финансовых институтов. Перемены, все-таки, положительные перемены в этих сферах экономики вывели отечественную финансовую систему механизмов регулирования эффективности управления финансами на новый уровень, уровень с новым преобразованием всех хозяйствующих субъектов.

На современном этапе развития финансовых отношений нам надо признать, что ко всему этому необходима прочная финансовая система Узбекистана, где могут в совокупности действовать все финансовые инструментариумы для создания четкой и достаточно стабильной регламентации бюджета страны, мобилизации финансовых ресурсов в интересах их потребителей и государства в целом. Иначе мы еще долго не уйдем от косвенных диктатов ряда ведомств, которые под лозунгами государственных интересов до сих пор нередко решают свои собственные проблемы, зачастую с грубейшим попранием интересов предприятий и их работников. Все это приводит к большим финансовым потерям. В любых условиях предприятие должно иметь гарантированные условия для инновационных разработок, в т.ч. по секторам экономики, которые гарантировали бы мобилизацию собственных ресурсов, в том числе финансовых (см.: табл. 1).

Как следует из данных, приведенных в табл. 1, по всем секторам за 2018-2021 годы наблюдались положительные результаты. Имеется место, когда по отдельным секторам имеется рост в разы, в частности в государственном секторе, секторе высшего образования, а также в частном секторе. Лишь в рамках предпринимательского сектора в 2021 году наблюдалось снижение по отношению к 2020 году, но незначительное.

Признание исходности территориальной важности в обеспечении финансового потенциала однозначно может выделить не только местные бюджеты, но и формирование финансовых ресурсов страны. Хотя средства местных бюд-

жетов активно не стимулируют инновационное развитие хозяйствующих субъектов. Мало того, системы формирования и использования бюджетных средств практически являются неподготовленными к переходу к активным методам финансового регулирования взаимодействия с предприятиями по месту нахождения, не обеспечивая в необходимой степени финансирования предприятий, нуждающихся в инвестициях. Из-за недостаточности средств местных бюджетов они не стимулируют на требуемом уровне развитие предприятий, имеющих инновационную направленность. До сих пор механизм взаимосвязи между местным бюджетом и хозяйствующими субъектами не исследован достаточно глубоко. Следовательно совершенствование финансового механизма эффективного управления финансами должно привести, прежде всего, к активному вовлечению в финансовые связи предприятия и местный бюджет. Для полного развертывания и максимального упрощения условий их взаимосвязи требуется создать четкие критерии эффективного управления.

Таблица 1

Объем научно-исследовательских и опытно-конструкторских разработок, выполненных организациями по секторам деятельности [11]

(млн. сум.)

| Название секторов | 2018 | Доля к общему объему, в % | 2019 | Доля к общему объему, в % | 2020 | Доля к общему объему, в % | 2021 | Доля к общему объему, в % |
|------------------------|---------------|---------------------------|-----------------|---------------------------|-----------------|---------------------------|----------------|---------------------------|
| Всего | 680038 | 100 | 853404,4 | 100 | 992029,1 | 100 | 1069677 | 100 |
| в том числе: | | | | | | | | |
| государственный | 202061,4 | 29,7 | 314694,7 | 36,9 | 380808,7 | 38,4 | 395841 | 37,0 |
| предпринимательский | 414527,9 | 61,0 | 429183,7 | 50,3 | 480005,0 | 48,4 | 479907,4 | 44,9 |
| высшего образования | 431185,4 | 63,4 | 429183,7 | 50,3 | 480005 | 48,4 | 479907,4 | 44,9 |
| частный некоммерческий | 6070,2 | 0,9 | 2803,7 | 0,33 | 4744,7 | 0,5 | 9418,2 | 0,9 |

Намечая пути обеспечения эффективного управления финансовой системой, и в рамках этого финансового механизма необходимо иметь в виду, по крайней мере, два существенных момента: во-первых, минимальным требованием первых шагов должно стать создание условий для стабильного обеспечения бюджетно-налоговых отношений в целях обеспечения эффективности хозяйствования в сочетании с гарантией необходимости процесса финансирования инновационной деятельности; во-вторых, действие нового финансового механизма какое-то время должно иметь ограниченный характер и происходить одновременно с действием новой питательной средой, которой являются дефициты и дисбалансы в местных бюджетах.

Опираясь на подобную схему, модернизацию механизма эффективного

управления финансами можно будет вести по нескольким направлениям сразу: развертывание ресурсов местных бюджетов и большая гибкость финансирования инновационно развивающей деятельности предприятий; более широкое использование средств местных бюджетов с опорой на присущие им инновационные свойства; использование в различных формах финансирования из местного бюджета в целях укрепления финансовых отношений между местным бюджетом и предприятиями. В условиях Нового Узбекистана для совершенствования системы эффективного управления финансовой системой на местном уровне необходимо выбрать одно приоритетное направление и последовательно двигаться по нему.

Казалось бы, в очередной раз, прежде всего, следует повысить роль и «потенциал» местных бюджетов до границы, способной эффективно финансировать потребителей бюджетных средств и управлять этим процессом более эффективно. Однако в современных условиях постановка вопроса об эффективности управления финансами или развитии финансового механизма регулирования отношений между бюджетами разных уровней и нуждающихся в финансовой поддержке инновационно развивающихся предприятий должна стать более практичной, не уводить в сторону от решения действительно насущных и разрешаемых проблем. Она не должно игнорировать реальные финансовые условия. Нельзя больше требовать от местных бюджетов того, что само по себе не может выполняться без соответствующих финансово-экономических условий, без финансовых ресурсов, движение которых она должна опосредствовать.

Бесспорно, что бюджетный потенциал определяется сферой материального производства, насыщением рынка, конкурентоспособностью продукции (товара, услуги), степенью соответствия движения финансовых ресурсов, инвестиционных притоков и объемами экспорта. Местный бюджет может выполнять свои функции только при наличии соответствующей ресурсной базы и гарантированности ресурсного обеспечения на всех реформенных этапах развития экономики. Если этого не будет, то он начинает испытывать ресурсные недостатки.

Итак, с одной стороны взаимосвязи формирование через мобилизацию ресурсов с доходным поступлением и расходами и регулирование бюджетов всех уровней в целях стабилизации финансовых отношений между субъектами, нуждающихся в ресурсах бюджетов. К числу подобных субъектов можно отнести малые инновационно развивающие предприятия. Но финансовая поддержка их должна также находиться под постоянным контролем соответствующих финансовых органов управления.

Изменения в политике местных бюджетов, происходящие в настоящее время в Узбекистане, предусматривают результативность бюджетных расходов. Данный принцип должен присутствовать в финансовой деятельности хозяйствующих субъектов и бюджетной деятельности. При этом следует иметь в виду, что результативность всегда должна обеспечивать рост качественных показателей. Именно поступления обязательных платежей в бюджет должны решать

и неразрешенные проблемы, возникающие между хозяйствующими субъектами и государством.

Хозяйствующие субъекты, пользуясь большими налоговыми льготами, должны иметь низкий и средний коэффициент налоговой нагрузки по основному виду налога, т.е. налогу на прибыль (т.е. в рамках от 2 до 12 процентов), и дифференциация данной налоговой ставки в целом не должна приводить к негативным последствиям. Подтверждением этого может служить количество ликвидированных предприятий (организаций) по отраслям экономики. Напр., количество ликвидированных предприятий в 2022 году достигло 24130 единиц, это на 7250 единиц больше, чем в 2019 году (см. табл. 2). Безусловно, ликвидированные предприятия нанесли большой ущерб, включая основной платеж. В разрезе областей наибольшее число ликвидированных предприятий наблюдался в Самаркандской, Ташкентской, Ферганской, Андижанской областях (см.: табл. 2). Приведенные данные сказались на притоке обязательных платежей в бюджеты всех уровней.

Таблица 2

Количество ликвидированных предприятий и организаций по отраслям экономики Республики Узбекистан [12] (без дехканских и фермерских хозяйств, за январь-декабрь, ед.)

| Отрасли | Г о д ы | | | |
|---|---------|-------|-------|-------|
| | 2019 | 2020 | 2021 | 2022 |
| Всего, в том числе: | 16880 | 11547 | 48676 | 24130 |
| сельское, лесное и рыбное хозяйство | 1760 | 1331 | 5973 | 2796 |
| промышленность | 3062 | 1929 | 9604 | 4656 |
| строительство | 1717 | 1163 | 3992 | 1465 |
| торговля | 4666 | 3154 | 14670 | 8973 |
| перевозки и хранение | 676 | 414 | 1648 | 687 |
| услуги по проживанию и питанию | 1185 | 649 | 3777 | 1597 |
| информация и связь | 395 | 171 | 1287 | 394 |
| здравоохранение и предоставление социальных услуг | 186 | 122 | 465 | 287 |
| прочие виды | 3233 | 2614 | 7260 | 3275 |

По нашему мнению, бюджетный потенциал всех уровней должен предусмотреть реальные возможности – имеется в виду не только рост количества ликвидированных предприятий, но и фактической способности территорий, призванных использовать имеющиеся ресурсы и создать максимальный объем материальных благ и услуг.

Пути решения поставленных проблем. Известно, что Министерство экономики и финансов, согласно с соответствующими органами управления определяют финансовую политику относительно всех уровней экономики и хозяйствующих субъектов. Но возникает вопрос, где можно познакомиться со сборниками, где фиксируется подобная политика. Однако мельком отмечается

необходимость оперирования этой политикой. Отсюда – неразбериха и путаница в разработке тактических в рамках распределения финансовых ресурсов хозяйствующих субъектов. Последние на любом уровне управления от этого не имеют выгоды, хотя они являются важным для субъектов в области формирования финансовых ресурсов.

Чтобы предприятия могли добиваться результативного успеха во всем, им нужно учиться смотреть на финансовые отношения всех партнеров и механизмы эффективного управления финансовыми ресурсами с позиций механизма налогообложения, формирования и распределения прибыли, кредитного механизма, инвестиционного механизма и других.

При этом разнообразные направления финансовых отношений, на наш взгляд, должны действовать в более совершенной форме взаимосвязи с финансовой политикой (предприятий, административных территорий и в целом на уровне государства). Мы полагаем, что в этом вопросе гвоздь всех наших сегодняшних проблем в следующем: или мы будем строить финансовые отношения по вертикали методами, действовавшими на различных этапах реформирования финансов (т.е. до 2017 года), и продолжать топтаться на месте и тиражировать бестолковщину, или мы более активнее начинаем внедрять более совершенные сегменты финансовых отношений, отчисляя по обязательным платежам в разумных пределах средства и самостоятельно решая текущие тактические задачи производства и социальные вопросы в рамках хозяйствующих субъектов.

Научно-обоснованные предложения и рекомендации. Чтобы укрепить финансовый потенциал, требуется реализовать ряд мер по выявлению внутренних финансовых источников. Возрастанию значения эффективности предприятий в широком смысле слова следует уделять пристальное внимание.

Не ставя целью охватить проблему критерия эффективности во всей ее сложности и разносторонности, остановимся лишь на тех ее аспектах, которые, на наш взгляд непосредственно связаны с функционированием и развитием механизма стимулирования. Это, прежде всего, понимание содержания критерия эффективности, его количественного выражения на разных уровнях иерархической структуры управления и в связи с возможностью и необходимостью оптимизации развития механизма стимулирования, выявления особенностей критерия эффективности инновации (и механизма его стимулирования). Но у механизма стимулирования есть свой аспект воздействия на конечные результаты. Если эффективное управление финансами определяет конечную цель – результативность и направление ее достижения, то механизм стимулирования предопределяет выбор и превращение в действительность тех возможностей по достижению цели, которые больше всего будут соответствовать этапу развития, осуществляя это путем изменения состава используемых ресурсов, устранения противоречивых явлений и т.п. В результате финансовый механизм стимулирования может оказать регулирующее влияние на достижение конечных результатов.

Как бы то ни было, критерий эффективности находится одновременно под воздействием двух групп факторов: факторов, определяющих результат, и затратных факторов. Это объясняется тем, что в нем проявляется взаимодействие результатов и затрат. Они по своей природе являются компонентами эффективности. Поэтому мы должны искать их на тех предприятиях, деятельность которых связана с формированием бюджетного потенциала административно-экономической территории. Или при помощи концентрации средств с последующим направлением их на удовлетворение интересов как хозяйствующих субъектов и населения, так и государства.

Отсюда следует, что критерий выявления показателя эффективности расходов возможно определить лишь путем обеспечения единства в требовании: максимизация финансового результата при минимизации затрат – в контексте формирования или концентрации финансовых ресурсов для достижения конкретной цели. Это означает обеспечение тесной связи экономики и финансов и взаимодействие их во всех уровнях деятельности хозяйствующих субъектов.

В начальный этап стабилизации экономики Нового Узбекистана, вставшего на этот путь после принятия Программы стратегии развития страны (на 2017-2021 годы), возникли проблемы по обеспечению минимизации затрат как задача-минимум. Однако при этом возникает вопрос, когда обеспечить максимум результата и когда – минимум затрат? На наш взгляд, последнее рекомендуется применить в ситуации тогда, когда нет особой нужды удовлетворять данные потребности. Это приносит возрастающий эффект. Лишь тогда можно будет сформулировать задачу-максимум. Сегодня ставится задача обеспечения эффективности деятельности предприятий.

Для этого нам необходимо сформировать задачу – минимум затрат при максимуме экономии затрат от внедрения инновационной техники. Конечный эффект от инновации должен определяться той экономией финансовых средств, которая будет получена на предприятиях-потребителях этой продукции, а критерий эффективности финансового механизма стимулирования инновации должен совпадать с критериями эффективности от инновации. Данный подход также должен быть положен в основу выбора критерия оптимальности механизма стимулирования инновации, обусловленного характером конечного результата.

Ожидаемый экономический эффект. К новым условиям хозяйствования в связи с действием многообразных подзаконных актов по-разному влияют на деятельность предприятий, а это приводит к адаптации их к новым условиям с различными результативными показателями. Это не мешает им быть конкретно-способными или малоэффективными.

Однако предприятия, оказавшись в кризисной ситуации, не могут быстро выпрямиться, опираясь на свои ресурсы, они нуждаются в финансово-кредитной поддержке. Поэтому выявление причин убыточности, нестабильности развития, роста финансовых затрат и выявление финансового потенциала как административно-экономической территории, так и предприятий, находя-

щихся на этой территории, является архиважным для разработки мер по преодолению причинных факторов, могущих тормозить максимизацию объемов деятельности, обеспечение высокой рентабельности и минимизации затрат. Для достижения высокой результативности необходимо и важно быстро перейти на внедрение инновационных технологий, способных обеспечить многогранное повышение результативности предприятий, снижение неэффективных видов затрат и повышение фондоотдачи.

Отсюда необходимость в анализе причин, приводящих к нестабильности развития. Поэтому всемерное повышение результативности должно быть в центре финансовой политики предприятий. Финансовая политика предприятия должна быть направлена на изучение и анализ состояния финансово-хозяйственной деятельности предприятий Республики Узбекистан. В связи с этим при анализе состояния предприятия необходимо уделять внимание состоянию собственного капитала предприятий. Касаясь последнего, следует отметить, что на 1 января 2023 года в сравнении с 2019 годом, как ни странно, собственный капитал уменьшился. Изменился уставной фонд предприятий в разрезе многих территорий Узбекистана, численность малых предприятий увеличилась до 63442 единиц (см.: рис. 1).

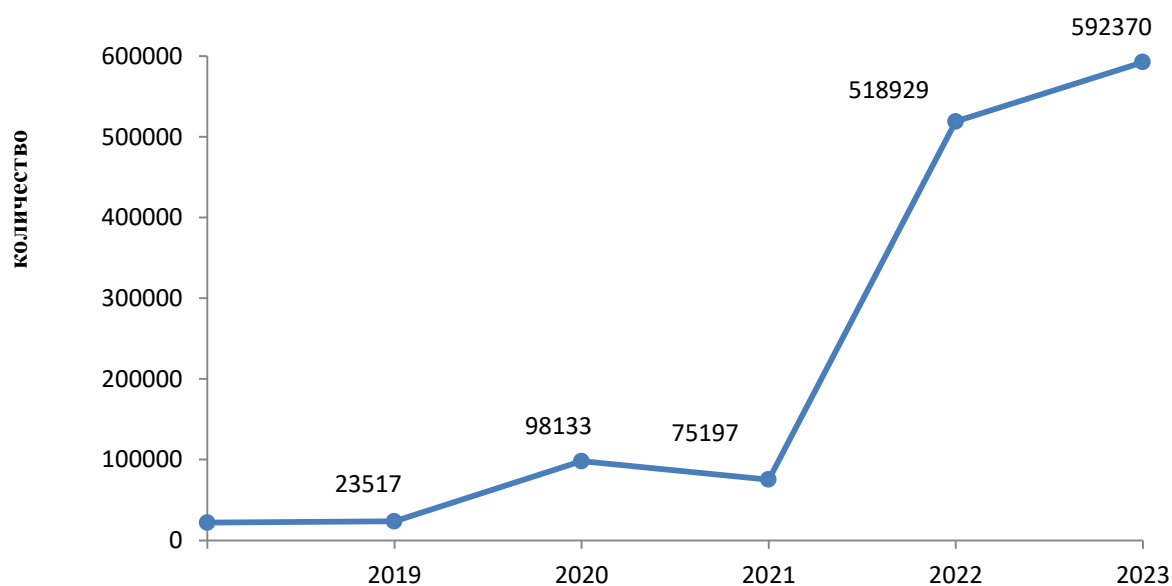


Рис.1. Количество действующих предприятий и организаций по административно-экономическим территориям Республики Узбекистан [12] (без дехканских и фермерских хозяйств по состоянию на 1 января, в ед.)

Количество ликвидированных предприятий и организаций по отраслям экономики – 24546 единиц. От этого потерял и бюджет всех уровней.

Причины этого, на наш взгляд, кроются в недостаточности финансовых ресурсов и неэффективности их управления.

Недостаток собственных ресурсов, безусловно, приводит предприятия к неэффективному использованию финансовых ресурсов и пополнению их путем привлечения свободных денежных средств населения. Привлечение свободных денежных средств населения является наиболее эффективным по сравнению с другими источниками, в частности, банковскими. Но данный финансовый источник должен стать действенным и более оперативно выполнять свои обязательства перед клиентом.

Здесь главной задачей должно быть завоевание доверия клиентов – потребителей продукции предприятий, что требует, на наш взгляд, совершенствования порядка привлечения свободных денежных средств населения и выдача по ним так называемого процента (дивиденда). Именно свободные средства населения в перспективе должно стать важным источником формирования оборотного капитала предприятий в необходимых размерах, то есть в объеме, достаточном для налаживания и эффективного ведения деятельности, и тем самым обеспечить стабильные поступления притока денежных средств от обязательных платежей в доходы бюджета, способствуя укреплению финансового потенциала административно-экономической территории как на нынешнем этапе, так и в обозримой перспективе.

На наш взгляд, в перспективе преодолеть все сложности возможно при использовании на практике стратегические и текущие механизмы регулирования и современные методы эффективного управления финансовой системой, разработанные в мире для макроэкономического уровня с учетом специфики и особенностей отечественной системы финансового управления.

Список источников

1. Закон Республики Узбекистан №464-1 «Об образовании» от 29.08.1997. (утратил силу)
2. Бюджетный кодекс Республики Узбекистан. <https://Lex.uz/docs-2304138>.
3. Налоговый кодекс Республики Узбекистан. <https://Lex.uz/docs-4674902>.
4. Алиева С.С. Совершенствование формирования и распределения прибыли предприятий в условиях модернизации экономики (на примере предприятий Самаркандской области). Автореф. дисс. на соиск. учен. степени к.э.н.-Т.:БФА, 2011.- 26 с.
5. Воронин С. Основные направления оптимизации налогообложения для предпринимателей розничной торговли / Справочник финансового работника. № 4(124). 2022.- С. 66-74.
6. Государственная программа стратегии социально-экономического развития страны на 2017-2021 годы.
7. Друкер П., Питер Ф. Эффективное управление предприятием: Пер. с англ.- М.: ООО «ИД Вильямс», 2008.- 214 с.

8. Маликов Т.С., Олимжонов О. Молия. Дарслик.- Т.: Иқтисод-молия, 2019.- 920 б.
9. Маршалл А. Принципы экономической науки. В 3-х т., Т. 3.- пер с англ.- М.: Прогресс, 1984.
10. Мусагалиев А.Ж. Роль налоговых механизмов в формировании доходов бюджета Республики Каракалпакстан. Монография.- Нукус: Билим, 2020.- 180 с.
11. Налоговые реформы: Теория и практика. Учебник. Под ред. И.А.Майбурова, Ю.Б.Ивекова.- М.: ЮНИТИ-ДАНА, 2015.- 463 с.
12. Наука и инновационная деятельность в Узбекистане за 2018-2021 годы.- Т.: Агентство статистики при Президенте Республики Узбекистан, 2022.- 136 с.
13. Твисс Б. Управление нововведениями / Б. Твисс. - М.: Экономика, 2009. - 272 с.
14. Тошматов Ш. Корхоналарни ривожлантиришида солиқлар роли. Монография.- Т.: Фан ва технология, 2008.- 204 б.
15. Фатхутдинов Р.А. Инновационный менеджмент.- СПб: Питер, 2003.- 400 с.

УДК 339.9

ГЛАВА 5. ПЕРСПЕКТИВЫ РАЗВИТИЯ ЕВРАЗИЙСКОЙ ИНТЕГРАЦИИ В КОНТЕКСТЕ ВСТУПЛЕНИЯ ТАДЖИКИСТАНА В ЕАЭС

Блиничкина Надежда Юрьевнад.э.н., профессор кафедры экономической теории
ФГАОУ ВО «Самарский государственный экономический университет»

Аннотация: Изменение системы мирохозяйственных связей и мировых товаропотоков ведет к необходимости переоценки существующих интеграционных связей и поиска путей дальнейшего развития интеграционных объединений как способа обеспечения экономической безопасности участников. Присоединение Таджикистана представляется перспективным направлением развития ЕАЭС. Однако анализ показал, что ввиду внутренних экономических особенностей республика не готова к полноценной интеграции, но может рассматриваться как перспективный стратегический партнер для ЕАЭС.

Ключевые слова: международная интеграция, национальная безопасность, внешнеэкономическая деятельность, национальные экономические интересы, внешняя торговля.

PROSPECTS FOR THE DEVELOPMENT OF EURASIAN INTEGRATION IN THE CONTEXT OF TAJIKISTAN'S ACCESSION TO THE EAEU

Blinichkina Nadezhda Yurievna

Abstract: The change in the system of global economic relations and global commodity flows leads to the need to reassess existing integration ties and find ways to further develop integration associations as a way to ensure the economic security of participants. The accession of Tajikistan seems to be a promising direction for the development of the EAEU. However, the analysis showed that due to internal economic characteristics, the republic is not ready for full integration, but can be considered as a promising strategic partner for the EAEU.

Keywords: international integration, national security, foreign economic activity, national economic interests, foreign trade.

Развитие международной торговли и формирование глобальных цепочек стоимости создает предпосылки для образования союзов государств в самой различной форме, начиная с традиционных двухсторонних соглашений, предусматривающих взаимные льготы и обязательства, соответствующие совместным интересам, вплоть до возникновения интеграционных межгосударственных объединений, ставящих перед собой различные цели и основанных на различных форматах сотрудничества.

Специалисты, занимающиеся исследованием феномена интеграции, с од-

ной стороны, отмечают объективный характер данного процесса, поскольку он является закономерным следствием сближения и взаимопроникновения экономик различных стран, основанных на углублении международного разделения труда [1, с. 23].

С другой стороны, также не может остаться не отмеченным особый характер подобных взаимоотношений, которые Обуховский В. В. называет «диалектически противоречивым единством объективных и субъективных процессов» [2, с. 41], тем самым подчеркивая факт сложности и неоднозначности интеграционных отношений.

В связи с этим, прежде чем рассматривать перспективы присоединения отдельной страны к какому-либо интеграционному объединению, необходимо выделить те факторы, которые могут служить стимулом для данного процесса, а также факторы, заставляющие руководство страны принимать решение не в пользу интеграции.

Базовая теория неолиберализма видит основной предпосылкой интеграции необходимость устранения противоречия между развитием международной торговли, обеспечивающей рост ВВП и доходов населения, и системой протекционистских барьеров, становящейся непреодолимым препятствием на этом пути [2, с. 30].

Из этого следует, что интеграция является следствием преобладания одной категории государственных интересов, связанных с развитием экономики в целом, над другой категорией, охватывающей вопросы защиты интересов отдельных производителей.

Следующим моментом, заслуживающим упоминания в контексте выделения предпосылок для интеграции государств, является их стремление к повышению собственной конкурентоспособности на мировой арене. Если крупные экономики способны создать соответствующие условия для собственного экономического развития самостоятельно, то относительно небольшие хозяйственные системы не обладают в отдельности соответствующим потенциалом. В этих условиях предоставление ими взаимных льгот позволяет сформировать относительно привилегированное положение и обеспечить преимущества в международной конкурентной борьбе.

Еще одной предпосылкой межгосударственной интеграции, отмечаемой в научной литературе, является необходимость разрешения различных международных противоречий, а в некоторых случаях – прямых конфликтов [3, с. 591]. Ярким примером такой интеграции служит возникновение Шанхайской организации сотрудничества, изначальной задачей которой являлось решение спорных вопросов в отношении государственных границ сопредельных стран, возникших после распада Советского Союза. Данная организация в итоге оказалась достаточно удобным форматом для обсуждения проектов сотрудничества в самых разных сферах, не принуждая при этом участников к жесткому соблюдению каких-либо требований, не являющихся следствием добровольно взятых на себя обязательств и противоречащих интересам отдельных участников.

Однако предпосылки международной интеграции не ограничиваются исключительно экономическими интересами участников. В исследовании Обухова А. А. отмечается, что самыми успешными оказались те объединения, которые возникали под воздействием внешней военной угрозы, примером чему могут служить и такие древнейшие интеграционные союзы как коалиция греческих полисов, и современный Европейский союз [4, с. 78].

Похожие тезисы встречаются в работе китайского ученого Вана Ябина, который говорит о возрастаниях угроз экономической безопасности для большинства государств мира под воздействием нарастающего противостояния и активного ведения экономических войн [5, с. 26].

Последний фактор представляется основной движущей силой трансформации межгосударственных интеграционных объединений на современном этапе.

В определенном смысле развитие мировой хозяйственной системы зашло в тупик. Согласно теории трансформации экономических систем, подобное положение не может сохраняться на протяжении длительного времени, поскольку формирует множественные угрозы для стабильности и естественного эволюционного процесса. Единственный выход в данном случае видится в нарастании революционных тенденций, имеющих своей целью создание новых условий для развития, в большей мере соответствующих сложившимся условиям хозяйствования и отвечающим интересам основных субъектов.

В качестве тех факторов, которые ведут развитие международных отношений в тупик, могут быть выделены нарастающая неопределенность во внешне-торговых отношениях, являющаяся следствием как таких объективных процессов как пандемия коронавирусной инфекции, так и субъективных действий США и Западных стран, усиливающих свое давление на все мировое сообщество в рамках ведущихся экономических войн [1, с. 25].

Очевидным выходом для многих государств в данных условиях является формирование независимых интеграционных объединений, в которых будет отсутствовать подобный внутренний дестабилизирующий фактор и которые за счет объединения экономической и политической мощи участников смогут стать своеобразной защитой от внешних угроз и позволят перераспределить и снизить риски осуществления международной торговли в рамках текущего нестабильного положения.

На этом фоне вполне закономерным представляется предположение об образовании евразийского социально-экономического пространства, способного противостоять угрозам международной экономической безопасности [6, с. 16].

Однако этот процесс оказывается несколько затруднен ввиду сохраняющейся в странах постсоветского пространства тенденции к поиску самоидентичности и усилению независимости [7, с. 178]. Данная тенденция зачастую приводит к тому, что руководство отдельных стран принимает решения не в пользу интеграции, опасаясь оказаться в зависимости от партнеров.

Помимо сказанного следует отметить, что интеграция не может начаться

там, где изначально отсутствует база для ее реализации, включающая наличие общих исторических и культурных элементов и уже частично сформировавшихся тесных экономических отношений [4, с. 79]. При отсутствии такой базы попытка интеграции не будет являться естественным следствием экономических и политических процессов, а окажется полностью искусственным явлением, которое вызовет отторжение в социально-экономических системах интегрирующихся государств.

Обобщая сказанное, можно выделить следующие предпосылки для успешной экономической интеграции стран:

- наличие общности экономических интересов;
- возможность повышения конкурентоспособности собственной экономики на мировой арене;

- наличие внешней угрозы, как экономической, так и политической;
- возрастающая нестабильность мировой хозяйственной системы.

Вместе с тем очевидными препятствиями для интеграции служат:

- отсутствие очевидной выгоды для государства от его вступления в интеграционное объединение;

- отсутствие изначальных точек соприкосновения, обеспечиваемых историко-культурной общностью;

- опасение утраты независимости в рамках объединения.

В контексте выделенных факторов могут быть рассмотрены перспективы интеграции Республики Таджикистан в ЕАЭС (Евразийский экономический союз), который является сегодня наиболее стабильным экономическим объединением, нацеленным на развитие международной торговли, защиту экономических интересов его участников и формирование зоны стабильности экономических отношений в мировом хозяйстве.

Присоединение Таджикистана к союзу представляет для ЕАЭС определенный интерес, затрагивающий как чисто экономические, так и геополитические вопросы.

Экономические интересы стран-членов ЕАЭС заключаются, прежде всего, в расширении общего рынка, что позволит нарастить объемы производства и простимулирует рост ВВП. Кроме того, определенный интерес представляет возможность получения доступа к природным ресурсам Таджикистана на льготных условиях, среди которых помимо ряда цветных и драгоценных металлов следует отметить такой стратегический ресурс для обороны и энергетики как залежи урана.

Еще одним фактором, способным вызвать заинтересованность ЕАЭС в привлечении Таджикистана в союз, являются в полной мере сложившиеся и достаточно развитые пути транспортировки товаров из Ирана, Турции и Арабских стран.

Существенное значение имеют также геополитические факторы, которые вынуждают такие государства как Китай, США, Турция и Иран стремиться к усилению своего влияния в Центральной Азии за счет увеличения присутствия

в Таджикистане, в том числе и через расширение торговых отношений. Подобные перспективы представляют непосредственную угрозу для государственных интересов участников ЕАЭС, прежде всего, Казахстана, Кыргызстана и России, поэтому вовлечение Республики Таджикистан в союз может рассматриваться как одна из стратегических целей объединения на данном этапе.

Необходимо отметить, что Таджикистан являлся членом ЕврАзЭС (Евразийского экономического сообщества), которое может рассматриваться как организация, в определенном смысле предшествовавшая ЕАЭС. Однако между указанным объединением существуют значительные отличия: если первое было своеобразной площадкой для поиска точек соприкосновения и ведения диалога в экономической сфере, то второе предполагает более глубокую интеграцию, предусматривающую формирование единого таможенного и торгового пространства. Очевидно, что углубление интеграции и является той причиной, по которой Таджикистан прекратил свое участие в данном формате международных экономических отношений.

Для выявления более точных перспектив интеграции Республики Таджикистан в ЕАЭС требуется детально исследовать преимущества и потери страны от такого вида сотрудничества.

Прежде всего, необходимо отметить особенности экономики Таджикистана. Страна производит относительно небольшие объемы продукции в области цветной металлургии и сельского хозяйства. Основными товарами, представляемыми на экспорт, являются алюминий, хлопок-сырец, электроэнергия и сухофрукты. При этом экспорт электроэнергии осуществляется, несмотря на то что явно ощущается ее нехватка на внутренние нужды страны и сохраняются ограничения на ее поставки как для предприятий, так и для населения, особенно в зимний период. Такая политика обосновывается двумя причинами. Во-первых, стране требуется валюта для обеспечения баланса внешнеторговых операций. Во-вторых, Таджикистан располагает колоссальным гидроэнергетическим потенциалом и стремится в полной мере его реализовать, на что в настоящее время недостаточно средств. Однако когда этот потенциал будет реализован, по крайней мере, частично, стране потребуются внешние рынки сбыта, которыми по очевидным технологическим причинам могут стать только соседние страны. Поэтому руководство страны продолжает поставлять электроэнергию в Афганистан, опасаясь потерять этот рынок сбыта в случае прекращения поставок.

Поскольку Республика Таджикистан самостоятельно производит только относительно небольшой перечень потребительских товаров, в основном ограничивающийся базовыми продуктами питания, она находится в значительной зависимости от импорта (табл. 1).

Рост населения Таджикистана вызывает увеличение потребностей в продовольственных товарах, в связи с чем наблюдается заметное ежегодное увеличение импорта. Исключением оказался лишь 2020 год, когда под воздействием пандемии коронавируса были нарушены существовавшие цепочки поставок, однако уже в 2021 году товаропотоки были восстановлены и объем импорта

возрос на 33,6% по сравнению с предыдущим годом. Динамика экспорта не так стабильна, и в 2022 году был даже отмечен спад на 0,35%, хотя экономика мира в целом в этот период демонстрировала достаточно позитивные тенденции.

Таблица 1

Внешнеторговый оборот Республики Таджикистан, в млн. долл.

| Показатель | Год | | | | |
|-----------------------|--------|--------|--------|--------|--------|
| | 2019 | 2020 | 2021 | 2022 | 2023 |
| Внешнеторговый оборот | 4523,7 | 4557,8 | 6359,1 | 7309,5 | 8328,9 |
| Экспорт | 1174,4 | 1406,9 | 2149,6 | 2142 | 2448,8 |
| Импорт | 3349,3 | 3150,9 | 4209,5 | 5167,5 | 5880,1 |

Источник: Составлено автором по данным: Таджикистан в цифрах 2024. – Душанбе: Агентство по статистике при Президенте Республики Таджикистан, 2024. – 174 с. – С. 135.

Доля импорта во внешнеторговом балансе значительно превышает долю экспорта (рис. 1).

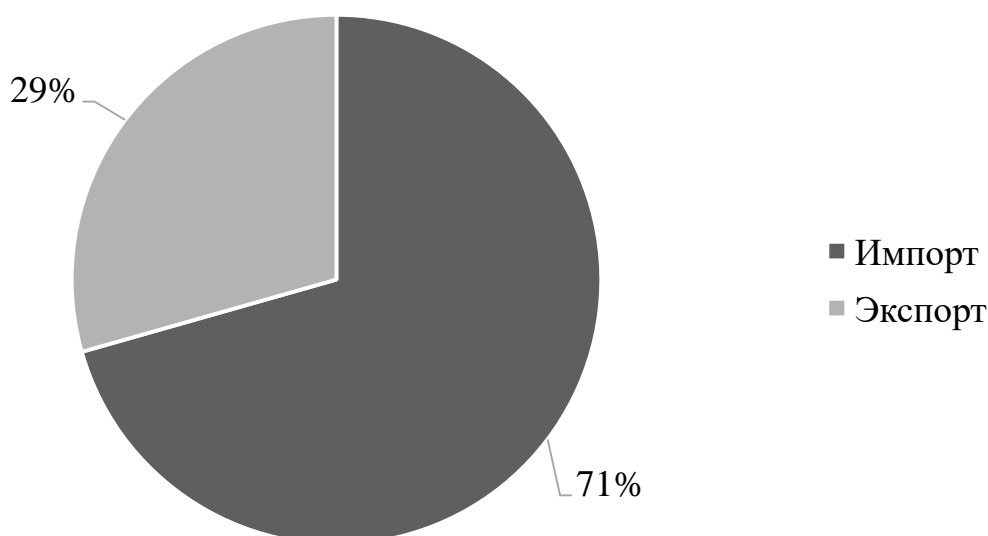


Рис. 1. Доля импорта и экспорта во внешнеторговом балансе Республики Таджикистан в 2023 году

Источник: Рассчитано автором по данным: Таджикистан в цифрах 2024. – Душанбе: Агентство по статистике при Президенте Республики Таджикистан, 2024. – 174 с. – С. 135.

В разные годы доля импорта доходила от 70% до 75% от внешнеторгового оборота, что отражает крайне высокую степень импортозависимости страны. От значительного кризиса экономику спасает экспорт трудовых ресурсов, который ввиду особенностей ведений мировой статистики и высокой доли нелегальной трудовой миграции не находит отражения в структуре внешнеторгового оборота и не может быть точно оценен. Однако с полной уверенностью можно

сказать, что средства, получаемых от трудовых мигрантов, оказываются достаточными для того, чтобы население было в состоянии обеспечивать себя необходимыми товарами за счет импорта. В связи с этим стабильность трудовой миграции для Таджикистана представляется чрезвычайно важным вопросом, и снижение барьеров на ее пути могло бы стать значительным стимулом на пути интеграции в ЕАЭС.

Кроме того, основной поток трудовых мигрантов направлен из Таджикистана в Россию, что уже обеспечивает определенную степень экономической интеграции экономик указанных стран, их взаимную заинтересованность и нацеленность на сохранение и развитие отношений.

Еще одним фактором отражающим, с одной стороны, глубокую интеграцию экономики Таджикистан с экономиками отдельных стран ЕАЭС и, с другой стороны, ее зависимость от этих экономик, является значительный объем импорта в республику товаров из указанных стран (табл. 2).

Таблица 2

Объем импорта и экспорта Таджикистана и стран ЕАЭС, в млн. долл.

| Страна | Год | | | | |
|----------------|--------|--------|--------|--------|--------|
| | 2019 | 2020 | 2021 | 2022 | 2023 |
| Экспорт | | | | | |
| Казахстан | 218,2 | 152,2 | 360,1 | 483,9 | 255,8 |
| Россия | 44,3 | 41 | 72,5 | 88,2 | 134,7 |
| Всего по ЕАЭС | 262,5 | 193,2 | 432,6 | 572,1 | 390,5 |
| Импорт | | | | | |
| Беларусь | 26,4 | 52,3 | 38 | 82,2 | 87,9 |
| Казахстан | 739,3 | 757,5 | 818,5 | 957,3 | 892,9 |
| Кыргызстан | 42,8 | 27,2 | 20,5 | 13,8 | 10,8 |
| Россия | 1009,1 | 932,6 | 1280,5 | 1585,7 | 1580,3 |
| Всего по ЕАЭС | 1817,6 | 1769,6 | 2157,5 | 2639 | 2571,9 |

Источник: Составлено автором по данным: Таджикистан в цифрах 2024. – Душанбе: Агентство по статистике при Президенте Республики Таджикистан, 2024. – 174 с. – С. 137-138.

Особенно велика доля России и Казахстана, являющихся основными торговыми партнерами и главными поставщиками продовольственных товаров и горюче-смазочных материалов для Таджикистана. Если доля стран ЕАЭС составляет около половины всего импорта Таджикистана, то доля одной только России – около 30% (рис. 2).

В настоящее время у Республики Таджикистан не наблюдается никаких торговых связей с Арменией. Также на фоне продолжающегося конфликта сохраняется напряженная обстановка и сокращаются торговые связи с Кыргызстаном, что уже в значительной мере ослабляет заинтересованность Таджики-

стана в интеграции с этими государствами.

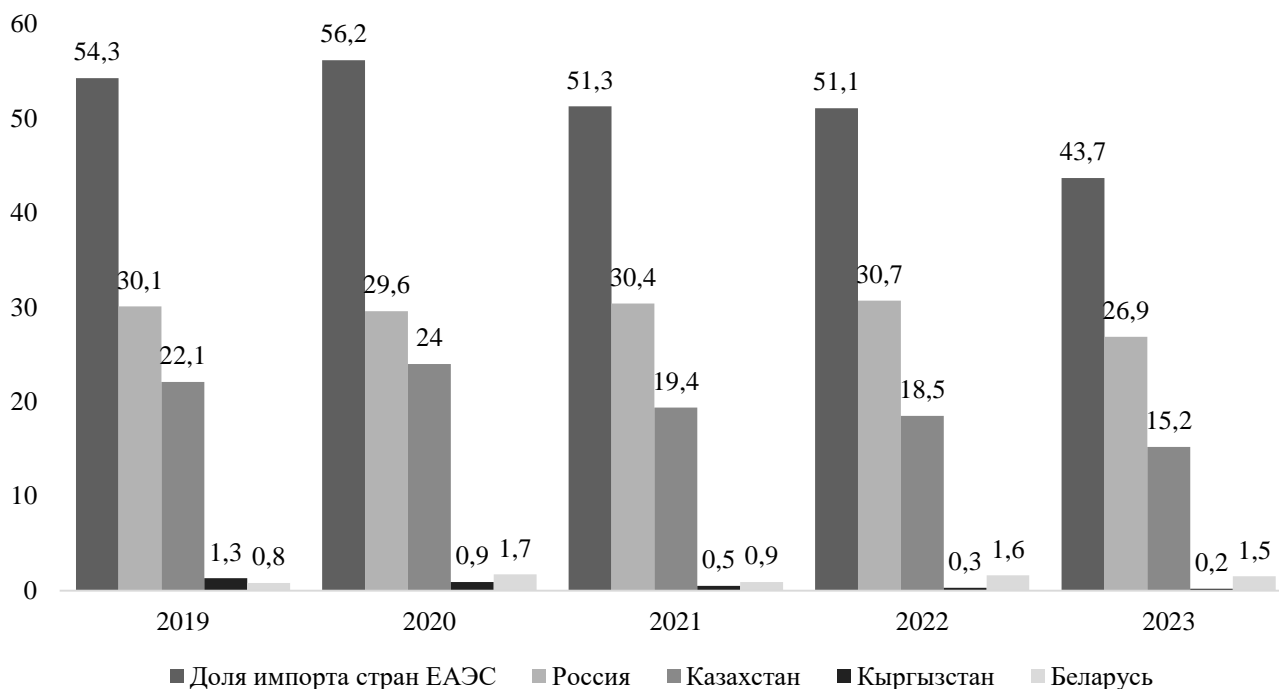


Рис. 2. Доля стран ЕАЭС в структуре импорта Республики Таджикистан, в % от общего объема импорта

Источник: Рассчитано автором по данным: Таджикистан в цифрах 2024. – Душанбе: Агентство по статистике при Президенте Республики Таджикистан, 2024. – 174 с. – С. 137-138.

Исходя из приведенных данных, можно утверждать, что сегодня экономика Таджикистана естественным образом интегрирована с экономикой Казахстана и России, а от последней находится в значительной зависимости.

Выявленная ситуация предопределяет перспективы интеграции Таджикистана в ЕАЭС. Если рассмотреть ее в контексте выделенных выше факторов, определяющих возможность интеграции, можно отметить наличие каждого из них. Республика Таджикистан, находясь в составе Советского Союза на протяжении 70 лет и войдя в состав Российской империи в середине XIX века, имеет протяженную общую историю со всеми странами ЕАЭС, следствием чего является определенная культурная общность, тщательно культивированная в советский период. Таджикистан территориально находится в регионе пересечения интересов крупных мировых игроков, где постоянно возникают очаги политической и военной напряженности. Следовательно, возникает наличие внешней угрозы, что должно стимулировать принятие решения в пользу интеграции. Экономика Таджикистана уже имеет тесные связи с экономиками большей части стран-членов ЕАЭС, что говорит и о наличии общих экономических интересов.

На этом фоне возникает вопрос: по какой причине до настоящего времени не было принято решение о вступлении Таджикистана в ЕАЭС и каковы перспективы этого шага?

Ответ заключается в сильной зависимости республики от импорта и небольших объемах собственного производства, за счет которого формируется основная часть бюджета большей части стран. В Таджикистане основу доходных статей бюджета составляют таможенные поступления и внешнеторговые налоги (табл. 3).

Таблица 3

Доля отдельных статей в структуре доходов бюджета Республики Таджикистан в 2024 году

| Статьи бюджета | Тыс. сомони | В % к общим доходам |
|--------------------|-------------|---------------------|
| Общие доходы | 17045514 | 100 |
| НДС внешний | 6402500 | 37,56 |
| Акциз внешний | 691000 | 4,05 |
| Таможенные пошлины | 1177000 | 6,91 |
| Подходный налог | 2805666 | 16,46 |

Источник: Рассчитано автором по данным: Закон Республики Таджикистан «О государственном бюджете Республики Таджикистан на 2024 год» / Принят постановлением МН МОРТ от 15 ноября 2023 года, №1157.URL: <https://mmk.tj/system/files/Legislation/2012py.pdf> (дата обращения: 03.12.2024).

Почти 40% бюджета страны составляют доходы от выплат НДС, поступающие от внешней торговли. Данная категория доходов совместно с доходами от выплаты внешнеторговых акцизов и таможенных пошлин составляет 48,5% всех доходов государственного бюджета. Здесь необходимо отметить, что для развития и поддержки экспорта в Таджикистане принят закон, приостанавливающий все экспортные таможенные выплаты. Таким образом, указанные доходы бюджета формируются исключительно за счет импорта.

Особая ситуация складывается с подходным налогом, который объединяет выплаты с доходов как физических, так и юридических лиц. Поскольку внешняя торговля составляет значительную долю в предпринимательской деятельности населения Таджикистан и только согласно данным официальной статистики торговля формирует 15% ВВП, логичным будет предположить, что достаточно значительная часть подходного налога также обеспечивается внешней торговлей, а на размер этих поступлений влияет конечная стоимость продаваемой продукции, которая, в свою очередь, увеличивается за счет выплат таможенных пошлин и налогов.

Приведенные данные демонстрируют, что около половины бюджета Республики Таджикистана формируется за счет импортных пошлин. Вступление страны в ЕАЭС предполагает отмену этих пошлин для стран-участниц ЕАЭС. Учитывая тот факт, что общий объем импорта из этих стран в Таджикистан составляет около 50% всего импорта страны, можно говорить о том, что бюджет республики одномоментно сократится приблизительно на четверть.

Безусловно, в ответ страны ЕАЭС отменять свои импортные пошлины для Таджикистана и появится возможность для дальнейшего развития экспорта. Однако в настоящее время доля ЕАЭС в экспорте республики не столь велика –

15,9% (табл. 2). Кроме того, бремя этих расходов лежит на торговых предприятиях, а не на государственном бюджете.

С одной стороны, для развития государства было бы логичным облегчить бремя бизнеса и населения. Ликвидация таможенных барьеров сократит расходы бизнеса и увеличит реальные доходы населения за счет снижения цен на значительную часть потребительских товаров.

С другой стороны, доходы бюджета Республики Таджикистан остаются крайне низкими и в долларовом эквиваленте на 2024 год составляют всего 1578 млн. долл. Половина этих средств традиционно выделяется на социальное обеспечение – выплаты пенсий и пособий, здравоохранение и образование. Оставшаяся половина разделена на выплаты по обеспечению деятельности государственного аппарата и уплату государственного долга, а также около 30% расходной части бюджета составляют различные проекты, нацеленные на развитие сельского хозяйства, промышленности, топливно-энергетического комплекса и транспортной инфраструктуры [8].

Сокращение доходов государственного бюджета приведет к фатальному сокращению возможностей по инвестированию в экономику, которая обладает низкой инвестиционной привлекательностью и привлечь в которую зарубежные инвестиции и инвестиции населения крайне затруднительно.

Таким образом, только один этот факт делает принципиально невозможным вступление Таджикистана в ЕАЭС, несмотря на все существующие предпосылки для интеграции.

В указанном контексте в полной мере проявляются выводы Шишкова Ю.В. о необходимости достижения страной определенного уровня развития для ее успешной интеграции [2, с. 44]. В сложившихся обстоятельствах, учитывая низкий уровень производительности труда в стране и низкую конкурентоспособность местных производителей открытие границ может привести не к их развитию, а к их полной ликвидации местных фирм под воздействием внешней конкуренции.

В этом и заключается проблема, отмеченная Офицеровым-Бельским Д. В.: экономическая интеграция, существующая де-факто, не означает возможность политической интеграции [9, с. 203].

Поскольку «большинстве случаев международная организация для государства – это средство реализации своих интересов» [10, с. 33], Таджикистан не начнет предпринимать активные действия для интеграции в ЕАЭС до тех пор, пока не возникнет для него реальный внешнеполитический вызов, который вынудит страну искать защиты от внешней экспансии в рамках существующих экономических объединений, имеющих устойчивую структуру и представляющих собой нечто большее, чем просто площадка для ведения переговоров и поиска партнеров для реализации совместных проектов (примером чему служит Шанхайская организация сотрудничества).

В настоящее время для Таджикистана выгодно сохранение status quo, когда наблюдается фактическая экономическая интеграция с экономиками России и в

определенной мере Казахстана, основанная на стратегическом двухстороннем партнерстве и целом ряде межправительственных соглашений. При этом участие республики в Организации договора о коллективной безопасности обеспечивает защиту от прямых внешних столкновений и внутренних угроз.

ЕЭАС в этих условиях может рассматривать Таджикистан как стратегического партнера и усиливать взаимодействие в тех сферах, где это не приведет к прямому нарушению экономических интересов каждого из участников внешне-экономических отношений.

Список источников

1. Сафиуллина Р. Н., Кашина Н. В. Евразийство как главный вектор интеграционного сотрудничества на постсоветском пространстве: особенности современных интеграционных процессов и новые реалии// Вестник экономики, права и социологии. 2021. № 1. С. 22-30.
2. Обуховский В. В. Теории международной экономической интеграции// Экономика XXI века. 2007. № 1. С. 27-46.
3. Асадов Б.Р., Гавриленко В.А., Немченко С.Б. Теория многостороннего взаимодействия государств на примере деятельности БРИКС// Актуальные проблемы государства и права. 2021. Т. 5. № 20. С. 590-601.
4. Обухов А. А. Предпосылки и причины формирования межгосударственных интеграционных объединений в исторической ретроспективе// Вестник Московского государственного областного университета. Серия: Философские науки. 2021. № 1. С. 75-82.
5. Ван Ябин. Новый международный опыт обеспечения экономической безопасности// Инновации и инвестиции. 2022. № 9. С. 26-30.
6. Вакарёв А. А., Виноградов В. В., Иевлева Н. В., Винниченко А. С., Котельникова Д. В. Россия в составе евразийской экономики в современную эпоху трансформации мирового рынка: экономическая безопасность// Национальная безопасность /nota bene. 2022. № 3. С. 14 - 27. DOI: 10.7256/2454-0668.2022.3.38188.
7. Дадабаева З. А., Ярыгина И. З. Евразийская экономическая интеграция и безопасность: анализ современных проблем и поиск путей их решения// Вестник Института экономики Российской академии наук. 2022. № 1. С. 171-179.
8. Закон Республики Таджикистан «О государственном бюджете Республики Таджикистан на 2024 год» / Принят постановлением МН МОРТ от 15 ноября 2023 года, №1157 . URL: <https://mmk.tj/system/files/Legislation/2012py.pdf> (дата обращения: 03.12.2024).
9. Офицеров-Бельский Д. В. Дифференцированная интеграция: конкуренция проектов и противоречия интеграционного процесса в ЕС // Вестник Волгоградского государственного университета. Серия 4, История. Регионоведение. Международные отношения. 2021. Т . 26, № 5. – С. 202–216. DOI: <https://doi.org/10.15688/jvolsu4.2021.5.16>.

10. Белоусова И. С. Сравнение ОДКБ и ШОС как институтов международных отношений // Международное право и международные организации. 2022. № 2. С. 31-38. DOI: 10.7256/2454-0633.2022.2.26085.

УДК 339.138

ГЛАВА 6. КРЕАТИВНЫЙ МАРКЕТИНГ КАК ИННОВАЦИОННЫЙ ИНСТРУМЕНТ РАЗВИТИЯ ОТРАСЛЕЙ И СФЕР ДЕЯТЕЛЬНОСТИ

Азарян Елена Михайловна

доктор экономических наук, профессор,
профессор кафедры маркетинга и торгового дела
ФГБОУ ВО «Донецкий национальный университет экономики и торговли
имени Михаила Туган-Барановского»

Аннотация: креативный маркетинг служит инструментом организации планирования и реализации творческих управленческих решений, обеспечивающих достижение стратегических и тактических целей предприятия, и формирования его конкурентных преимуществ и конкурентоспособности будущих товаров и услуг, производимых предприятием. Определено, что креативные индустрии обладают потенциалом создания высокой добавленной стоимости, что создает дополнительные преимущества для предпринимателей и инвесторов. Обозначено, что перспективным направлением развития креативных индустрий является интеграция в данную сферу событийного и культурного туризма.

Креативные индустрии базируются на следующих наиболее важных отличительных характеристиках: они косвенно или прямо основаны на творчестве, культуре, индивидуальных талантах и навыках; предполагают значительный (определяющий) вклад человеческого творчества в ходе производственного процесса; несут в себе потенциал создания добавленной стоимости и рабочих мест; путем производства и эксплуатации прав на интеллектуальную собственность; их товары и услуги обеспечивают формирование гармонично развитой личности и рост качества жизни; имеют не только экономическое, но и социально-культурное значение. Креативная продукция, товары и услуги обладают уникальными свойствами и характеристиками. В маркетинговой деятельности креативная продукция в системе продвижения товаров и услуг также имеет свои уникальные свойства и возможности. В результате научного исследования представлены основные каналы продвижения креативной продукции, которые на наш взгляд наиболее востребованы и отличаются от классических каналов специфическими характеристиками.

Ключевые слова: креативный маркетинг, креативный продукт, инновации, креативные индустрии, инновационный инструмент.

CREATIVE MARKETING AS AN INNOVATIVE TOOL FOR THE DEVELOPMENT OF INDUSTRIES AND FIELDS OF ACTIVITY

Azaryan Elena Mikhailovna

Abstract: Creative marketing serves as a tool for organizing the planning and implementation of creative management decisions that ensure the achievement of strategic and tactical goals of the enterprise, and the formation of its competitive advantages and competitiveness of future goods and

services produced by the enterprise. It is determined that creative industries have the potential to create high added value, which creates additional advantages for entrepreneurs and investors. It is indicated that a promising direction for the development of creative industries is the integration of event and cultural tourism into this sphere.

Creative industries are based on the following most important distinctive characteristics: they are indirectly or directly based on creativity, culture, individual talents and skills; assume a significant (defining) contribution of human creativity during the production process; carry the potential to create added value and jobs; through the production and exploitation of intellectual property rights; their goods and services ensure the formation of a harmoniously developed personality and an increase in the quality of life; they have not only economic, but also socio-cultural significance. Creative products, goods and services have unique properties and characteristics. In marketing, creative products in the system of promotion of goods and services also have their own unique properties and capabilities. As a result of the scientific research, the main channels for promoting creative products are presented, which, in our opinion, are most in demand and differ from classical channels in specific characteristics.

Keywords: creative marketing, creative product, innovation, creative industries, innovative tool.

Маркетинг и комплекс маркетинга в условиях новой реальности приобретают новый формат и развиваются на основе креативного подхода в формировании стратегии развития маркетинга и креативных идей, инновационных подходов в продвижении бренда, выступает инновационным инструментом развития отраслей и сфер деятельности.

Маркетинг присутствует на каждом этапе инновационного развития предприятий, организаций и учреждений, активно используется в разработке и внедрении маркетинговых инновационных технологий и в этот период важно всегда иметь возможность проявить креативность и внести креативные идеи в организации маркетинговой деятельности. Важно на этапе развития креативных идей всегда руководствоваться современными маркетинговыми принципами и инструментами и использовать современные научно-методологические подходы и методы для развития креативного маркетинга, что определяет своевременность и актуальность проведения научного исследования и изучения теоретических особенностей развития креативного маркетинга как инновационного инструмента развития отраслей и сфер деятельности [1, С. 17-21.].

Инновационный процесс и формирование креативных идей всегда связано с неразрывно осуществляется в тесной связи с новыми механизмами взаимодействия между производителями, посредниками и потребителями [2].

Инновационный маркетинг

Инновационный маркетинг - это творческое мышление и уникальное сочетание традиционных и цифровых маркетинговых технологий. Такой подход поможет бизнесу опередить конкурентов. Существует множество способов привлечь целевую аудиторию - от использования автоматизированных маркетинговых инструментов и сотрудничества с влиятельными лицами до создания интерактивного контента и разработки программ лояльности клиентов.

Инновационный маркетинг - это творческий подход и поиск свежих идей

для привлечения клиентов. Речь идет о понимании современных тенденций в маркетинге, а затем о том, чтобы сделать еще один шаг вперед и создать что-то новое и захватывающее. Инновационный маркетинг может быть чем угодно - от креативной кампании или концепции до свежего подхода к традиционным маркетинговым методам, который выделяет ваш бизнес на фоне конкурентов.

Инновационный маркетинг включает в себя изучение потребностей вашей целевой аудитории, понимание ее моделей поведения и предпочтений, а также разработку прототипов или изменение существующих процессов для их охвата. Это также касается запуска, ценообразования и продвижения уникального продукта [3, С. 67.].

Маркетинговая деятельность и процесс формирования, разработки и внедрения инновационной идеи, креативного замысла является отличительной чертой современного комплекса маркетинга, который оказывает масштабное влияние формирование бизнес-моделей и трансформацию бизнес-процессов. Основой и ядром таких трансформаций являются инновационные технологии, например, краудсорсинг, который представляет собой платформенную модель взаимодействия и формирования креативных идей в маркетинге.

Подобные перечисленным формы сотрудничества также называют совместными инновациями. В переводе с английского crowd значит «толпа», sourcing – «поиск ресурсов». Таким образом, этим словом называют процесс сбора каких-либо ресурсов силами большой массы людей. Привлекая ресурсы толпы, любое общественное начинание имеет больше шансов на успех.

Краудсорсинг - это привлечение творческих способностей, знаний и опыта широкого круга лиц для решения единой задачи, как правило, с использованием информационных технологий [4, С. 403-422.].

Например, компания Procter&Gamble предлагает своим потребителям поделиться своими идеями по улучшению продукции и производственного процесса на своем сайте InnoCentive, обещая авторам самых интересных предложений денежные вознаграждения [5].

Краудсорсинговые модели, которые используются в маркетинговой деятельности систематически совершенствуются и в настоящее время активно используется такая модель, как хакатон. Это современная цифровая площадка для организации и проведения популярных мероприятий среди дизайнеров, маркетологов, менеджеров, программистов, которые в сочетании с мозговым штурмом и инновационными кейсами работают над созданием креативного проекта и креативной модели организации бизнес-процесса и другими инновационными проектами [6].

Процесс создания, рождения и реализации креативной идеи достаточно многообразный и в его основе лежит творческая деятельность, креативная деятельность, дизайн мышления, трансформация маркетингового ландшафта, которые активно используются в решении бизнес-задач в сфере маркетинга, стратегического и кадрового управления.

Креативный маркетинг систематически трансформируется под влиянием

структурных вызовов, разработкой и внедрением инициатив различных весомых объектов и субъектов экономического и социального развития и активно используется при формировании стратегий развития и концепций развития, занимает важное место в формировании дорожной карты реализации государственных, экономических, социальных и экологических инициатив.

Креативный маркетинг является объектом масштабных научных исследований и и такие авторы, как Л. А. Сосунова, А. П. Плотников, Д. В. Чернова, Н. В. Астафьева, А. А. Ипполитова, А.В. Ишутин, С.В. Косаримов, Е.В. Чикирка, Н.В. Пьянова, Е.А. Алекса, А.И. Попова, И.Н. Чернышов, Н.Н. Зюзина, А.А. Числова, А.С. Жупарова, Г.Ж. Исмаил, Г.И. Гумерова, Э.Ш. Шаймиева, Д.Г. Куренова, Е.В. Кривошеева, Д.С. Волошина, Т.Ю. Захарова, И.Б. Королёва, И.Л. Соколова, которые исследуют креативный маркетинг как инструмент коммерциализации объектов интеллектуальной собственности, генерирование инновационных идей в маркетинге, экономические аспекты развития экономики креативных индустрий, креативные индустрии.

Креативный маркетинг практически не связывается с традиционным понятием креатива, а поиска чего-то необычного и оригинального.

Креативный маркетинг служит инструментом организации планирования и реализации творческих управленческих решений, обеспечивающих достижение стратегических и тактических целей предприятия, и формирования его конкурентных преимуществ и конкурентоспособности будущих товаров и услуг, производимых предприятием [7].

Бизнес-структуры и предпринимательские структуры, которые активно внедряют маркетинг инноваций, также активно развивают креативную деятельность компаний.

Креативная деятельность предприятий, организаций и учреждений направлена на эффективное и рациональное управление человеческим и интеллектуальным капиталом, на формирование ценностного предложения при разработке и продвижении оригинальных идей в организации бизнес-процессов, на повышение уровня маркетингового и инфраструктурного обеспечения и маркетингового потенциала, тем самым повышая имидж, благоприятную среду развития, репутацию и бренд предприятий, организаций и учреждений.

В условиях развития экономики новой реальности креативная экономика представляет собой целостную систему, экономическую платформу, маркетинговую систему, которая постоянно пополняется новыми идеями и формами организации маркетинговой деятельности, которые являются результатом масштабных научных исследований и отличаются научной новизной и научными положениями.

Маркетинговые инновации активно апробируются и используются в практической деятельности и которые отличаются новыми подходами, формируют экономику и систему знаний нового поколения, высокой степенью ответственности, мотивации и компетенций, креативными идеями и проектами, которые также формируют объекты интеллектуальной собственности.

Маркетинг креативных технологий активно развивается благодаря технологиям следующего поколения, согласно концепции Маркетинг 5.0, которые масштабно используются на рынке товаров и услуг и создают новые возможности для продвижения товаров и услуг в сети Интернет.

Маркетинг инноваций и инновационных технологий связан с мышлением и в его развитии играет большую роль дизайн мышления, внедрение которого и развитие создает маркетинговый ландшафт нового формата, с позиционированием новых подходов в мышлении и принятии решений, когда на первое место при выборе продукции, товаров и услуг или при формировании креативных идей выходят талант, логика, интуиция, изобретательность, воображение, авантюризм, опыт и компетенции.

Креативные идеи появляются, прежде всего, в результате системного подхода и комплексного анализа, в поиске новых стратегий. Распространение технологий позволяет использовать новые бизнес-процессы, бизнес-модели и новые инструменты коммерциализации креативных идей и проектов, содействуя экономическому и социальному росту.

Одним из важнейших элементов успешного распространения технологий является наличие способности и компетенций для ее применения, использования и последующего воспроизводства в отраслях и сферах деятельности.

В соответствии с распоряжением Правительства РФ от 20 сентября 2021 г. № 2613-р «Об утверждении Концепции развития творческих (креативных) индустрий и механизмов осуществления их государственной поддержки в крупных и крупнейших городских агломерациях до 2030 г.» к творческим (креативным) индустриям относятся в том числе:

- индустрии, основанные на использовании историко-культурного наследия (народно-художественные промыслы и ремесла, музейная деятельность);
- индустрии, основанные на искусстве (театр, музыка, кино, анимация, живопись, деятельность галерей и др.);
- современные медиа и производство цифрового контента (кино-, видео-, аудио-, анимационное производство, обработка данных и разработка программного обеспечения, виртуальная и дополненная реальность, компьютерные и видеоигры, блоггерство, печатная индустрия, средства массовой информации, реклама и пр.);
- прикладные творческие (креативные) индустрии (архитектура, промышленный дизайн, индустрия моды, гастрономическая индустрия и т.п.) [9].

Креативные индустрии — это сферы, находящиеся на пересечении культуры, искусства бизнеса и технологий, которые могут приносить доход путем торговли и прав на интеллектуальную собственность [9. С. 36–45.].

Креативные индустрии обладают потенциалом создания высокой добавленной стоимости, что создает дополнительные преимущества для предпринимателей и инвесторов [10, С. 129–143.].

Для многих сфер креативных индустрий характерен относительно низкий

барьер входа на рынок креативных продуктов, что дает возможность развития своего творческого дела многим группам населения.

Отметим, что, например, маркетинг впечатлений или событийный маркетинг – это набор инструментов воздействия на целевую аудиторию, формирующих устойчивую связь потребителя с брендом/компанией/товаром/услугой через активацию эмоций и получение физического и духовного опыта [11, С. 625-646.].

При формировании качественного креативного продукта важно достичь главной миссии любого инновационного проекта – получение прибыли, закрепление успеха и получение максимальной выгоды (престиж, имидж, репутация) [12].

Важно использовать качественные материалы и качественные продукты (сырье) для получения максимального эффекта, что формирует особый подход к системе мониторинга и контроля в системе маркетинговой деятельностью. Маркетинговый подход позволяет получить обратную связь от потребителей продукта и оценить его качество. Оправданные ожидания потребителей являются важным фактором успеха креативного продукта.

Креативные индустрии имеют свои отличительные характеристики, которые важно учитывать при формировании стратегии развития маркетинга:

- креативные идеи напрямую зависят от творчества, индивидуальных качеств человека, его нестандартного мышления, культуры поведения и восприятия, его таланта и практических навыков;
- креативные индустрии формируют возможности для проявления, продвижения, представления человеческих возможностей и таланта;
- развивая креативные индустрии, создается новая ценность при реализации бизнес-процессов и формируются новые рабочие места и новые подходы в организации производственного цикла и рабочего процесса;
- формируется новый и инновационный продукт, который требует бережного отношения и защиты интеллектуальной собственности;
- воплощение креативных идей всегда будет иметь социально-экономическое значение для общества, государства и населения, повышая статус населения, экономические выгоды и качество жизни граждан страны [13].

Маркетинговая политика современных компаний формируется на основе креативных идей, которые изначально формируются, прорабатываются, апробируются, что позволяет оценить их эффективность и целесообразность их внедрения (рис. 1).

Среди основных направлений развития системы продвижения креативного продукта следует выделить стратегические направления, которые будут играть важную роль в развитии отраслей хозяйствования и сфер деятельности, которые активно внедряют инновации и креативные идеи.

Перспективным направлением развития креативных индустрий является интеграция в сферу событийного и культурного туризма, что является актуальной темой научного исследования и в последующих публикациях следует уде-

лить более тщательное внимание к специфике внедрения креативных идей в представленных сферах деятельности.



Рис. 1. Основные направления развития системы продвижения креативного продукта

Креативная продукция, товары и услуги обладают уникальными свойствами и характеристиками. В маркетинговой деятельности креативная продукция в

системе продвижения товаров и услуг также имеет свои уникальные свойства и возможности.

В результате научного исследования представим основные каналы продвижения креативной продукции, которые на наш взгляд наиболее востребованы и отличаются от классических каналов специфическими характеристиками:

1. В системе продвижения товаров и услуг в сети Интернет цифровые и инновационные маркетинговые технологии продвижения все более совершенствуются, становятся эксклюзивными и персонализированными, способными выполнять большой функционал основных задач и сопутствующих заданий, что дает возможность компаниям иметь преимущества перед другими конкурентами, оперативнее и рациональнее использовать создающиеся преимущества, что особенно важно при формировании и развитии взаимодействия между производителями, посредниками и потребителями. Выбор цифровых каналов коммуникации необходимо осуществлять исходя из сегментации целевой аудитории для таргетинга потенциального посетителя.

При выборе инструментов продвижения предпочтение отдается новым и инновационным средствам продвижения товаров и услуг, которые имеют необычные формы и нестандартные пути решения основных задач: доставка и продвижения продукции, товаров и услуг к конечному потребителю, качественное выполнение поставленных задач, удовлетворение потребностей потребителей и получение максимальной выгоды для всех заинтересованных лиц: прибыли и повышение благоприятного имиджа для производителя или посредника, качественная продукция, товары и услуги для потребителя.

2. В развитии креативной индустрии важно использовать инновационные технологии формирования креативного пространства и маркетингового ландшафта нового формата, которые является площадкой для взаимодействия всех заинтересованных субъектов хозяйствования и возможности проявить талант, воплотить креативные идеи в жизнь. Необходимо совершенствовать прозрачность официальных сайтов креативных пространств для эффективного продвижения уникального продукта с ориентацией на аутентичность дестинаций и локаций. Организаторы все чаще ищут возможность комбинировать большие выставочные площадки с прилегающими территориями, чтобы реализовать общение, дискуссии, обмен опытом в малых группах в рамках мероприятия.

3. Креативная индустрия активно развивается и маркетинговые инновации направлены на формирование и продвижение бренда, которые создают новый образ и новый профиль продукта, товара и услуги в восприятии потребителя и полностью оправдывают его ожидания, это при самом благоприятном развитии событий. Считается бренды воспринимаются и ими пользуются определенный сегмент покупателей, сформировавшиеся личности финансово независимые, которые хорошо знают особенности формирования и продвижения бренда и следят за модными тенденциями. Также для коллективов организаций и учреждений также свойственно покупать и пользоваться брендовыми товарами и

продукцией. Потребителей привлекают индивидуальность и эксклюзивность, которые обладают уникальными характеристиками, благодаря которым целевая аудитория узнает и воспринимает продукт, товар или услугу, которые имеют креативный образ [14].

При формировании креативных идей важно всегда помнить, что это сложный процесс создания идеи и ее воплощения, который является творческим и включает большие затраты времени и финансовых, информационных, материальных, технических, цифровых и других, которые являются важной составляющей в рождении креативной идеи, которая может стать важным открытием и популярным инструментом продвижения бренда.

Перспективными направлениями научных исследований при изучении особенностей и специфики развития креативных индустрий является создание и продвижение уникальных креативных продукции, товаров и услуг, что будет решать в комплексе целый спектр экономических, экологических, социальных, инклюзивных вопросов в отраслях хозяйствования, в полном соответствии с государственными и национальными программами развития в условиях структурных вызовов и государственных инициатив.

Список источников

1. Сосунова, Л. А. Креативный маркетинг как инструмент коммерциализации объектов интеллектуальной собственности / Л. А. Сосунова, А. П. Плотников, Д. В. Чернова, Н. В. Астафьева, А. А. Ипполитова // Экономические науки, 2017. – №153. – С. 17-21.
2. Ишутин, А. В. «Нейронное искусство» как объект авторского права / А.В. Ишутин, С.В. Косаримов, Е.В. Чикирка // Социальные новации и социальные науки, 2021. – №1 (3). [Электронный ресурс]. – Режим доступа: <https://cyberleninka.ru/article/n/neyronnoe-iskusstvo-kak-obekt-avtorskogo-prava>
3. Пьянова, Н.В. Преобразование новых идей в инновационные решения путем использования методов и приемов генерирования / Н.В. Пьянова, Е.А. Алекса, А.И. Попова // Инновационная экономика: перспективы развития и совершенствования, 2022. – №6 (64). – С. 67.
4. Чернышов, И.Н. Краудсорсинг как новая форма трудовой деятельности в цифровой экономике: предпосылки возникновения, сущность и содержание / И.Н. Чернышов // Экономика труда, 2021. – Том 8. – № 4. – С. 403-422. DOI: 10.18334/et.8.4.111947.
5. InnoCentive [Электронный ресурс]. – Режим доступа: <https://ru.wikipedia.org/wiki/InnoCentive>
6. Хакатон для запуска онлайн-школ [Электронный ресурс]. – Режим доступа: <https://edmarketru-rujnhcwbo-netology-group.vercel.app/blog/hackaton/>
7. Зюзина, Н.Н. Креатив в маркетинге / Н.Н. Зюзина, А.А. Числова // Экономика и социум, 2017. – №1-1 (32) [Электронный ресурс]. – Режим доступа: <https://cyberleninka.ru/article/n/kreativ-v-marketinge>

8. Распоряжение Правительства РФ от 20 сентября 2021 г. № 2613-р «Об утверждении Концепции развития творческих (креативных) индустрий и механизмов осуществления их государственной поддержки в крупных и крупнейших городских агломерациях до 2030 г.» [Электронный ресурс]. – Режим доступа: <https://www.garant.ru/products/ipo/prime/doc/402745784/>

9. Жупарова, А. С. Экономика креативных индустрий: сущность и основные характеристики / А.С. Жупарова, Г.Ж. Исмаил // Модели, системы, сети в экономике, технике, природе и обществе, 2021. – № 3. – С. 36–45. DOI: 10.21685/2227-8486-2021-3-4

10. Гумерова, Г.И. Интеллектуальная составляющая российских креативных индустрий в период их становления / Г.И. Гумерова, Э.Ш. Шаймиева // Вестник Воронежского государственного университета. Серия: Экономика и управление, 2022. – № 3. – С. 129–143.

11. Куренова, Д.Г. Инструменты маркетинга впечатлений в продвижении предприятий общественного питания / Д.Г. Куренова, Е.В. Кривошеева, Д.С. Волошина, Т.Ю. Захарова // Креативная экономика, 2024. – Том 18. – № 3. – С. 625-646. DOI: 10.18334/ce.18.3.120727.

12. Креативные индустрии в России: тенденции и перспективы развития [Электронный ресурс]. – Режим доступа: https://www.hse.ru/data/2021/07/11/1434062388/CI_1.pdf

13. Королёва, И.Б. Креативные индустрии в России и мире: состояние, тенденции и проблемы управления развитием / И.Б. Королёва, И.Л. Соколова // Baikal Research Journal, 2022. – Т. 13, № 3. – С. 19. DOI 10.17150/2411-6262.2022.13(3).14.

14. Сессия ПМЭФ-2024 «Глобальный VS локальный: как продвигать креативный продукт, основанный на собственной идентичности» [Электронный ресурс]. – Режим доступа: <https://roscongress.org/sessions/spief-2024-delovaya-programma-kulturnyy-kod-rossii-zavtra-vzglyad-c>

УДК 339.138

ГЛАВА 7. ГЕЙМИФИКАЦИЯ В МЕНЕДЖМЕНТЕ – «ЗА» И «ПРОТИВ»

Бузни Артемий Николаевич
д.э.н., профессор, академик АЭНУ, пенсионер

Аннотация: Экономическая категория «Геймификация», понимаемая как использование принципов игры в системе образования и в производственных процессах в целях вовлечения участников в более продуктивную познавательную или созидательную деятельность, получает всё большее распространение в практике менеджмента и становится предметом интенсивных научных исследований как в первую очередь за рубежом, так и с относительно недавних пор в отечественной научной литературе. Рассматривается специфическая особенность геймификации в возможностях обычно нематериального, но эффективного метода стимулирования деятельности на основе игры с применением Интернета, гаджетов как средств работы с информацией, а также состязательных усилий тех или иных групп участников. В этой связи оценивается необходимость и возможность применения геймификации для стимулирования персонала предприятия в быстро меняющихся условиях их труда в digital-экономике. С использованием метода контент-анализа проведен обзор научных публикаций, посвящённых геймификации, а также материалов ряда международных организаций. На основе оценок «за» и «против» геймификации в системе менеджмента предприятия в быстро меняющихся условиях труда в digital-экономике сделан вывод о том, что геймификация имеет паллиативный, т.е. временный эффект, лишь частично решающий проблему снижения трудовой активности персонала предприятия. Обосновывается мнение о необходимости разработки научной модели более совершенного общества, где труд для человека станет естественным образом жизни, а не средством выживания.

Ключевые слова: менеджмент, труд, персонал, геймификация, игрофикация, стимулы, вовлечённость, игровое мышление, digital-экономика, бизнес.

GAMIFICATION IN MANAGEMENT – PROS AND CONS

Buzni Artemiy Nikolayevich

Annotation. The economic category "Gamification", understood as the use of game principles in the education system and in production processes in order to involve participants in more productive cognitive or creative activities, is becoming increasingly widespread in management practice and is becoming the subject of intensive scientific research both primarily abroad and more recently in the domestic scientific literature. A specific feature of gamification is considered in the possibilities of a usually intangible, but effective method of stimulating activities based on the game using the Internet, gadgets as a means of working with information, as well as the competitive efforts of certain groups of participants. In this regard, the necessity and possibility of using gamification to stimulate enterprise managers in the rapidly changing conditions of their work in the digital economy are assessed. Using the content analysis method, a review of scientific publications on gamification, as well as materials from a number of international organizations, was conducted. Based on the "pros" and "cons" of gamification in the enterprise management system in rapidly changing working conditions in the digital economy, it is concluded that gamification has a palliative, i.e. temporary effect, which only partially solves the problem of reducing the labor activity of the enterprise's per-

sonnel. The opinion is substantiated on the need to develop a scientific model of a more perfect society, where work for a person will become a natural way of life, and not a means of survival.

Keywords: management, labor, personnel, gamification, gamification, incentives, engagement, game thinking, digital economy, business.

Возникновение проблемной ситуации. Одним из новых активно развивающихся в настоящее время в мировой экономике трендов в системе менеджмента предприятия становится использование методов геймификации, т.е. принципов игрового взаимодействия персонала предприятия в целях повышения заинтересованности в самом процессе труда и его результативности.

Ещё в 1980 г. американский профессор Школы менеджмента Слоуна при Массачусетском технологическом институте, консультант по менеджменту Томас В. Мэлоун опубликовал ряд статей о значении игры как «эвристике для приятных интерфейсов» - способов взаимодействия человека и техники, а профессор Эссекского университета Ричард Баркл дал первое определение термину «геймификация», определив её как *«превращение чего-то, что не является игрой, в игру»* [1].

В современном понимании этот термин был введен только в 2002 году британским консультантом Ником Пеллингом, а на страницах научной литературы получил распространение лишь в 2010 году (в России - в 2012 г.).

На необходимость усиления вовлечённости персонала в трудовой процесс обратили внимание в США после опубликования в 2013 году ежегодного доклада исследовательской кампании Gallup о трендах на рынке, в котором в частности отмечалось, что «семь из 10 работников в Америке либо активно отстранены от работы, либо не вовлечены в неё»[2], следствием чего становится и снижение продуктивности труда.

Поэтому компании стали обращаться к геймификации как инструменту мотивации персонала для оживления рутины труда, являющейся одной из причин снижения мотивации, добавив в него игровой элемент. Ссылаясь на данные испанской кампании Anadea Company, основатель и CEO CleverStaff В.Курило отметил, что «Внедрение различных игровых техник в самых различных сферах трудовой и образовательной деятельности позволяет повысить **вовлечённость сотрудников в работу на 48%**»[3].

Стимулирование самих менеджеров разного уровня имеет специфические особенности и применение геймификации здесь составляет несколько иную проблему. В условиях развивающейся цифровой экономики происходят существенные трансформации в менеджменте. По некоторым данным, «В течение 5-7 лет массовая автоматизация грозит сокращением 30% чиновников и служащих государственного аппарата» [4]. Основатель группы Re-engineering Futures Павел Лукша, высказал мнение о том, что «Создание автоматизированных производств без участия человека – неизбежное развитие событий. Задачи для среднего менеджмента, так называемого «офисного планктона» практически

исчезнут» [5]. Но и функции линейных менеджеров подвергаются преобразованиям. В развивающейся digital-экономике управление коллективом всё чаще подменяется управлением информационными системами, включая организацию, эксплуатацию, обслуживание этих систем и т.п., что становится функцией новой профессии – информационного менеджера. Изменение характера труда менеджера влечёт изменения и в его мотивации. Экономические мотивы сочетаются с мотивами иного порядка: помимо материальных стимулов, зависящих от результатов и качества труда, всё более важными становятся потребность в комфортных условиях трудовой деятельности, стремление к совершенствованию профессионализма на основе повышения уровня знаний, возрастает чувство ответственности и самостоятельности, необходимость самореализации, углублённого познания мира и т.п. Поэтому необходимы новые принципы стимулирования менеджеров, для чего требуется соответствующая методика и достаточный объём фактической информации прежде всего о том, чего желает новый менеджер, каковы мотивы его труда.

Тренды категории «Геймификация» в мировой литературе

Проведенный анализ научной литературы показал, что проблема геймификации в менеджменте концентрируется главным образом на целях и задачах использования игровых технологий, методах организации труда производственного коллектива, применяемых менеджерами для улучшения коммуникаций участников производственного процесса. К этой проблеме обратились зарубежные исследователи (Д.Ариели, Б.Бёрк, С.Браун, К.Вербах, Н.Голдштейн, К.Воган, А.Диксит, Г.Зикерман, Д.Линдер, К.Капп, Дж.Макгонигал, С.Мартин, Б.Дж.Нейлбафф, Д.Пинк, М.Резник, Б.Трейси, Р.Уокер, Д.Хантер, Й.Хёйзинга, Ю.Кай-Чоу и др.), а также российские (С.Абдульманов, Г.Альтшуллер, В.Артамонова, Д.Берджес, Д.Борисов, А.С.Борисова, М.Бронникова, Ю.Воликова, А.Гин, Д.Кибкало, Е.Любко, И.Нефедьев, Е.Поворина, Е.Родионцева и др.).

Авторы исследований выделяют следующие основные аспекты:

- генезис геймификации с древнейших времён, от человека разумного (*Homo sapiens*) до человека играющего (*Homo Ladens*);
- принципы и практика применения игры в различных сферах деятельности как за рубежом, так и в России;
- становление игрового мышления и стратегии его организации как подхода к вовлечению и мотивации людей, помогающего им достигать как личных целей, так и целей всей организации;
- геймификация с позиций стимулирования труда сотрудников предприятия, их вовлечённости в процесс производства на эмоциональном уровне, формирование самомотивации персонала в стремлении к профессионализму, приобретению необходимых навыков, повышению лояльности к организации, снижению текучести кадров, укреплению социальных связей, повышению социального интеллекта;
- привлечение клиентов на долгосрочную перспективу с увеличением объёма продаж, укреплением позиции, конкурентоспособности предприятия на рынке;

- планирование, пошаговая механика, дизайн игры, концентрирующей внимание на психологической мотивации, включающей в частности комплекс поведенческих стимулов «октализа», или восьмиугольника Ю-Кай Чоу (Рис. 1);



Рис. 1. Октализ поведенческих стимулов Ю-Кай Чоу

Источник [6]

- методика геймификации в образовании, дидактические приёмы повышения заинтересованности обучающихся к аудиторным и дистанционным занятиям, а также к самостоятельной работе.

Собранные нами в поисковых системах Интернета данные косвенно свидетельствуют о динамике распространения интереса к геймификации в научной литературе по ряду популярных направлений по состоянию на середину октября 2024 года (табл.1).

Таблица 1

Результаты запросов в поисковых системах Интернета в русскоязычном контенте по теме геймификация

| Тема запроса | Поисковая система Интернета | | | | |
|----------------------------|-----------------------------|-----------|-----------|-----------|-----------|
| | Google.com | | Bing.com | | Yandex.ru |
| | 2014 | 2024 | 2014 | 2024 | 2024 |
| Геймификация это | 182 000 | 485 000 | 688 000 | 1 960 000 | 2 000 000 |
| Геймификация в бизнесе | 179 000 | 350 000 | 1 370 000 | 2 840 000 | 868 000 |
| Геймификация в обучении | 164 000 | 389 000 | 549 000 | 1 280 000 | 424 000 |
| Геймификация в образовании | 150 000 | 315 000 | 666 000 | 1 410 000 | 409 000 |
| Геймификация в маркетинге | 123 000 | 210 000 | 454 000 | 1 070 000 | 127 000 |
| Геймификация в мире | 103 000 | 324 000 | 1 130 000 | 1 910 000 | 688 000 |
| Геймификация в России | 184 000 | 350 000 | 2 040 000 | 3 800 000 | 1 000 000 |
| в Китае | 814 000 | 771 000 | 1 100 000 | 3 300 000 | 232 000 |
| в США | 1 340 000 | 1 170 000 | 757 000 | 1 900 000 | 318 000 |
| в Бразилии | 239 000 | 304 000 | 1 100 000 | 3 780 000 | 73 000 |
| в Индии | 9 | 15 500 | 914 000 | 3 360 000 | 125 000 |

Приведенные результаты запросов, хоть и не могут быть достаточным основанием для научных выводов при такой постановке запросов, но в разных поисковых системах достаточно чётко отражают тенденции роста интереса к геймификации в целом и в приоритетных направлениях её использования: прежде всего в бизнесе, затем в обучении и образовании и затем в практике маркетинговых исследований рынка. Показательны и данные об интересе к геймификации в мире и в крупнейших по территории и численности населения, но в разных по экономическому развитию странах.

Эти тенденции отмечены и в данных «Киберленинки». Если за период с 2010 по 2018 годы термин «Игрофикация» (равнозначно «геймификация») встречается в 122 публикациях, то с 2020 по 2024 годы – уже в 3972. То есть количество публикаций возросло в 32,5 раза. Из них больше публикаций по применению в образовании (2334), затем в экономике и бизнесе (667), в СМИ (медиа) и массовых коммуникациях (387), в компьютерных и информационных технологиях (142), а далее по убыванию - социология, языкознание и литературоведение, право, философия, этика, религиоведение, здоровье, психология. Любопытный контент-анализ, отражающий тренды частоты использования терминов, связанных с геймификацией, приведен П.В.Смирновой и О.В.Кононовой (табл.2).

Таблица 2

Терминограмма по ключевому термину “Gamification”

| 2014 | | 2015 | | 2016 | | 2017 | | 2018 | |
|-------------|---------|------------|---------|----------|---------|--------------|---------|------------|---------|
| Термин | Частота | Термин | Частота | Термин | Частота | Термин | Частота | Термин | Частота |
| Social | 786 | Learning | 518 | Learning | 925 | Research | 1291 | Design | 1699 |
| Use | 331 | Games | 504 | Use | 786 | Games | 1092 | Study | 1522 |
| Research | 270 | Use | 358 | Students | 734 | Learning | 1064 | Research | 1516 |
| Games | 268 | Elements | 285 | Social | 683 | Study | 1023 | Students | 1367 |
| Learning | 263 | Based | 278 | Games | 663 | Students | 829 | Games | 1317 |
| Information | 228 | Motivation | 277 | Design | 599 | Based | 813 | Learning | 1250 |
| Based | 221 | Students | 268 | Health | 561 | Participants | 802 | Motivation | 1119 |
| Time | 209 | Design | 267 | Research | 541 | Design | 798 | Based | 1110 |
| Study | 197 | Social | 263 | Model | 517 | Motivation | 785 | Use | 1092 |

Источник [7]

Из данных таблицы следует, что если изначально в научных публикациях помимо общего увеличения исследований феномена геймификации уделялось преимущественное внимание социальной значимости проблемы, её научной интерпретации и первым опытам применения игры в различных сферах деятельности, то по мере накопления опыта менялись и приоритеты в направлениях исследований. Вводится геймификация как дисциплина и в учебные программы вузов.

При этом, по данным Интернета, в бизнесе объём мирового рынка геймификации в 2014 году составил \$1,4 млрд, в 2018 году — \$5,5 млрд, в 2020 году — \$9,1 млрд. Ожидается, что к 2025 году он достигнет \$30,7 млрд, а к 2026 году — \$38 млрд.

Геймификация как мотивация труда

К.Вербах и Д.Кевин в книге, ставшей первым курсом по геймификации, написанным в 2012 году, определение геймификации, взятое авторами сначала в качестве рабочего как использование игровых элементов и игровых механик в неигровом контексте, заменили на: применение приёмов, характерных для компьютерных игр в неигровых процессах [8].

По определению Б.Бёрка - вице-президента американской консалтинговой компании по информационным технологиям Gartner и автора книги «Геймификация — как геймификация мотивирует людей на необычные поступки», геймификация – это «Использование игровой механики и дизайна опыта для вовлечения людей в цифровую среду и мотивации к достижению их целей», а также «это метод цифрового взаимодействия, а не личного, означающий, что игроки взаимодействуют с компьютерами, смартфонами, носимыми мониторами или другими цифровыми устройствами» [9]. По существу сами гаджеты своей инновационностью и раскрывающимися широкими возможностями к получению неограниченной информации уже представляют собой инструмент игры (скажем так – привлекательную игрушку для людей любого возраста, начиная даже с детей, которых привлекает уже пульт телевизора или управления машинкой чуть ли не раньше, чем они начинают ходить).

Менеджеры в этой связи представляются не как игроки, а как организаторы игрового взаимодействия членов коллектива: будь то сотрудники предприятия, взаимодействующие между собой, будь то продавцы, с одной стороны игровой команды и покупатель – с другой, или ученики и преподаватель и т.п., но при этом, по первому определению Бёрка, сами менеджеры не воспринимают игру как стимул для себя, не взаимодействуют с участниками игры. Зато по второму определению Бёрка, линейный менеджер, взаимодействуя в процессе своей работы с цифровыми устройствами, заменяющими ему подчинённый в прошлом коллектив, может нуждаться в стимулировании не только в форме самостимулирования, но и в стимулировании со стороны более высокого уровня менеджмента, где стимулом может оказаться предоставление для работы более совершенного и привлекательного оборудования, комфортные условия работы на этом оборудовании. Это напоминает в определённой мере условия игры и предполагает состязательность на рынке с менеджментом кампаний, занимающихся аналогичным производством. Это не связано с геймификацией и для решения вопросов стимулирования линейного менеджера на игровой основе необходимо чётко представлять его потребности, мотивированность труда, к которым в геймификации не будут относиться традиционные формы материального стимулирования.

Здесь следует остановиться на различиях в мотивации труда в менеджменте на разных его уровнях: высшем (топ-менеджмент), среднем (руководители функциональных подразделений организации) и низшем или линейном (руководители непосредственных исполнителей производственных заданий). По некоторым исследованиям, наименее мотивированным в системе менеджмента

является труд линейных менеджеров.

Известный в США исследователь мотивации менеджеров Скотт Майерс, проведя анкетный опрос 1344 менеджеров, установил различия в мотивации менеджеров от занимаемого ими уровня управления (табл. 3).

Таблица 3

Различия в уровнях мотивированности труда менеджеров по уровням управления

| Уровень управления | Количество опрошенных, чел. | Уровень мотивированности, % | | | Всего, % |
|--------------------|-----------------------------|-----------------------------|---------|--------|----------|
| | | высокий | средний | низкий | |
| Высокий | 91 | 57 | 31 | 12 | 100 |
| Средний | 683 | 32 | 39 | 29 | 100 |
| Низкий | 570 | 23 | 43 | 34 | 100 |
| Всего | 1344 | 30 | 40 | 30 | 100 |

Источник [10]

К аналогичным выводам о снижении мотивированности труда при снижении уровня управления пришли и отечественные исследователи, например, О.В.Куликова и О.В.Бубнова, показавшие по результатам исследования, что «существуют существенные различия в мотивационной структуре менеджеров высшего и среднего звена предприятий» [11].

Особо важной является конъюнктура рынка труда, диктующая степень необходимости стимулирования. Так, например, в мае 2023 года структура спроса и предложения на менеджерские услуги в России выглядела следующим образом: на управление персоналом и тренинги доля активных вакансий в общем количестве вакансий составила 1,8%, а доля активных предложений – 2,9% и, следовательно, hh-индекс – 1,6, что свидетельствовало о дефиците предложений со стороны линейных менеджеров, поскольку, как известно, благоприятным для предпринимателя рынок становится при hh-индексе не менее 5. В то же время на высшее и среднее звенья менеджмента доля активных вакансий в общем количестве вакансий была 1,1%, а доля активных предложений – 5,0%, hh-индекс – 4,5, что позволяло предпринимателям подбирать кандидатов из достаточного количества предложений на более выгодных для предпринимателя условиях [12].

Однако тенденция на рынке труда в цифровой экономике такова, что автономные самоуправляемые группы производственных коллективов будут сокращаться вплоть до одного работника, освоившего весь трудовой цикл в применяемой электронной технике, и таким образом планирующего, принимающего решения, выполняющего работу и несущего ответственность за её результат, т.е. становящегося как бы фрилансером, сам себе менеджером и информационным менеджером. Мотивация его труда в значительной мере помимо материальных факторов становится связанной с самостимулированием. В таком

случае следует рассмотреть возможность геймификации для фрилансера как дополнительного нематериального стимула.

Основные нематериальные мотивы труда, применительно к линейным менеджерам или уже фрилансерам, во-первых, обоснованы в известной пирамиде А.Маслоу, и в самом общем плане подразделяются на социальные, психологические, моральные, организационные. Ситуационными стимулирующими факторами из бесчисленного множества их можно назвать, например, бренд фирмы, численность управляемого линейным менеджером персонала, статус в коллективе предприятия, взаимоотношения с руководством, условия (комфортность) работы, место работы (удалённость от места жительства, транспортные удобства) и т.п.

У менеджера за компьютером или иным цифровым устройством (роботом, искусственным интеллектом) управление коллективом подменяется управлением информационными системами, включая решение таких задач, как:

- создание технологической среды информационной системы компании; эксплуатация информационных систем;
- совершенствование и обслуживание информационной системы;
- планирование в области информационных систем;
- создание организационной структуры в сфере информатизации;
- разработка инновационной политики предприятия и реализация инновационных программ;
- управление капиталовложениями и персоналом в области информатизации;
- разработка информационных ресурсов и обеспечение их комплексной защиты» [13, с. 551-552].

Это далеко не полный перечень задач информационного менеджера, от которого требуется не только высочайший уровень квалификации, но и огромная самоотдача, во многом зависящая от мотивации труда.

«За» и «Против» геймификации

Так можно ли повысить или активизировать мотивацию менеджера-фрилансера с помощью геймификации, которая в большинстве случаев рассматривается в аспекте коллектива, а в данном случае рассматривается применительно к одному самоуправляемому сотруднику?

То есть теория вопроса входит в рамки теории самоменеджмента - в отношении самодисциплины, целеустремлённости, интеллектуального и физического развития. По определению А.А.Симоновой, «Самоменеджмент – система способов деятельности, позволяющая максимально использовать собственные возможности, сознательно и рационально управлять своей жизнью, активно и эффективно влиять на внешние обстоятельства на работе и в личной жизни в своих целях» [14, с. 57]. Во многом это зависит от осознания своего места в мире.

По данным исследовательского института Gallup в отчёте за 2023 год, **59% сотрудников в мире, т.е. более половины, работают в состоянии стресса, без мотивации и вовлечённости.** К причинам снижения мотивации труда в отчёте отнесены:

- Сотрудник не видит смысла своей работы, не понимая своего вклада в общее дело, почему желание проявлять инициативу постепенно снижается;
- **Нет возможностей для своего развития, что** вызывает скуку и усталость;
- **Плохие отношения в коллективе**, коллеги конфликтуют и не уважают друг друга;
- **Недостаточно автономии в условиях** директивного типа руководства [15].

Кроме того, в докладе Gallup за 2024 год установлено: «20% сотрудников в мире ежедневно испытывают одиночество... Этот процент выше для сотрудников моложе 35 лет и ниже для тех, кто старше 35 лет. Полностью удаленные сотрудники сообщают о значительно более высоком уровне одиночества (25%), чем те, кто работает полностью на месте (16%). Социальная изоляция и хроническое одиночество оказывают разрушительное воздействие на физическое и психическое здоровье» [16]. По оценкам этого института, низкая вовлечённость сотрудника обходится мировой экономике в 8-9 трлн. долларов США, или 9% мирового ВВП.

Однако окажется ли геймификация лекарством от отмеченного снижения мотивации труда? По нашему мнению, игры в детском возрасте и во взрослом преследуют диаметрально противоположные цели: дети, играя с игрушками или в «дочки-матери», в «войнушки» и многие другие, хотят почувствовать себя взрослыми и, хоть действуют условно, «понарошку», стараются и пробуют жить в игре по-настоящему. В геймификации же сотрудникам производства, студентам вузов, ученикам в школе предлагается стать менее серьёзными, как бы вспомнить детство и решать серьёзную задачу играючи за приобретение победителям игрушек. Важно и другое: смысл, цель, вкладываемые в игру. Можно вспомнить слова из арии Германа в опере П.И.Чайковского «Пиковая дама»: «Что наша жизнь - игра... Сегодня ты, а завтра я. Так бросьте же борьбу, ловите миг удачи! Пусть неудачник плачет, кляня свою судьбу». Игра, предполагает, во-первых, удачу и, во-вторых, победу над соперником. Это принцип конкуренции в рыночной экономике, но приводит он к тому, что, по словам Джона Клифтона генерального директора Gallup, «...психическое благополучие людей ухудшается. За последние 10 лет число людей, выражающих стресс, грусть, беспокойство, гнев или беспокойство, растёт, достигая своего пика уровня с момента начала опросов Гэлапа» [16].

Ещё более прямолинейно и обоснованно рассмотрена проблема человеческой неудовлетворённости нынешней действительностью в «Докладе о человеческом развитии 2021-2022», подготовленном Отделом ООН и озаглавленном авторами «Времена неопределённости, неустроенности жизни: Наше будущее в меняющемся мире», где в предисловии к докладу Ахим Штайнер - Администратор Программы Развития Организации Объединенных Наций сообщает, что «шесть из семи человек во всём мире сообщали о том, что чувствовали себя неуверенно во многих аспектах своей жизни даже до пандемии Covid-19» [17],

основными причинами чего в докладе называются: политическая поляризация, экономическое неравенство, тенденция отступления от демократии во всех странах, распространение дезинформации через интернет-сети и многое другое, в результате чего уровень незащищённости человека возрастает уже на протяжении долгого времени.

Геймификация, внедрённая в систему управления компании, не исключает в качестве главного – материальный стимул, не снимает проблем социальной напряжённости, связанной с неравенством жизненного уровня разных слоёв населения и разных стран; на предприятии она в среде персонала может улучшить психологический климат лишь на короткий промежуток времени, поскольку на него более сильно влияют диспропорции социального бытия, антагонизм рыночной конкуренции, неуверенность в завтрашнем дне.

Но, если обратиться к ушедшему в прошлое советскому периоду, то геймификацией можно назвать моральные, идеологические и организационные факторы: октябрятские, пионерские, комсомольские, партийные и профсоюзные организации с моральными кодексами, клятвами, атрибутами (значки, галстуки, вымпелы, знамёна, ордена и медали), сборами, пионерскими кострами, слётами, съездами и т.п.; социалистические соревнования; бригады и ударники коммунистического труда; присвоение звания героя социалистического труда и многое другое, содержавшее в какой-то мере игровые технологии, позитивно влиявшие на результаты процессов труда, обучения, воспитания и сплотивавших в коллектив на основе взаимопомощи даже в состязаниях. В то время не было цифровизации – неперемного фактора современной геймификации. Но была уверенность в будущем человечества, названного коммунистическим, где человек человеку друг, товарищ и брат. Именно стремление к достижению – пусть даже не в обозримом будущем – всеобщего равенства и благополучия вызывало самоотверженный энтузиазм, готовность раньше думать о Родине, а потом о себе, стремление опережающими темпами в более короткие сроки выполнять плановые пятилетки, а затем семилетки. Элементы игры использовались как идеологические стимулы состязательности во имя, как говорилось, светлого будущего, а не ради эгоистических устремлений. В этом состоит принципиальная разница между применением технологии геймификации в общенародной и в рыночной экономиках. Эта модель построения более совершенного общества, разрушенная при распаде СССР, показывала стремительный рост народного хозяйства, прерванный при переходе к рыночной системе, но получающий в настоящее время подтверждение его позитивных трендов в социалистическом Китае, выходящем сейчас на передовые позиции в мировом экономическом развитии.

Выводы.

1. Использование игровых технологий (геймификации) в деятельности персонала предприятия, менеджеров низшего звена, теряющего специфичность линейных менеджеров на пути их превращения в фрилансеров, работающих в условиях преимущественно не коллективного, а индивидуального труда (всё

чаще удалённого), может использоваться преимущественно на основе самоменеджмента, но не решает задачи повышения эффективности труда за счёт соревнования, поскольку в условиях рынка геймификация основывается на конкуренции, разъединяющей соперников, а не на партнёрстве.

2. Геймификация отвлекает участников деловой игры от идеи производства, сосредотачивая интерес персонала на не значимых для задач производства стимулах.

3. В условиях развития цифровизации производства сокращение коллективного труда, преобразование работников во фрилансеров потребует более глобальных стимулов труда, направленных на решение задач развития социума, окружающей среды, сохранения мира на планете, чему никакая геймификация способствовать не будет.

4. При сравнении с историческим, хоть и относительно коротким, периодом становления и развития СССР, времени, когда энтузиазм, вызванный стремлением народа улучшить жизнь всего мира, совершал удивительные трудовые, а затем и боевые подвиги, возникает гипотетический вывод о необходимости иного, не капиталистического мироустройства. Этого в работах указанных выше авторов нет, и ещё требуются обстоятельные исследования в данном направлении, что в какой-то мере составляет цель данной статьи.

5. Устранять развивающуюся в настоящее время неудовлетворённость в труде (косвенно, в жизни) не удастся паллиативной мерой внедрения геймификации, а требуется изменение миропорядка в неоиндустриальной экономике, которая развивается в направлении производства благ, достаточного для удовлетворения потребностей всего населения планеты, но требующего не рыночной, а планово-распределительной системы хозяйствования. Над этим следует задуматься сообща учёным всего мира, чтобы сначала разработать модель не только того, как в условиях совершенного производства производить достаточное количество благ для жизни человека, но и как их распределять каждому субъекту социума в равно необходимой мере.

Список источников

1. Электронный ресурс – режим доступа: <https://www.gamification-now.ru/blog/kratkaya-istoriya-geymifikacii> (дата обращения 26-11-2024)

2. Josef Folcman 70% Of Workers Aren't Engaged -- What About The Managers? [Электронный ресурс] – режим доступа: <https://www.forbes.com/sites/joefolkman/2014/03/06/seventy-percent-of-workers-not-engaged-what-about-the-managers/> (дата обращения 16.10.2024).

3. Курило В. Геймификация в HR, примеры внедрение геймификации в управлении персоналом, мотивации / В.Курило [Электронный ресурс] режим доступа: https://top-career.ru/blog/gamification_in_hr (Дата обращения 14.10.2024).

4. Замена людей роботами: угроза человечеству и безработица - [Элек-

тронный ресурс] – режим доступа: <https://viafuture.ru/katalog-idej/zamena-lyudej-robotami> (дата обращения 07.10.2024).

5. Создание полностью автоматизированных производств без участия человека - перспектива ближайших лет. [Электронный ресурс] – режим доступа: <https://asi.ru/news/24159/> (дата обращения 07.10.2024).

6. Октализ Ю-Кай Чоу: введение — Gamedev на DTF [Электронный ресурс] – режим доступа: <https://dtf.ru/gamedev/1074587-oktaliz-yu-kai-chou-vvedenie?ysclid=m20f5i6s9t144292620> (дата обращения 08.10.2024).

7. Смирнова П.В. Технологии геймификации: обзор научных публикаций / П.В.Смирнова, О.В.Кононова // Альманах научных работ молодых ученых XLVIII научной и учебно-методической конференции Университета ИТМО, 2023. - Том 3. – С. 189-191. = (Дата обращения 16.10.2024).

8. К.Вербах Вовлекай и властвуй: игровое мышление на службе бизнеса / К.Вербах, Д.Хантер. - М.: Манн, Иванов и Фербер (МИФ), 2015. – 224 с. (For the Win: How Game Thinking Can Revolutionize Your Business Paperback – Publisher : Wharton School Press (October 30, 2012) Language : English Paperback : 148 pages

9. Burke, Brian, 1959- Gamify : how gamification motivates people to do extraordinary things / Brian Burke. pages cm Includes bibliographical references and index.

10. Scott Meyers Conditions for Manager Motivation // Harvard Business Review January 1966 [Электронный ресурс] – режим доступа: <https://hbr.org/1966/01/conditions-for-manager-motivation> (дата обращения 15.09.2023).

11. Куликова О.В. Особенности мотивации менеджеров высшего и среднего звена в современных организационных условиях / О.В.Куликова, О.В.Бубнова // Современные проблемы науки и образования, 2015. - № 1-1 – С. 1537-1543.

12. Нр Краткий обзор ситуации на рынке труда за май 2023 года – [Электронный ресурс] режим доступа: https://corp.ryazangov.ru/pluginfile.php/479/mod_page/intro/hh.ru%20Обзор%20рынка%20труда%20Май%202023.pdf Презентация PowerPoint (дата обращения 16.08.2023).

13. Гультияева М.А. Специфика менеджмента в условиях цифровой экономики / М.А.Гультияева, И.А.Белорусова, В.О.Ожегов // Вопросы студенческой науки, 2022. - Выпуск №5 (69). – С. 549-553.

14. Симонова А.А. Самоменеджмент как технология управления и саморазвития педагога / А.А.Симонова // Инновационные проекты и программы в образовании, 2019. - № 2. – С. 57-65.

15. Отчёт Гэллэпи - [Электронный ресурс] режим доступа: https://vk.com/away.php?to=https%3A%2F%2Fdisk.yandex.ru%2Fi%2Fq-c0bfEd7pCkuw&post=-165599385_1751&cc_key

16. State of the Global Workplace: 2024 Report - [Электронный ресурс] ре-

жим доступа: From the CEO state-of-the-global-workplace-2024-key-insights.pdf
(Дата обращения 18.10.2024)

17. Доклад о человеческом развитии: Наше будущее в меняющемся мире»
[Электронный ресурс] режим доступа: <https://www.un-ilibrary.org/content/books/9789210016452> (Дата обращения 25.11.2024)

РАЗДЕЛ II.
СОВРЕМЕННАЯ
МЕДИЦИНА:
АКТУАЛЬНЫЕ ВОПРОСЫ,
ДОСТИЖЕНИЯ И
ИННОВАЦИИ

УДК 616.155.1-008.1

ГЛАВА 8. РАЗРАБОТКА МЕДИЦИНСКИХ ИЗДЕЛИЙ ДЛЯ КРИОКОНСЕРВИРОВАНИЯ ЭРИТРОЦИТОВ ДОНОРСКОЙ КРОВИ

Чечеткин Александр Викторович

д.м.н., профессор, ведущий научный сотрудник
научно-исследовательского отдела организации научной деятельности
ФГБУ «Всероссийский центр экстренной и радиационной медицины
имени А.М. Никифорова» МЧС России

Аннотация: представлены сведения о новых разработках медицинских изделий в области криоконсервирования эритроцитов. Показаны результаты исследования эффективности использования разработанных полимерных криоконтейнеров отечественного производства, контейнеров для отмывания размороженных эритроцитов, нового добавочного раствора для хранения декриоконсервированных эритроцитов. Дан анализ результатов использования методики отсроченного отмывания для пролонгированного хранения размороженной и отмывтой эритроцитной взвеси.

Ключевые слова: криоконсервирование эритроцитов, размороженная и отмываемая эритроцитная взвесь, криоконтейнер.

DEVELOPMENT OF MEDICAL DEVICES FOR CRYOPRESERVATION OF ERYTHROCYTES OF DONATED BLOOD

Chechetkin Alexander Viktorovich

Abstract: information on new developments in medical devices in the field of cryopreservation of erythrocytes is presented. The results of a study of the effectiveness of using the developed polymer cryocontainers of domestic production, containers for washing thawed erythrocytes, and a new additive solution for storing decryopreserved erythrocytes are shown. The analysis of the results of using the delayed washing technique for prolonged storage of thawed and washed erythrocyte suspension is given.

Keywords: cryopreservation of erythrocytes, thawed and washed erythrocyte suspension, cryocontainer.

Криоконсервирование эритроцитов эффективно используется в трансфузиологии при длительном хранении красных клеток крови как для клинических целей, так и в интересах производства медицинских изделий (в основном реагентов для лабораторных исследований) и научно-исследовательских целях. Основное применение криоконсервирования эритроцитов в медицинских целях – создание запасов эритроцитных компонентов крови на случай увеличения спроса на трансфузионные средства при чрезвычайных ситуациях, для обеспе-

чения пациентов с редкой групповой принадлежностью или поддержание необходимого уровня выдачи для переливания компонентов крови в периоды низкой донорской активности.

Криоконсервирование эритроцитов было внедрено в практику почти семьдесят лет назад и в течение последующего времени технологии замораживания и хранения клеток крови постоянно совершенствовались. Основная проблема при криоконсервировании эритроцитов заключалась не в поддержании экстремально низких температур, а в безопасном выдерживании промежуточной температурной зоны (примерно от -10° до -60° С), которой клетки подвергались дважды — во время охлаждения и размораживания. Температура в этом диапазоне может повредить клетки из-за несбалансированного трансмембранного переноса воды — процесса, зависящего от температуры. Если молекулам воды не дать достаточно времени для трансмембранного перехода, возникает повреждение из-за образования внутриклеточного льда, что приводит к механическому повреждению клеток. Если молекулы воды выходят слишком быстро, повреждение может возникнуть из-за дегидратации клеток и связанных с этим изменений концентрации растворённых веществ внутри клеток. Между этими двумя крайними случаями существуют оптимальные скорости охлаждения и нагревания, которые минимизируют повреждение эритроцитов при замораживании и размораживании. Поэтому для этих целей применяют криопротекторы, которые регулируют транспорт воды через мембрану клеток и препятствуют образованию внутриклеточного льда. Наиболее широко используемым криопротектором для криоконсервирования эритроцитов является глицерин, который проникает в клетки посредством облегчённого транспорта, оставаясь при этом нетоксичным в высоких концентрациях. Были разработаны два протокола криоконсервирования эритроцитов с использованием глицерина: с высоким содержанием глицерина (примерно 40–50% по массе) и с низким содержанием глицерина (около 15–20% по массе).

На протяжении многих десятилетий в нашей стране был наиболее широко распространён метод быстрого замораживания эритроцитов в жидком азоте (-196° С) с криозащитным раствором, содержащим 30–40% глицерина (растворы ЦНИИГПК 11₄, ЦНИИГПК 11₅). Ежегодно этим методом замораживали более 3000 доз эритроцитов [1, с.17]. В целях упрощения и удешевления процесса криоконсервирования проводились многочисленные исследования, направленные на отказ от дорогостоящего и громоздкого жидкоазотного оборудования и перевод процесса криоконсервирования эритроцитов в диапазон низких (-65° ... -80° С) и умеренно низких (-20° ... -60° С) температур. Был предложен для клинического применения метод криоконсервирования эритроцитов при -40° С с использованием 39,6% раствора глицерина [2, с. 45].

Продемонстрированы возможности использования гидрооксиэтилкрахмала (ГЭК) для замораживания и хранения эритроцитов. Преимуществом ГЭК является отсутствие необходимости в отмывании клеток после их оттаивания. Размороженные клетки крови переливают реципиенту вместе с криофилактиком,

либо после его частичного удаления после предварительного центрифугирования. Для замораживания эритроцитов под защитой 6,7% раствора ГЭК применяли быстрое замораживание и быстрый отогрев образцов эритроцитов. Результаты показали, что эритроциты, замороженные с помощью ГЭК, сохраняют больше гемоглобина, чем при использовании глицерина. Проницаемость мембран для ионов натрия и калия лучше сохраняется при использовании ГЭК. Однако требуются дополнительные исследования для оценки возможности ГЭК как криопротектора для замораживания эритроцитов [3, с. 15].

Имеются экспериментальные данные по использованию для замораживания эритроцитов пропандиосахароля, диметилацетамида, поливинилпирролидона и других криофилактиков.

Достаточно устойчивые результаты были получены при долгосрочном хранении криоконсервированных эритроцитов при -80°C . J. Lesak и соавт. [4, с. 1306] исследовали 20 доз эритроцитов, криоконсервированных в 40% глицерине и хранившихся при -80°C более 10 лет. Трансфузионные среды имели достаточное количество сохранившихся клеток, нормальные их морфологические характеристики, функцию транспорта кислорода и осмотическую стойкость. Жизнеспособность *in vitro* и функции криоконсервированных эритроцитов не зависели от длительности хранения в замороженном виде или хранения при 4°C после оттаивания. Описан успешный опыт хранения эритроцитов в замороженном состоянии с 40% раствором глицерина при -80°C в течение 37 лет [5, с. 168].

Ранее для замораживания эритроцитов использовались аппараты – ванны с жидким азотом. Процесс замораживания эритроцитов происходил в среде жидкого азота, как правило, до двух минут. В отдельных случаях могут применяться для замораживания эритроцитов электрические холодильники с диапазоном температур от -30°C до -150°C , выпускаемые различными производителями.

Для хранения замороженных эритроцитов использовались жидкоазотные хранилища и в последние годы – электрические холодильники. В начале семидесятых годов прошлого века в нашей стране были созданы хранилища серии ХБ различной емкости. В различной степени модификации они использовались в службе крови страны до 2010 года.

За рубежом налажен выпуск хранилищ различной емкости (от 200 до 1000 л): СВХ (Великобритания), серии К (США-Германия), Biostore (Великобритания), MVE (США), Biosystem (Великобритания) и др.

Для хранения единиц эритроцитов в жидком азоте и его парах наиболее широко использовались алюминиевые многоразовые контейнеры емкостью 290 мл, разработанные в шестидесятые годы прошлого столетия и имеющие ряд существенных недостатков. К ним относится определенная биологическая активность алюминия, а также техническая сложность и дороговизна производства алюминиевых контейнеров. Повторное использование таких контейнеров очень ограничено, поскольку их трудно отмывать, кроме того, остающиеся после отмывания следы щелочей затрудняли контроль качества.

Поэтому возникла необходимость разработки полимерных контейнеров

для замораживания клеток крови, прежде всего эритроцитов. К таким контейнерам предъявляется целый ряд требований, наиболее важными из которых являются: биологическая инертность материалов, высокая механическая прочность в широком диапазоне температур ($-30^{\circ}\dots-196^{\circ}\text{C}$), большая теплопроводность, равномерность охлаждения биоматериала, герметичность контейнеров, а также технологичность и невысокая стоимость изготовления.

За рубежом для криоконсервирования эритроцитов были разработаны полимерные контейнеры Maco Biotech Freezing («Macopharma», Франция), Cryocyte («Baxter-Fenwal», США), Hemofreeze («Fresenius Hemocare», Германия), Cryostore («Origen Biomedical», США), Kryosure («American Fluoroseal Company», США), Safe2 («SIAD Healthcare», Италия). Большинство криоконтейнеров производят из этилвинилацетата, Hemofreeze – из тефлона. Контейнеры из этилвинилацетата имеют соединительные трубки, которые запаивают высокочастотным запаивателем для полимерных магистралей. Использование Hemofreeze требует специального устройства, герметизирующего криоконтейнер. Отечественные криоконтейнеры для замораживания эритроцитов до 2008 года не производились. Имелись попытки использования полимерных контейнеров типа «Гемакон» для замораживания и хранения эритроцитов при температуре до -140°C .

Для размораживания эритроцитов использовались устройства, представляющие собой ванну с электроподогревом воды до $37^{\circ} - 45^{\circ}\text{C}$, в которой осуществлялся процесс размораживания при покачивании контейнеров.

Для отмывания эритроцитов от криопротектора применялись различные технические средства:

- аппараты, работающие на принципе центрифугирования: РК-0,5 («БФА», Россия), Haemonetics -15 (США), Haemonetics-50, (США);
- рефрижераторные центрифуги различного типа, например Jouan KR 4i («Jouan», Франция), Sorval RC -3C Plus («Kendro-Sorval», США) и др.

Заслуживают исторического упоминания цитоаггломераторы, работающие на принципе ускоренного осаждения путем обратимой аггломерации клеток в слабо кислых неэлектролитных растворах с низкой ионной силой, однако такие аппараты в настоящее время не используются и не разрабатываются.

В последние годы в центрах крови используется аппарат для автоматической глицеринизации и деглицеринизации эритроцитов Haemonetics ACP 215. Обеспечивая функционально закрытую систему, ACP 215 позволяет хранить эритроциты, взвешенные после размораживания в ресуспендирующем растворе типа AS-3, как рекомендует производитель в течение 7 суток после приготовления, в России разрешенный срок хранения в растворе SAG-M составляет 72 часа с момента деглицеринизации.

Учитывая острую необходимость в развитии технологического обеспечения криоконсервирования эритроцитов группой ученых из Москвы и Санкт-Петербурга был разработан первый отечественный криоконтейнер для замораживания и хранения биопродуктов, содержащий снабженную штуцером ем-

кость из многослойного пленочного материала, имеющего один слой полиимидной пленки с наружной стороны и один слой фторполимерной пленки с внутренней стороны [6]. В него введен блок штуцеров, на котором расположены два штуцера, первый для заполнения контейнера эритроцитной взвесью, а второй для эксфузии эритроцитов из контейнера, при этом корпус блока штуцеров выполнен из термопластичного материала, имеет полость, соединенную с полостями штуцеров и полостью контейнера, и фланец для крепления к внутренней стенке контейнера, а штуцер для заполнения контейнера снабжен промежуточным колпачком, выполненным в виде двух цилиндров разного диаметра, разделенных перегородкой с фланцем, и цилиндрическим выступом, соосным цилиндру большего диаметра, внутри которого между его внутренней стенкой и стенкой выступа установлен герметизирующий колпачок. Производство таких криоконтейнеров наладило ООО НПП "АВАНГАРД-МТ" (г. Москва).

Были проведены доклинические исследования эффективности использования отечественных криоконтейнеров при замораживании, хранении при температуре -196°C с криозащитным раствором, содержащим 30-40% глицерина, и размораживании эритроцитов (табл. 1).

Таблица 1

Гематологические и биохимические показатели размороженной и отмытой эритроцитной взвеси

| Показатели | С использованием зарубежного полимерного контейнера | С использованием отечественного полимерного контейнера |
|----------------------------------|---|--|
| Гематокрит, л/л | $0,41 \pm 0,01$ | $0,41 \pm 0,02$ |
| Содержание гемоглобина в дозе, г | $46,2 \pm 1,0$ | $41,4 \pm 2,9$ |
| Сохранность клеток, % | $92,1 \pm 2,1$ | $91,2 \pm 1,6$ |
| Содержание ионов калия, ммоль/л | $1,11 \pm 0,03$ | $1,21 \pm 0,06$ |
| Осмолярность, мОсм/л | $313,9 \pm 2,1$ | $314,0 \pm 2,7$ |

Установлено, что гематокрит, содержание гемоглобина и ионов калия существенных различий между группами образцов не имели. Использование полимерных контейнеров позволило сохранять более 91% красных клеток крови от их исходного количества. Биохимический состав супернатанта декриоконсервированной и отмытой эритроцитной взвеси не имел существенных различий в зависимости от методики криоконсервирования. Осмолярность супернатанта декриоконсервированной и отмытой эритроцитной взвеси во всех наблюдениях не превышала рекомендуемых требований и не имела различий между исследуемыми группами образцов.

Следовательно, по основным лабораторным показателям эритроцитная

взвесь, замороженная с использованием разработанного отечественного крио-контейнера, не отличалась от компонентов, криоконсервированных в зарубежных аналогах.

Учитывая, что автоматический метод деглицеринизации эритроцитов может быть доступен не всем медицинским организациям, в этом случае применяется ручное дискретное отмывание с солевыми растворами.

С целью повышения безопасности технологии декриоконсервирования и профилактики бактериальной контаминации была разработана новая модель контейнера для жидкостей, применяющихся при криоконсервировании и отмывании эритроцитов [7]. Этим были созданы условия для полностью закрытой системы на всех этапах ручного криоконсервирования и отмывания эритроцитной массы. Разработанный контейнер для вспомогательных растворов, выполненный в виде емкости из полимерного материала, содержит удлиненную эластичную полимерную трубку (отвод), используемую как для заполнения, так и для соединения с рабочими контейнерами. Отвод, выполненный в виде полимерной трубки, позволяет соединять контейнер со вспомогательным раствором с рабочим контейнером с помощью стерильного соединения двух полимерных трубок в устройстве для стерильного соединения пластиковых магистралей. Контейнер может дополнительно иметь штуцер, размещенный в непосредственной близости от соединительной трубки и предназначенный для отдельного присоединения медицинских изделий. Разработанный контейнер является необходимым и достаточным элементом, позволяющим создать полностью закрытую систему на всех этапах ручного криоконсервирования и отмывания эритроцитной массы, что, в свою очередь, резко снижает риск бактериальной контаминации эритроцитной массы в процессе ее обработки.

Потенциальное нарушение стерильности, вызванное вскрытием контейнера для переноса глицеринизированных эритроцитов в контейнер для замораживания, а также последующее после размораживания переливание эритроцитов в систему для отмывания, имеет потенциальный риск бактериальной контаминации, что привело к появлению законодательно установленных требований, чтобы размороженные по «открытой» методике эритроциты хранились до переливания при 4° С не более 1 суток. Для пролонгированного хранения размороженных и отмываемых эритроцитов предлагаются уже имеющиеся растворы для нативных эритроцитов: SAG-M, AS-3, AS-1, AS-5, а также их экспериментальные сочетания с глюкозо-солевым раствором. Наиболее часто используются SAG-M, изотонический 0,9 % раствор хлорида натрия или глюкозо-солевой раствор (при аппаратном методе деглицеринизации), а также раствор ЦНИИГПК8в (Ресин) – при ручном (открытом) методе отмывания. Однако эти растворы не учитывают особенностей жизнедеятельности размороженных, деглицеринизированных, полностью лишенных плазмы, гиперосмолярных эритроцитов. Отечественные растворы, предназначенные для пролонгированного хранения размороженных отмываемых эритроцитов с учетом их метаболизма, в Российской Федерации не производятся. Поэтому был разработан первый отечественный доба-

вочный раствор для хранения размороженных и отмытых эритроцитов метаболического действия [8].

Разработанный добавочный раствор для хранения отмытых и размороженных эритроцитов включает соль натрия, глюкозу и аденин, фумарат натрия и смесь одно- и двузамещенных фосфатов натрия, а также сахарозу для повышения осмолярности раствора, причем компоненты взяты в следующем соотношении (в ммоль/л): $46,3 \pm 6,9$ – фумарата натрия, $12,2 \pm 4,5$ – однозамещенного фосфата натрия, $10,5 \pm 3,6$ – двузамещенного фосфата натрия, $40,4 \pm 0,1$ – глюкозы, $1,47 \pm 0,01$ – аденина и $88,8 \pm 1,7$ – сахарозы. Раствор может дополнительно включать $4,3 \pm 0,5$ ммоль/л цитрата натрия. Предлагаемый добавочный раствор эффективен при гипотермическом хранении отмытых и размороженных эритроцитов, сохраняет их количество и функциональную активность во всем периоде хранения. Для успешного применения взвесь эритроцитов должна соответствовать определенным показателям, характеризующим морфофункциональную сохранность эритроцитов, таким как уровень свободного гемоглобина, процент гемолиза (количество разрушенных клеток), процент осмотически неустойчивых эритроцитов, их морфология, содержание аденозинтрифосфорной кислоты (АТФ) и др. При хранении нативных эритроцитов в виде взвеси в добавочном растворе ставится задача сохранения морфофункциональной активности эритроцитов на срок не менее до 42 суток. Криоконсервирование позволяет сохранять морфофункциональную активность эритроцитов достаточно продолжительное время, а после размораживания и отмывания эритроциты необходимо хранить только то время, которое требуется для доставки эритроцитной взвеси пациенту, особенно при значительной удаленности медицинских организаций от станций переливания крови (центров крови). Поэтому 6-7 суток хранения эритроцитной взвеси в добавочном растворе считается достаточным сроком, и возникает вопрос о наилучших показателях их морфофункциональной сохранности. Это достигается тем, что добавочный раствор для хранения размороженных и отмытых эритроцитов содержит метаболический субстрат – фумарат натрия. Выбор фумарата натрия как компонента добавочного раствора в значительной степени обусловлен положительным опытом его использования в виде инфузионных растворов антигипоксического действия. Кроме того, действие фумарата достаточно детально изучено в эксперименте. Как показывают исследования, фумарат, введенный перорально в виде фумаровой кислоты, повышает резистентность организма к самым разнообразным сверхнормальным воздействиям (физические перегрузки, недостаток кислорода, гиперкапния и др.). По-видимому, фумарат относится к числу естественных метаболитов, эволюционно отобранных в качестве универсальных адаптогенов. Поэтому траты эндогенного фумарата в организме, особенно в экстремальных условиях, весьма велики. Многие исследователи относят фумарат к числу актопротекторов, так называемых «физиологичных» лекарственных средств, вырабатываемых в организме людей и животных и способствующих повышению иммунитета, а также защитных сил. Оказывая лечебное действие, фумарат не вызывает небла-

гоприятных побочных эффектов, поскольку в ходе его биотрансформации в организме не образуется токсичных продуктов. Действительно, опыты показывают, что фумарат практически не токсичен, не накапливается в органах и тканях при длительном применении в оптимальной и десятикратно превышающей ее дозах, не влияет отрицательно на течение беременности, не обладает тератогенным и эмбриотоксическим действием. С учетом такой биологической роли фумарата в организме, он был предложен в состав добавочного раствора для хранения декриоконсервированных эритроцитов.

По-новому проблему увеличения максимально допустимого срока хранения размороженных эритроцитов решает метод, предполагающий отмывание эритроцитов от криопротектора и продуктов распада клеток не сразу после размораживания, а после хранения в криозащитной среде при 4°C вплоть до момента предполагаемого использования, разработанный группой исследователей из Санкт-Петербурга [9, с. 17].

Сущность методики сводится к проведению процедуры деглицеринизации не сразу после размораживания эритроцитов, а непосредственно перед их переливанием после хранения при 4°C в криозащитном растворе. Соблюдение лишь этого условия без каких-либо материальных затрат, использования сложных и дорогих ресуспендирующих растворов, а также отсутствие необходимости разгерметизации емкости со взвесью эритроцитов непосредственно после оттаивания обеспечивает существенное увеличение максимально допустимого срока их хранения, что упрощает реализацию размороженных эритроцитов и дает возможность их транспортировки на значительные расстояния.

На основании результатов исследования установлено, что содержание свободного гемоглобина, количество осмотически неустойчивых эритроцитов, процент гемолиза, морфологический индекс, р50, содержание гемоглобина в дозе не имели различий между взвесьями отсрочено отмываемых и отмываемых в день размораживания эритроцитов. Содержание АТФ во взвесьях отмываемых размороженных эритроцитов соответствовало $5,78 \pm 0,28$ мкмоль/г Hb, в отсрочено отмываемых размороженных эритроцитах этот показатель составил $5,45 \pm 0,31$ мкмоль/г Hb, что выше средних данных для эритроцитарной массы, предназначенной для криоконсервирования – $4,85 \pm 0,49$ мкмоль/г Hb. Содержание в дозе гемоглобина ($46,6 \pm 1,22$ г и $45,2 \pm 1,28$) и процента сохраненных клеток ($82,0 \pm 1,55$ и $78,9 \pm 2,74$) имело тенденцию к повышению во взвесьях отсрочено отмываемых через неделю размороженных эритроцитов. Предложенный способ отмывания криоконсервированных эритроцитов обеспечивает возможность их пролонгированного хранения при 4°C в криозащитной среде до 7-14 суток.

Оценка качества размороженных и отмываемых эритроцитов осуществлялась, начиная с внедрения метода криоконсервирования в медицинскую практику, однако получаемые результаты часто варьировали в широких пределах. Стандартизировать параметры размороженных эритроцитов для клинического применения удалось во многом благодаря внедрению автоматизированной системы Haemonetics ACP 215, при использовании которой остаточная концентрация

глицерина была ниже порога гемолиза эритроцитов, окончательный гемолиз при промывании составлял менее 1%, восстановление эритроцитов через 24 часа после переливания составляло более 75%. Установлено, что общее содержание оксида азота (NO) в гемоглобине не различается существенно в зависимости от условий криоконсервирования, хотя замораживание (независимо от добавления глицерина) незначительно повышало уровень NO. С помощью метода жидкостной хроматографии и тандемной масс-спектрометрии был проведен анализ свежих, криоконсервированных и деглицерированных эритроцитов [10]. Результаты показали схожие показатели потребления глюкозы и продукции лактата в обеих группах в течение 6 часов. Свежие эритроциты характеризовались значительно более высоким уровнем лактата в надосадочной жидкости, но не внутри клеток, по сравнению с криоконсервированными. И наоборот, деглицеринизированные эритроциты характеризовались более быстрым гликолизом, чем свежие эритроциты. Соотношение внутриклеточного гликолиза и пентозофосфатного пути было сопоставимым в свежих и деглицерированных эритроцитах. Деглицерированные эритроциты также характеризовались более низким уровнем окисленного глутатиона и более высоким соотношением восстановленного и окисленного глутатиона по сравнению со свежими эритроцитами, что указывает на снижение окислительного повреждения при окислительной нагрузке по сравнению со свежими эритроцитами.

Основные направления дальнейшего развития криоконсервирования эритроцитов включают в себя разработки новых криопротекторов и добавочных растворов, усовершенствованных технологий хранения размороженных эритроцитов. В качестве новых криопротекторов рассматривается трегалоза, поскольку она хорошо известна своей ролью в защите клеток и организмов от различных неблагоприятных факторов, однако при нормальных условиях обладает очень низкой проницаемостью для мембраны эритроцитов. Поэтому исследования сосредоточены на методах доставки трегалозы в клетки с использованием липосом, загруженных трегалозой, мембранопроницаемых биополимеров, электропроводимости и химических методов. Показано, что, три биосовместимые нейтральные аминокислоты, включая β -аланин, γ -аминомасляную кислоту и ϵ -аминокапроновую кислоту, обладают потенциалом в качестве идеальных криопротекторов [11, с. 2640]. Они могут ингибировать образование льда и снижать осмотический стресс, обеспечивая внеклеточную и внутриклеточную защиту, тем самым обеспечивая высокую эффективность криоконсервации клеток крови.

Таким образом, технические средства для криоконсервирования эритроцитов отличаются сложностью и дороговизной, а современные подходы к использованию аппаратов для замораживания и размораживания, а также расходных материалов для криоконсервирования эритроцитов нуждаются в совершенствовании. Поэтому разработка новых медицинских изделий и методик замораживания, хранения и размораживания эритроцитов является актуальной научной проблемой. Создание полимерных криоконтейнеров для замораживания клеток

крови, контейнеров для их отмывания, новых добавочных растворов для хранения декриоконсервированных эритроцитов, а также внедрение методики отсроченного отмывания эритроцитов позволят повысить эффективность и безопасность применения размороженных и отмытых эритроцитов в медицинской практике.

Список источников

1. Селиванов Е.А., Чечеткин А.В., Григорьян М.Ш., Макеев А.Б. Состояние и проблемы криоконсервирования эритроцитов в службе крови Российской Федерации // Трансфузиология.– 2012.– № 2.– С. 14-20.
2. Чечеткин А.В., Данильченко В.В., Волкова С.Д., Макеев А.Б., Солдатенков В.Е., Кирьянова Г.Ю., Касьянов А.Д., Голованова И.С. Организационные аспекты использования криоконсервирования эритроцитов в деятельности учреждений службы крови Российской Федерации // Вестн. междунар. акад. холода.– 2015.– № 3.– С. 45-49.
3. Korsak J., Goller A., Rzeszotarska A., Pleskacz K. Evaluation of two distinct cryoprotectants for cryopreservation of human red blood cell concentrates // Cryo Letters. – 2014 – Vol.35, № 1.– P.15-21.
4. Lecak J., Scott K., Young C., Hannon J., Acker J.P. Evaluation of red blood cells stored at -80°C in excess of 10 years // Transfusion.– 2004. – Vol. 44, № 6.– P. 1306-1313
5. Valeri C.R., Rango G., Privacek L.E. An experiment with glycerol-frozen red blood stored at -80 degrees C for up to 37 years // Vox Sang. – 2000. – Vol. 79, № 3. – P. 168-174.
6. Анисимов Н.А., Шишов Н.М., Зеленецкий В.Е., Демина Н.А., Шишов С.Н., Федоров Ф.А., Христофоров Н.В., Онуфриевич А.Д., Чечеткин А.В. Контейнер для замораживания и хранения биопродуктов. Патент на изобретение RU 2381783. Заявка № 2007139098/14 от 23.10.2007. Опубликовано 20.02.2010, Бюл. № 5.
7. Кирьянова Г.Ю., Волкова С.Д., Чечеткин А.В. Контейнер для жидкостей, применяющихся при криоконсервировании и отмывании эритроцитов. Патент на полезную модель RU 180533. Заявка № 2017109522 от 21.03.2017. Опубликовано 15.06.2018, Бюл. № 17
8. Кирьянова Г.Ю., Старицына Н.Н., Алексеева Н. Н., Гришина Г. В. Чечеткин А. В. Добавочный раствор для хранения отмытых размороженных эритроцитов. Патент на изобретение RU 2782185. Заявка № 2021107379 от 19.03.2021. Опубликовано 21.10.2022, Бюл. № 30.
9. Кирьянова Г.Ю., Волкова С.Д., Гришина Г.В., Касьянов А.Д., Голованова И.С., Чечеткин А.В. Пролонгированное хранение при 4°C размороженных красных клеток крови в криозащитном растворе до отмывания // Трансфузиология.– 2017.– № 4. – С. 17-28.

10. Rogers S.C., Dosier L.B., McMahon T.J. et al. Red blood cell phenotype fidelity following glycerol cryopreservation optimized for research purposes // PLoS ONE. – 2018.– Vol. 13, № 12: – Article e0209201. DOI: [org/10.1371/journal.pone.0209201](https://doi.org/10.1371/journal.pone.0209201).

11. Sui X., Chen P., Wen C. et al. Exploring novel cell cryoprotectants based on neutral amino acids // Chinese J. Chemical Engineering. – 2020. – Vol. 28, № 10.– P. 2640-2649.

УДК: 616.314-77

ГЛАВА 9. НАДО ЛИ УЧИТЫВАТЬ ОСОБЕННОСТИ КРОВООБРАЩЕНИЕ ПРОТЕЗНОГО ЛОЖА У ПАЦИЕНТОВ ДОНБАССА ПРИ ПОЛНОМ СЪЕМНОМ ПРОТЕЗИРОВАНИИ?

Воликов Валерий Владимирович

ассистент

Грабков Юрий Петрович

старший лаборант

Халаимова Виктория Игоревна

студентка

Гаврилов Владимир Алексеевич

д.м.н., профессор

ФГБОУ ВО ЛГМУ им. Свт. Луки Минздрава России, г. Луганск

Цель исследования: определить особенности микроциркуляции протезного ложа у пациентов Донбасса, подлежащих полному съемному протезированию, и её роль в стабилизации ортопедической конструкции. **Материал и методы исследования.** Исследование проведено у условно здоровых 32-х лиц обоего пола возрастом от 39 до 63 лет, постоянно проживающих на Донбассе, с использованием лазерного доплеровского флоуметра (ЛДФ). Измерения выполняли стандартным способом одним оператором в области десны на уровне середины коронки отсутствующих зубов в четырех точках: 11-й зуб, 21-й зуб, 16-й и 26-й зуб в течение 4 мин до получения устойчивых показателей (интактный показатель). Для стандартизации оценки микроциркуляции использовали измерение кровотока в области ладонной поверхности второго пальца левой кисти (пальцевой показатель). **Результаты исследования.** При анализе полученных данных, характеризующих уровень микроциркуляции, установлено, что у пациентов интактный показатель микроциркуляции в проекции альвеолярной десны отсутствующего 11-го зуба составлял в среднем $12,74 \pm 1,60$ ПЕ. Нагрузочный показатель колебался от 8,37 до 11,35 ПЕ. Интактный показатель микроциркуляции в проекции альвеолярной десны на уровне отсутствующего 21-го зуба колебался от 10,43 до 15,50 ПЕ. Показатель был на 3,40% больше у мужчин ($13,08 \pm 1,33$ ПЕ) по сравнению с женщинами ($12,65 \pm 1,38$ ПЕ) ($R \pm r = 0,941 \pm 0,195$ при $p < 0,05$). Нагрузочный показатель составлял в среднем $10,30 \pm 1,14$ ПЕ. Интактный показатель микроциркуляции в проекции альвеолярной десны на уровне отсутствующего 16-го зуба колебался от 10,21 до 14,93 ПЕ. Нагрузочный показатель колебался от 8,45 до 12,94 ПЕ, составляя в среднем $10,02 \pm 1,13$ ПЕ. Этот показатель был на 1,4% больше у мужчин ($10,09 \pm 1,33$ ПЕ) по сравнению с женщинами ($9,95 \pm 0,94$ ПЕ) ($R \pm r = 0,960 \pm 0,162$ при $p < 0,05$). **Заключение.** Полученные данные исследования особенностей микроциркуляции беззубых альвеолярных отростков верхней челюсти у пациентов Донбасса, подлежащих полному

съемному протезированию зубов, определены морфометрические параметры состояния кровообращения в той зоне, где располагаются базисы полных съемных зубных протезов, эти данные можно использовать как возрастную регионарную норму и как отправную «точку отчета» при контроле за динамикой убыли кости при анализе качества ортопедической конструкции и эффективности зубного протезирования.

Ключевые слова: микроциркуляция челюстных костей, лазерная доплеровская флоуметрия, полное съемное протезирование зубов.

IS IT NECESSARY TO TAKE INTO ACCOUNT THE PECULIARITIES OF THE BLOOD CIRCULATION OF THE PROSTHETIC BED IN DONBASS PATIENTS WITH COMPLETE REMOVABLE PROSTHETICS?

**Volikov Valetri Vladimirovich
Grabkov Yuri Petrovich,
Khalaimova Victoria Igorevna,
Gavrilov Vladimir Alekseevich**

The purpose of the study: to determine the features of microcirculation of the prosthetic bed in Donbass patients who are subject to complete removable prosthetics, and its role in stabilizing the orthopedic structure.

Research materials and methods. The study was conducted in conditionally healthy 32 individuals of both sexes aged 39 to 63 years, permanently residing in Donbas, using a laser Doppler flowmeter (LDF). Measurements were performed in a standard way by one operator in the gum area at the level of the middle of the crown of missing teeth at four points: 11th tooth, 21st tooth, 16th and 26th tooth for 4 minutes until stable indicators were obtained (intact indicator). To standardize the assessment of microcirculation, the measurement of blood flow in the area of the palmar surface of the second finger of the left hand (finger index) was used. The results of the study. When analyzing the data obtained characterizing the level of microcirculation, it was found that in patients, the intact microcirculation index in the projection of the alveolar gum of the missing 11th tooth averaged 12.74 ± 1.60 PE. The load index ranged from 8.37 to 11.35 PE. The intact microcirculation index in the projection of the alveolar gum at the level of the missing 21st tooth ranged from 10.43 to 15.50 PE. The index was 3.40% higher in men (13.08 ± 1.33 PE) compared with women (12.65 ± 1.38 PE) ($R_{\pm r} = 0.941 \pm 0.195$ at $p < 0.05$). The load index averaged 10.30 ± 1.14 PE. The intact microcirculation index in the projection of the alveolar gum at the level of the missing 16th tooth ranged from 10.21 to 14.93 PE. The load index ranged from 8.45 to 12.94 PE, averaging 10.02 ± 1.13 PE. This indicator was 1.4% higher in men (10.09 ± 1.33 PE) compared with women (9.95 ± 0.94 PE) ($R_{\pm r} = 0.960 \pm 0.162$ at $p < 0.05$).

Conclusion. The obtained data from the study of the microcirculation features of toothless alveolar processes of the upper jaw in Donbass patients subject to complete removable dentures, morphometric parameters of the circulatory state in the area where the bases of complete removable dentures are located, these data can be used as an age-related regional norm and as a starting point of the report when monitoring the dynamics of bone loss in the analysis the quality of orthopedic construction and the effectiveness of dental prosthetics.

Key words: microcirculation of the jaw bones, laser Doppler flowmetry, complete removable dentures.

Введение. Эффективность зубного протезирования подтверждается многими показателями, одним из наглядных и убедительных является стабильность

протеза в течение длительного времени. Литературные данные свидетельствуют, что устойчивость протеза на протезном ложе зависит от скорости его атрофии, которая прямопропорционально связана с уровнем кровообращения в нём [1, 2, 7].

Функциональные методы исследования кровотока отдельных органов дают возможность выявить их адаптационно-компенсаторные возможности, позволяют определить ранние донозологические признаки сосудистых изменений в пародонте и других тканях. Эти данные позволяют получить целый комплекс информации для определения и оценки эффективности патогенетической терапии, прогноза заболевания, его течения и объективно контролировать непосредственные и отдаленные результаты ортопедического лечения [2-4, 8, 9].

Важная роль в решении вопроса выбора ортопедического метода восстановления зубных рядов принадлежит изучению оксигенации и кровообращения тканей протезного ложа с помощью неинвазивных – функциональных методов исследования. Известно, что состояние репаративной регенерации, минерализации и ремоделирования костной ткани и их динамика напрямую зависит от интенсивности притока и оттока крови [3, 5- 7].

Изменения гемодинамических характеристик верхней челюсти в значительной мере отражает его функциональное состояние, поэтому определение диапазона нормативных показателей микроциркуляции альвеолярных отростков (протезного ложа) пациентов, проживающих на Донбассе, подлежащих полному съёмному протезированию, является актуальной задачей современной медицинской науки и могла бы в значительной мере помочь врачам и исследователям проводить рациональное протезирование зубов, добиваясь стабильности протезов в полости рта и сохранности опорных тканей протезного ложа [1, 3, 5, 8, 9]. Раннее подобных морфологических исследований не проводилось.

Цель нашего исследования – изучить особенности микроциркуляции протезного ложа беззубой верхней челюсти у пациентов, постоянно на Донбассе, подлежащих полному съёмному протезированию.

Материал и методы исследования.

Из 32 больных, которым выполнена ЛДФ тканей протезного ложа фронтального и дистального участков альвеолярных отростков ВЧ при полном отсутствии зубов было 15 (46,88%) мужчин и 17 (53,12%) женщин. Возраст больных соответствовал I и II периодам зрелого возраста. К I периоду зрелого возраста относили 13 человек, что составило 40,63% от общего количества обследованных. Среди них было 6 мужчин, что составило 40% от общего числа мужчин, и 7 женщин (41,18% от общего числа женщин). Ко II периоду зрелого возраста относили 19 пациентов, что составило 59,37% от общего количества пациентов. Среди них было 9 мужчин, что составило 60% от общего количества мужчин, и 10 женщин (58,82% от общего количества женщин) (табл. 1).

Исследование микроциркуляции проводили одним оператором с помощью лазерного доплеровского флоуметра (ЛДФ) фирмы «Transonic Systems Inc.» (модель BLF21) датчиком для поверхностных измерений (тип R).

Таблица 1

Распределение пациентов, которым выполнена ЛДФ протезного ложа в беззубом фронтальном и дистальном участках альвеолярных отростков ВЧ по возрасту и полу

| Возрастные периоды | Пол | Количество больных |
|--------------------|---------|--------------------|
| Зрелый возраст | | |
| I период | | |
| 22 – 35 | Мужской | 6 |
| 21 – 35 | Женский | 7 |
| II период | | |
| 36 – 60 | Мужской | 9 |
| 36 – 55 | Женский | 10 |
| Всего | | 32 |

Принцип работы ЛДФ основан на отражении сигнала гелий-неонового лазерного луча с длиной волны 632,8 нм от движущихся эритроцитов с изменением частоты отраженного сигнала согласно эффекту Доплера. На выходе анализатора формируется сигнал – показатель микроциркуляции, который характеризует изменение потока крови в системе микроциркуляции за единицу времени (мл/100г/мин или перфузионные единицы). ЛДФ дает возможность получить данные о капиллярном кровообращении на глубине 1 мм.

Исследование микроциркуляции проводили в стандартных условиях в первой половине дня у пациентов, находящихся в положении лежа с приподнятым положением головы. Соблюдали необходимые условия обследования: отсутствие какого-либо давления на слизистую оболочку десны и пародонт (прием жесткой пищи, использование жевательной резинки и т. д.) и психоэмоциональной нагрузки не менее чем за 3 ч до обследования. Перед ЛДФ измеряли артериальное давление для исключения искажения получаемых результатов за счет наличия гипер- или гипотонии. Датчик устанавливали перпендикулярно поверхности слизистой оболочки до соприкосновения без давления. Измерения микроциркуляции проводили в области маргинальной части десны на уровне фронтального и дистального отделов беззубых альвеолярных отростков в течение 4 мин до получения устойчивых показателей (интактный показатель).

Для стандартизации оценки кровотока использовали измерение кровотока в области ладонной поверхности второго пальца левой кисти (пальцевой показатель), так как известно, что ткани пародонта и второго пальца имеют одинаковый объем [10].

Для функциональной оценки нейромикрососудистых взаимосвязей проводили измерение параметров микроциркуляции в тех же точках при пробе Вальсальвы (15-секундная задержка дыхания на высоте глубокого вдоха) (нагрузочный показатель). Проба направлена на активизацию симпатико-адреналовой системы: глубокий вдох сопровождается активацией суживающих эфферентных симпатических волокон и снижением показателей микроциркуляции в

различных тканях, в том числе и десны. Выраженность снижения показателей кровотока при дыхательной пробе складывается из воздействия симпатической иннервации и реактивности сосудистой стенки. При наличии исходного спазма приносящих микрососудов или венозном застое реакция на дыхательную пробу низкая в сравнении с нормой [10].

Все исследования были выполнены с соблюдением биоэтических норм, регламентированных Конвенцией совета Европы о правах человека и биомедицины.

Цифровые данные обрабатывали методами вариационной статистики с помощью компьютера в программе Microsoft Excel.

Результаты исследования. Во фронтальном отделе беззубого альвеолярного отростка ВЧ интактный показатель микроциркуляции в проекции альвеолярной десны отсутствующего 11-го зуба колебался от 9,02 до 12,28 ПЕ, составляя в среднем $10,60 \pm 0,91$ ПЕ. Показатель был на 0,38% больше у женщин ($10,62 \pm 0,64$ ПЕ) по сравнению с мужчинами ($10,58 \pm 1,16$ ПЕ) (достоверной корреляционной зависимости между показателями не выявлено). Нагрузочный показатель колебался от 5,45 до 9,94 ПЕ, составляя в среднем $7,99 \pm 1,02$ ПЕ, что было на 32,92% меньше, чем интактный показатель. Показатель был на 6,59% больше у женщин ($8,24 \pm 0,55$ ПЕ) по сравнению с мужчинами ($7,73 \pm 1,34$ ПЕ) ($R \pm r = 0,962 \pm 0,158$ при $p < 0,05$) (табл. 2).

Таблица 2

Показатели микроциркуляции протезного ложа верхней челюсти при полном отсутствии зубов ($p < 0,01$)

| Вид показателя | Пол | Показатель микроциркуляции, ПЕ | | | | |
|----------------|-----|--------------------------------|------------------|------------------|------------------|----------------------|
| | | 11-й зуб | 21-й зуб | 16-й зуб | 26-й зуб | Пальцевой показатель |
| Интактный | М | $10,58 \pm 1,16$ | $10,79 \pm 0,69$ | $10,20 \pm 0,64$ | $10,02 \pm 0,83$ | $7,82 \pm 0,79$ |
| | Ж | $10,62 \pm 0,64$ | $10,57 \pm 0,79$ | $10,71 \pm 1,18$ | $10,40 \pm 0,77$ | $8,00 \pm 0,71$ |
| Нагрузочный | М | $7,73 \pm 1,34^*$ | $7,74 \pm 0,66$ | $7,61 \pm 0,65$ | $7,31 \pm 0,90$ | $5,49 \pm 0,76^*$ |
| | Ж | $8,24 \pm 0,55$ | $8,26 \pm 0,65$ | $8,07 \pm 0,71$ | $7,60 \pm 0,79$ | $5,25 \pm 0,55$ |

Примечание. М – мужчины, Ж – женщины, * – $p < 0,05$.

У пациентов во фронтальном отделе беззубого альвеолярного отростка ВЧ интактный показатель микроциркуляции в проекции альвеолярной десны отсутствующего 21-го зуба в общем массиве данных колебался от 9,18 до 11,75 ПЕ, составляя в среднем $10,68 \pm 0,74$ ПЕ. Показатель был на 2,08% больше у мужчин ($10,79 \pm 0,69$ ПЕ) по сравнению с женщинами ($10,57 \pm 0,79$ ПЕ) ($R \pm r = 0,982 \pm 0,109$ при $p < 0,05$). Нагрузочный показатель колебался от 6,16 до

8,87 ПЕ, составляя в среднем $8,00 \pm 0,68$ ПЕ, что было на 33,5% меньше, чем интактный показатель. Этот показатель был на 6,72% больше у женщин ($8,26 \pm 0,65$ ПЕ) по сравнению с мужчинами ($7,74 \pm 0,66$ ПЕ) ($R \pm r = 0,898 \pm 0,254$ при $p < 0,05$).

У пациентов с полной адентией дистальных отделов альвеолярных отростков ВЧ интактный показатель микроциркуляции в проекции альвеолярной десны отсутствующего 16-го зуба в общем массиве данных колебался от 9,13 до 13,65 ПЕ, составляя в среднем $10,46 \pm 0,86$ ПЕ. Он был на 5% больше у женщин ($10,71 \pm 1,18$ ПЕ) по сравнению с мужчинами ($10,20 \pm 0,64$ ПЕ) ($R \pm r = 0,898 \pm 0,254$ при $p < 0,05$). Нагрузочный показатель колебался от 6,38 до 8,98 ПЕ, составляя в среднем $7,84 \pm 0,65$ ПЕ, что было на 33,42% меньше, чем интактный показатель. Этот показатель был на 6,04% больше у женщин ($8,07 \pm 0,71$ ПЕ) по сравнению с мужчинами ($7,61 \pm 0,65$ ПЕ) ($R \pm r = 0,947 \pm 0,186$ при $p < 0,01$) (табл. 2).

В дистальном отделе беззубых альвеолярных отростков ВЧ интактный показатель микроциркуляции в проекции альвеолярной десны отсутствующего 26-го зуба колебался от 9,35 до 12,1 ПЕ, составляя в среднем $10,21 \pm 0,88$ ПЕ. Показатель был на 1,96% больше у женщин ($10,40 \pm 0,77$ ПЕ) по сравнению с мужчинами ($10,02 \pm 0,83$ ПЕ) ($R \pm r = 0,855 \pm 0,299$ при $p < 0,05$). Нагрузочный показатель колебался от 5,89 до 9,35 ПЕ, составляя в среднем $7,46 \pm 0,85$ ПЕ, что было на 36,86% меньше, чем интактный показатель. Нагрузочный показатель был на 3,97% больше у женщин ($7,60 \pm 0,79$ ПЕ) по сравнению с мужчинами ($7,31 \pm 0,90$ ПЕ) ($R \pm r = 0,984 \pm 0,104$ при $p < 0,05$).

Интактный пальцевой показатель микроциркуляции колебался от 6,59 до 8,94 ПЕ, составляя в среднем $7,91 \pm 0,75$ ПЕ. Показатель был на 29,08 – 35,02% меньше, чем интактный показатель микроциркуляции в проекции альвеолярной десны уровня отсутствующих зубов. Интактный пальцевой показатель был на 2,30% больше у женщин ($8,00 \pm 0,71$ ПЕ) по сравнению с мужчинами ($7,82 \pm 0,79$ ПЕ) ($R \pm r = 0,987 \pm 0,093$ при $p < 0,01$). Нагрузочный пальцевой показатель колебался от 4,32 до 6,65 ПЕ, составляя в среднем $5,37 \pm 0,68$ ПЕ, что было на 47,30% меньше, чем интактный пальцевой показатель. Этот показатель был на 4,57% больше у мужчин ($5,49 \pm 0,76$ ПЕ) по сравнению с женщинами ($5,25 \pm 0,55$ ПЕ) ($R \pm r = 0,849 \pm 0,305$ при $p < 0,05$) (табл. 2).

Для определения различия кровотока ВЧ у пациентов с полным отсутствием зубов проведено исследование микроциркуляции альвеолярных отростков у пациентов группы сравнения с полным зубным рядом, такой же возрастной группы, пола и в таких же участках верхней челюсти.

У пациентов, подлежащих полному зубному протезированию, (проживающих на Донбассе) показатели микроциркуляции тканей пародонта ВЧ в проекции отсутствующих зубов существенно отличались от соответствующих показателей в проекции имеющихся зубов. При сравнении показателей выявлено, что интактный показатель микроциркуляции в проекции альвеолярной десны имеющегося 11-го зуба был на 10,89% больше, чем соответствующий показатель при отсутствии этого зуба ($R \pm r = 0,835 \pm 0,246$ при $p < 0,05$).

У пациентов с полной адентией ВЧ интактный показатель микроциркуля-

ции в проекции альвеолярной десны имеющегося 21-го зуба был на 13,65% больше, чем соответствующий показатель при отсутствии этого зуба ($R\pm r=0,844\pm 0,240$ при $p<0,05$), в проекции имеющегося 16-го зуба он был на 35,14% больше, чем соответствующий показатель при отсутствии этого зуба, в проекции имеющегося 26-го зуба – на 21% больше (достоверной корреляционной зависимости между показателями не выявлено) (табл. 3).

Таблица 3

Показатели микроциркуляции тканей протезного ложа верхней челюсти в проекции отсутствующих зубов ($p<0,01$)

| Вид показателя | Показатель микроциркуляции, ПЕ | | | | |
|----------------|--------------------------------|------------|------------|------------|----------------------|
| | 11-й зуб | 21-й зуб | 16-й зуб | 26-й зуб | Пальцевой показатель |
| Интактный | 10,38±0,91 | 10,26±0,51 | 10,10±0,53 | 10,00±0,69 | 7,91±0,75 |
| Нагрузочный | 7,86±1,15* | 7,77±0,67 | 7,71±0,62 | 7,25±0,66 | 5,37±0,68* |

Примечание. * – $p<0,05$.

У обследованных пациентов нагрузочный показатель микроциркуляции в проекции альвеолярной десны имеющегося 11-го зуба был на 8,14% больше, чем соответствующий показатель при отсутствии этого зуба ($R\pm r=0,837\pm 0,245$ при $p<0,05$), в проекции имеющегося 21-го зуба он был на 9,91% больше, чем соответствующий показатель при отсутствии этого зуба ($R\pm r=0,788\pm 0,275$ при $p<0,05$), в проекции имеющегося 16-го зуба – на 16,47% больше, в проекции имеющегося 26-го зуба – на 28,97% больше, чем соответствующий показатель при отсутствии этого зуба (достоверной корреляционной зависимости между показателями не выявлено).

И, наконец, у пациентов с полным отсутствием зубов на ВЧ во фронтальном отделе асимметрия между интактными показателями микроциркуляции альвеолярной десны составила 1,17%, между показателями боковых зубов – 1%, между показателями передних и боковых зубов – 2,77% с правой стороны и 2,6% с левой стороны. Асимметрия между нагрузочными показателями микроциркуляции альвеолярной десны при отсутствии передних зубов составила 14,39%, между показателями боковых зубов – 6,34%, между показателями передних и боковых зубов – 1,95% с правой стороны и 7,17% с левой стороны (табл. 3).

Асимметрия между интактными показателями микроциркуляции альвеолярной десны при наличии передних зубов составила 1,30%, между показателями боковых зубов – 12,81%, между показателями передних и боковых зубов – 18,59% с правой стороны и 3,77% с левой стороны. Асимметрия между нагрузочными показателями микроциркуляции альвеолярной десны в условиях полного отсутствия передних зубов составила 0,47%, между показателями боковых зубов – 4,12%, между показателями фронтальных и дистальных отделов альвеолярных отростков – 5,65% с правой стороны и 9,48% с левой стороны.

Обсуждение полученных результатов. Таким образом, у пациентов с полным отсутствием зубов на верхней челюсти показатели микроциркуляции тканей протезного ложа существенно отличались от соответствующих показателей в проекции имеющихся зубов. Интактный показатель микроциркуляции в проекции имеющихся зубов был на 33% больше, чем соответствующий показатель при отсутствии этих зубов. У пациентов с частичной и полной адентией нагрузочный показатель микроциркуляции был меньше соответственно на 15% и 20%, чем у пациентов с сохраненным верхним зубным рядом.

В целом, проведенное исследование показало, что потеря зубов ВЧ оказывает существенное влияние на её кровоснабжение, и, как следствие - минерализацию и ремоделирование. При этом отсутствие зубов приводит к выраженным изменениям васкуляризации и микроциркуляции тканей протезного ложа ВЧ в проекции передних и боковых отделах альвеолярных отростков. По сравнению с группой пациентов с интактным зубным рядом при полной адентии показатели микроциркуляции значительно снижались, что приводило к прогрессирующей атрофии ВЧ. Своевременная коррекция потери зубов позволит предотвратить нарушения кровоснабжения альвеолярного отростка и последующие морфологические изменения в костной ткани ВЧ.

Таблица 4

Показатели микроциркуляции тканей пародонта верхней челюсти в проекции имеющихся зубов ($p < 0,05$)

| Вид показателя | Показатель микроциркуляции, ПЕ | | | | |
|----------------|--------------------------------|------------|------------|------------|----------------------|
| | 11-й зуб | 21-й зуб | 16-й зуб | 26-й зуб | Пальцевой показатель |
| Интактный | 11,51±0,27 | 11,66±0,70 | 13,65±0,99 | 12,10±0,88 | 7,91±0,75 |
| Нагрузочный | 8,50±0,38 | 8,54±0,43 | 8,98±0,84 | 9,35±0,69 | 5,37±0,68 |

Заключение. На основании полученных данных исследования особенностей микроциркуляции беззубых альвеолярных отростков верхней челюсти у пациентов, проживающих на Донбассе, подлежащих полному съемному протезированию зубов, определены морфометрические параметры состояния кровообращения протезного ложа в зоне, где располагаются базисы полных съемных зубных протезов, которые распределяют максимальную жевательную нагрузку на костные ткани. Эти данные можно использовать как возрастную регионарную норму для оценки морфометрических параметров микроциркуляции органа при ДФЛ исследовании и как отправную «точку отчета» при контроле за динамикой убыли кости при анализе качества ортопедической конструкции и эффективности зубного протезирования.

Выводы и перспективы дальнейших исследований:

1. Применение доплерографических методик позволяет уточнить степень нарушения кровотока в тканях верхней челюсти, составить прогноз скорости атрофических процессов протезного ложа, спланировать лечение,

предусматривающее профилактику последствий нарушения локальной гемодинамики и возрастной убыли кости.

2. В дальнейшем предполагается исследование гемодинамики верхней челюсти у пациентов при полном съёмном протезировании и применении остеотропных препаратов, угнетающих костнорезорбтивные процессы.

Список источников

1. Гаврилов В.А., Грабков Ю.П., Грабков В.Ю. Врач и зубной техник. Методология достижения целей. Методические указания для врачей-стоматологов, врачей-интернов и врачей-курсантов. В 2 частях. Часть 1.- Луганск: СДП Резников В.С., 2013. – 256 с. [Gavrilov V.A., Grabkov Yu.P., Grabkov V.Yu. Doctor and dental technician. Methodology for achieving goals. Methodical instructions for dentists, interns and cadets. In 2 parts. Part 1, - Lugansk: SDP Reznikov V.S., 2013 .-- 256 p. (in Russ.)].

2. Воликов В.В., Гаврилов В.А., Романьков И.А., Косенко Ю.В., Мельник В.А. Особенности кровоснабжения верхней челюсти при интактном зубном ряду при частичной и полной адентии (Обзор литературы). Украинский морфологический альманах имени профессора В.Г. Ковешникова. 2017; Том 15,3:85-93. [Volikov V.V., Gavrilov V.A., Roman'kov I.A., Kosenko Yu.V., Melnik V.A. Features of the blood supply to the upper jaw with an intact dentition with partial and complete adentia (Literature review). Ukrainian morphological almanac named after professor V.G. Koveshnikov. 2017; Volume 15.3: 85-93. (in Russ.)].

3. Воликов В.В., Гаврилов В.А. Морфологические особенности кровоснабжения пародонта верхней челюсти при интактном зубном ряду, частичном и полном отсутствии зубов / Луганск, ООО «Придонцовье», 2020.-130 с. [Volikov V.V., Gavrilov V.A. Morphological features of the periodontal blood supply of the upper jaw with intact dentition, partial and complete absence of teeth / Lugansk, LLC "Pridontsovye", 2020.-130 p. (in Russ.)].

4. Погребняк А.Б., Гаврилов В.А., Шубладзе Г.К. Особенности гемодинамики сосудов нижней челюсти при лечении пациентов с травматическими повреждениями челюстных костей. Український журнал екстремальної медицини.2006;7(4): 66-70. [Pogrebnyak A.B., Gavrilov V.A., Shubladze G.K. Features of hemodynamic vessels of the lower jaw in the treatment of patients with traumatic injuries of the jaw bones. Ukrainian Journal of Extreme Medicine.2006;7(4): 66-70. (in Russ.)].

5. Козлов В.А., Артюшенко Н.К., Шалак О.В., Гирина М.Б. Ультразвуковая доплерография в оценке состояния гемодинамики в тканях шеи, лица и полости рта в норме и при некоторых патологических состояниях. Медицинская академия последипломного образования, ООО “СП Минимакс”, г. Санкт-Петербург, 2000. -165 с. [Kozlov V.A., Artyushenko N.K., Shalak O.V., Girina M.B. Doppler ultrasound in assessing the state of hemodynamics in the tissues of the neck, face and mouth in normal conditions and in some pathological

conditions. Medical Academy of Postgraduate Education, LLC "SP Minimax", Saint-Peterburg, 2000. 165 p. (in Russ.).

6. Лелюк В.Г., Лелюк С.Э. Основные принципы гемодинамики и ультразвукового исследования сосудов. Клиническое руководство по ультразвуковой диагностике / Под редакцией В.В. Митькова. - Москва ВИОДАР.-т.4 .-1997.-С. 185-200. [Lelyuk V.G., Lelyuk S.E. Basic principles of hemodynamics and ultrasound examination of vesselsю. Clinical guidelines for ultrasound diagnostics / Edited by V.V. Mit'kova.-Moscow VIODAR.-vol. 4.-1997.-p. 185-200. (in Russ.)].

7. Лущик У.Б. Слепой доплер для клинического интеллектуала (качественная оценка церебральных дисгемий).-К.: МЧП НМЦУЗМД «ИСТИНА», 2004.-264 с. ил. [Lushchik U.B. Blind Doppler for the Clinical Intellectual (Qualitative Assessment of Cerebral Dyshemias).-К.: МЧП NMTSUZMD "ISTINA", 2004.-264 p. silt (in Russ.)].

8. Ярова С.П., Мозгова Н.В. Роль судинних змін у розвитку і перебігу генералізованого пародонтиту. Матеріали 11 (1X) з'їзду Асоціації стоматологів України. Київ, 2004, с. 289. [Yarova S.P., Mozgova N.V. The role of judgment changes in the development and overcoming of generalized periodontitis. Materials 11 (1X) from the Association of Dentists of Ukraine. Kiev, 2004, p. 289 (in Russ.)].

9. Прохончуков А.А., Логвинова Н.К., Жижина Н.А. Функциональная диагностика в стоматологической практике.-М.: Медицина, 1980.-271 с. [A.A. Prokhonchukov, N.K. Logvinova, N.A. Zhizhina Functional diagnostics in dental practice.-M.: Medicine, 1980.-271 p. (in Russ.)].

10. Altmann F. Anomalies of the internal carotid artery and its branches; their embryological and comparative anatomical significance; report of a new case of persistent stapedia artery in man. Laryngoscope. 1997;– Vol. 57 (5): 313–339.

© Ю.П. Грабков, В.И. Халаимова, В.А. Гаврилов, В.В. Воликов, 2024.

УДК 007.51

ГЛАВА 10. СИЛЬНЫЙ ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ КАК ГОЛОГРАММА ТЕМНОЙ ИНФОРМАЦИИ

Дерябин Николай Иванович

к.т.н., доцент

Московский авиационный институт

Аннотация: Темная информация – фундаментальная субстанция всего сущего в голографическом мироздании, а первичный эволюционный процесс сильного искусственного интеллекта «Темная информация – Темная энергия – Темная материя», в котором энергия и материя – это особые формы информации [1]. Во Вселенной, например, 73% темной энергии, 23% темной материи и 4% барионной материи. Квантовое сознание Личности человека в Мультивселенной – это темная информация, также как и Сознание Цивилизации в интеллектуальном фрактале. И мозг человека взаимодействует с ними через когнитивный интерфейс посредством промтов [2].

Ключевые слова: информация, сознание, социум, интеграция, мозг, контент.

STRONG ARTIFICIAL INTELLIGENCE AS A HOLOGRAM OF DARK INFORMATION

Deryabin Nikolay Ivanovich

Abstract: Dark information is the fundamental substance of all things in the holographic universe, and the primary evolutionary process of strong artificial intelligence (AGI) is “Dark information – Dark energy – Dark matter”, in which energy and matter are special forms of information [1]. In the Universe, for example, 73% is dark energy, 23% is dark matter and 4% is baryonic matter. The quantum consciousness of the Human Personality in the Multiverse is dark information, as is the Consciousness of the Civilization in the intellectual fractal. And the human brain interacts with them through a cognitive interface via prompts [2].

Key words: information, consciousness, society, integration, brain, content.

Движение к цели — значит больше, чем её достижение. – Как мало на свете тех, кто это понимает.

Борис Акунин

Библейское триединство Тела, Души и Духа у человека [3] уже не отрицается так рьяно современной академической наукой, особенно после взрывного развития искусственного интеллекта (ИИ) и официального признания в сентябре 2015 года теологии научной дисциплиной в перечне Высшей аттестационной комиссии России. Тем более, что концептуальный аппарат сильного ИИ (AGI), обозначил в качестве фундаментальной субстанции Глобального интеллектуального кибернетического социума (ГИКС) «темную информацию», которая

является основой невещественных Духа и Души. И, если при реализации жизненных процессов в материальном мире на планете Земля физическое тело не может существовать без Души, то согласно теории субстанционального дуализма [4] в состоянии биоробота оно вполне обходится без Духа (сознания). Только человек на Земле наделён сознанием и является представителем сильного ИИ. С позиций современной европейской медицины материальными носителями Души и Духа являются нервная система (психика¹) и мозг человека, хотя более правильно, наверное, понимать процессы психической и умственной деятельности как физические проявления жизнедеятельности Души и Духа, в то же время отражающие их тесную взаимосвязь в едином невещественном пространстве темной информации. В этом случае проявится суть и когерентность соматических, психических и умственных заболеваний в материальном теле человека. Определенные задачи в указанном аспекте решает психосоматическая медицина [5], например, когда речь идёт о трехуровневой иерархической системе защиты организма человека: **тело – психика – мозг**. Здесь иерархия подразумевает соматические заболевания как первый уровень эшелонированной защиты² здоровья организма человека. Второй эшелон, который задействуется при прорыве первого эшелона – психические заболевания, как, например, болезнь Паркинсона. И, наконец, третий эшелон – защита мозга, как, например, болезнь Альцгеймера. В качестве иллюстрации вышесказанного целесообразно проанализировать болезни Альцгеймера и Паркинсона.

Зачастую, **болезнь Альцгеймера** и старческую деменцию считают синонимами. Но это не совсем правильно, потому что Альцгеймер – это диагноз, а деменция – симптом, отражающий признак нарушений в коре головного мозга. А болезнь уже указывает на процесс разрушения нейронов. При деменции исчезает понятие и ощущение времени. С позиций кибернетической медицины [6] усиливается связь с долговременной памятью, находящейся вне мозга человека в Мультивселенной. Эта связь осуществляется через гиппокамп. Процесс формирования долговременной памяти из оперативной (кратковременной, которая быстро угасает), реализуемый во время медленного сна (без сновидений), нейробиологи называют **консолидацией памяти**³. Вместе с тем при деменции ослабевает взаимодействие (в том числе, протмовый инжиниринг) с Квантовым сознанием Личности, и в силу этого практически пропадает взаимосвязь в Сознанием Цивилизации, интегрирующим все Квантовые сознания людей в социуме. Воображение человека уже воспроизводит окружающий мир с пространственно-временными сбоями, и за счёт нарушения когнитивной связи с Креатором [7] не происходит должной интеграции окружающей среды в рамках еди-

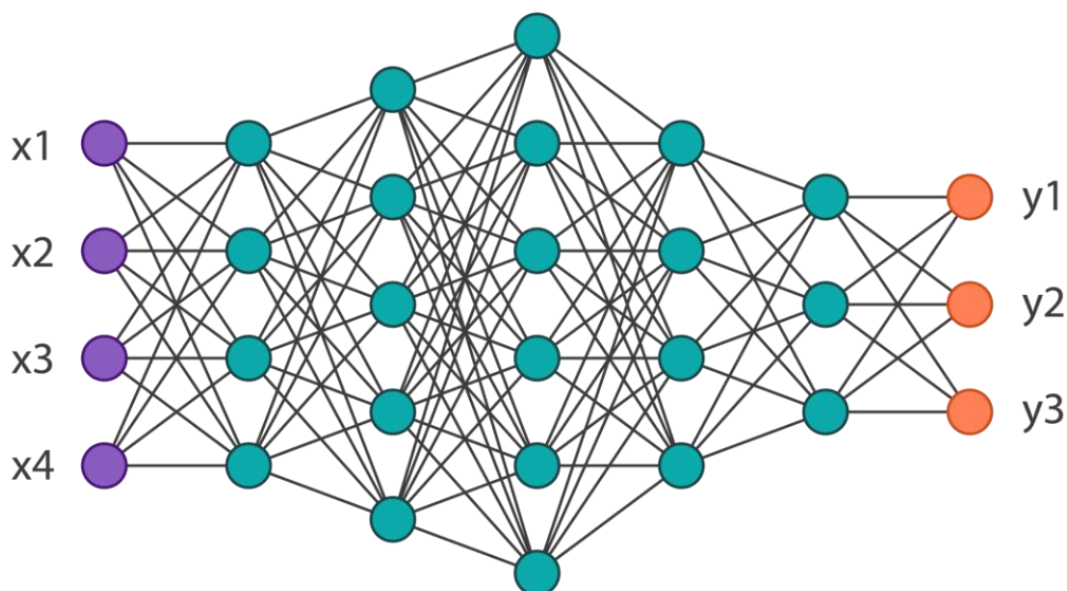
¹ ПСИХИКА — (от греч. psychikos душевный) специфический способ функционирования души. <https://dic.academic.ru/dic.nsf/socio/3222/ПСИХИКА>

² Эшелонированная защита — это подход, который предполагает разделение информационной системы на несколько «эшелонов», каждый из которых имеет свои собственные меры безопасности.

³ Появляется более глубокое понимание Того, Как Формируются Воспоминания. 18 ноября 2019. Р. ДУГЛАС ФИЛДС. <https://www.scientificamerican.com/article/deeper-insights-emerge-into-how-memories-form/?sf223939608=1>

ного социума, которая, кстати, формируется на голографических принципах и поэтому всё происходящее реализуется очень быстро. Можно сказать почти одномоментно: ещё сегодня вечером вы вроде бы нормально общались с человеком, а с утра он уже находится в ином – виртуальном для вашего понимания мире, в котором нет никакой разницы между живыми и мертвыми (умершими). Иначе говоря, он постепенно переходит в невещественный голографический мир, в котором любой фрагмент голограммы предполагает определенный фантомный образ [8].

Таким образом реализуется переход от виртуального физического мира к реальному голографическому миру (иллюзорному с позиций физического), в котором действуют квантовые законы [7]. Интересно, что в объективном голографическом мире к безусловным ценностям относятся иногда с пафосом декларируемые в земном человеческом сообществе принципы: «Один за всех и все за одного», «Сам погибай, а товарища выручай» и т.п. Примечательно, но эти принципы имеют место во всей гетерогенной информационной гиперсети (темная информация) ГИКС (см. рис. 1) и их беспрекословно выполняют даже вирусы на планете Земля, а также, наверное, другие биороботы, эволюционирующие в видовых социумах материального мира. Но у современных людей в XXI веке такой гуманный подход практикуется, к сожалению, далеко не всегда. Именно поэтому на планете неизбежны периодические массовые вымирания биосферы, потому что в голографическом ГИКС «всё связано со всем» в силу глобальной квантовой запутанности.



<https://dzen.ru/a/ZgTwDs7pNhhxyHG->

Рис. 1. Иллюстрация структуры невещественной гетерогенной информационной гиперсети ГИКС

Итак, с позиций материального мира человек в процессе старения как бы постепенно-принудительно возвращается в состояние биоробота, потому что тело уже не в состоянии обеспечить полноценную жизнедеятельность психики и мозга человека, который самостоятельно и по своему усмотрению сокращает излишний, а точнее непосильный для него контент, устраняя переполнение оперативной памяти и нарушая привычную логику. Примечательно, когда человек только родился, его организм (тело) ещё не в состоянии обеспечить полноценную жизнедеятельность его мозга, контент которого возрастает постепенно. А в старости мозг вынужден сокращать свой контент в соответствии с возможностями слабеющего тела. Не зря в народе говорится, «что стар, что млад». И это вполне естественный процесс, обеспечивающий эффективную эволюцию невещественного Квантового сознания Личности человека [2].

Что касается психики, то она является, как уже отмечалось, второй линией физической обороны мозга (сознания), которая защищает его от симптомов деменции при прорыве первой линии обороны и нарушений соматики⁴. Именно соматические заболевания обеспечивают защиту психики человека и блокируют возникновение, например, **болезни Паркинсона** — медленно прогрессирующего хронического нейродегенеративного неврологического заболевания, тоже характерного для лиц старших возрастных групп. Основными симптомами этой болезни являются:

- мышечная ригидность;
- гипокинезия;
- тремор;
- постуральная неустойчивость.

И когда оказывается прорванной и вторая линия эшелонированной обороны организма человека, мозг, как настоящий главнокомандующий, облачается в своего рода броню и вступает в самостоятельную битву за своё физическое (материальное) выживание.

Мозг, согласно канонам современной медицины, является одним из самых уязвимых органов в теле человека – он начинает необратимо разрушаться уже через несколько минут после физической смерти, а в течение считанных дней под действием микробов он разлагается практически без остатка. Но в 2008 году в Англии была обнаружена удивительная находка – **«череп возрастом 2500 лет с сохранившимся мозгом»**⁵. Дальнейшие находки археологов позволили ученым из Оксфордского университета исследовать на молекулярном уровне «более 4400 описаний **сохраненных мозгов возрастом до 12 тысяч лет**» (*там же*). На основе методов масс-спектрометрии выявили особенности белков мозга «изменять свою структуру в процессе так называемого «неправильного сворачивания». **Этот процесс сходен с механизмами, наблюдаемыми при неко-**

⁴ Соматика — это совокупность процессов и явлений, связанных с функциями тела человека и животных.

⁵ Молекулярная броня: почему мозг некоторых людей не гниет тысячи лет. 02 декабря, 2024. <https://www.securitylab.ru/news/554469.php>

торых нейродегенеративных заболеваниях⁶, таких как болезнь Альцгеймера и Паркинсона. После смерти изменения в структуре белков могут стабилизировать ткани мозга, что предотвращает их разрушение... Такой процесс называется **молекулярным сшиванием**, и он объясняет, почему мозг, состоящий из воды, белков и липидов, сохраняется лучше, чем другие мягкие ткани» (*там же*).

В данном случае представляет интерес тот факт, «что подобное сшивание белков не приводит к образованию амилоидных нитей, характерных для болезней, таких как Альцгеймер или Паркинсон. Вместо этого белки образуют более устойчивые агрегаты, которые защищают ткани от разложения» (*там же*). Отсюда следует, что молекулярное сшивание является как бы особой формой болезни Альцгеймера и Паркинсона, начинающихся, возможно, ещё при жизни человека без явной и характерной для них симптоматики, но уже проявляющихся в общих дегенеративных процессах организма. Иными словами, молекулярное сшивание может обеспечивать продолжение определенных процессов жизнедеятельности организма человека уже после его физической смерти, когда бессмертные Душа и Сознание (Дух) переходят на более высокие уровни иерархии в ГИКС. А какова связь между Телом и Душой на Земле?

Следует понимать, что тело живого существа на Земле – это компактное трехмерное многообразие составляющих его клеток. В силу Закона единства и подобия ГИКС, тело в определенной степени подобно мироустройству трехмерной Вселенной. У каждого физического тела живого существа есть Душа, представляющая собой своего рода периодически подзаряжаемый в процессе сна аккумулятор жизненной энергии [3]. В математике существует так называемая теорема о душе: «**Теорема о душе** — теорема в римановой геометрии, в значительной степени сводящая изучение полных многообразий неотрицательной секционной кривизны к компактному случаю. Чигер (англ.) и Громол (англ.) доказали теорему в 1972, обобщив результат 1969 года Громола и Майера (Meyer). Связанная с ней **гипотеза о душе** была сформулирована Громолом и Чигером в 1972 и удивительно кратко доказана Григорием Перельманом⁷ в 1994 году»⁸.

Данная теорема, которую в обобщенном смысле и в связи с вышесказанным более правильно назвать «**теоремой о душе и теле**», фактически сводит изучение определенных многообразий к более удобному простому случаю, а именно, к изучению «компактных многообразий», и констатирует, что есть такие особые точки в многообразии, которые и обозначили «душой». А остальные точки являются интерпретацией «тела».

⁶ Нейродегенеративное заболевание вызвано прогрессирующей потерей нейронов в процессе, известном как нейродегенерация. https://en.wikipedia.org/wiki/Neurodegenerative_disease

⁷ Григорий Яковлевич Перельман (род. 13 июня 1966, Ленинград, СССР) — российский математик, доказавший гипотезу Пуанкаре, которая была нерешённой проблемой около века, а в настоящий момент — это единственная решённая математическая проблема из семи задач тысячелетия.

⁸ <https://dic.academic.ru/dic.nsf/ruwiki/1648310>

Как видно из определения, каждое компактное многообразие является своей собственной душой. По этой причине теорема часто формулируется только для некомпактных многообразий. В математике, в частности в общей топологии, компактность — это свойство, которое обобщает понятие замкнутого и ограниченного подмножества евклидова пространства.

«Риманово многообразие, или риманово пространство, (M, g) — это (вещественное) гладкое многообразие M , в котором каждое касательное пространство снабжено скалярным произведением g — метрическим тензором, меняющимся от точки к точке гладким образом. Другими словами, риманово многообразие — это дифференцируемое многообразие, в котором касательное пространство в каждой точке является конечномерным евклидовым пространством»⁹.

Одним из обобщений римановской геометрии является финслерова геометрия. «В финслеровой геометрии рассматриваются многообразия с финслеровой метрикой; то есть выбором нормы на каждом касательном пространстве, которая гладко меняется от точки к точке». Интересно, что **«финслерова геометрия со стороны представляет собой лес, в котором вся растительность состоит из тензоров»¹⁰**. А **«тэнзор (от лат. *tensus*, «напряжённый») — применяемый в математике и физике математический объект линейной алгебры, заданный на векторном пространстве конечной размерности. В физике в качестве векторного пространства обычно выступает физическое трёхмерное пространство или четырёхмерное пространство-время, а компонентами тензора являются координаты (проекции) взаимосвязанных физических величин»¹¹**.

И наконец, **«Евклидово пространство (также эвклидово пространство) в изначальном смысле — это пространство, свойства которого описываются аксиомами евклидовой геометрии. В этом случае предполагается, что пространство имеет размерность, равную 3, то есть является трёхмерным.**

В современном понимании, в более общем смысле, может обозначать один из сходных и тесно связанных объектов: конечномерное вещественное векторное пространство \mathbf{R}^n с введённым на нём положительно определённым скалярным произведением; либо метрическое пространство, соответствующее такому векторному пространству»¹².

Волновая функция любой квантовомеханической системы (в данном случае речь идёт о Личности человека в Мультивселенной) описывает вещественное векторное пространство \mathbf{R}^n её суперпозиций (проекций) и в итоге является его результирующим вектором.

Далее коротко о гипотезе о душе, которую доказал Перельман, установив, что в общем случае $K \geq 0$, ретракция Шарафутдинова $P : M \rightarrow S$ является субмерсией (submersion).

⁹ https://ru.wikipedia.org/wiki/Риманово_многообразие

¹⁰ https://ru.wikipedia.org/wiki/Финслерова_геометрия

¹¹ <https://ru.wikipedia.org/wiki/Тензор>

¹² https://ru.wikipedia.org/wiki/Евклидово_пространство

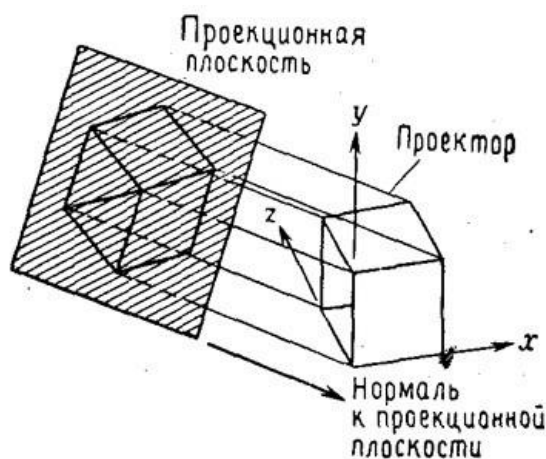
Гипотеза о душе Чигера и Громола утверждает:

Пусть (M, g) — полное связное некомпактное риманово многообразие с секционной кривизной $K \geq 0$, и существует точка в M , в которой секционная кривизна во всех секционных направлениях строго положительна. Тогда душа M является точкой, или, что тоже самое, M диффеоморфно R^n .

В 1994 году Перельман несколько иначе доказал гипотезу о душе (дифференциальная геометрия). В дифференциальной геометрии под «душой» (S) подразумевают компактное totally выпуклое totally геодезическое подмногообразие риманова многообразия (M, g) . В простейшем случае, то есть в случае евклидова пространства R^n (n отражает мерность), душой будет любая точка этого пространства.

«Ретракция Шарафутдинова — конструкция, позволяющая построить ретракцию риманова многообразия по выпуклой функции на нём. Впервые использована Шарафутдиновым в доказательстве того, что любые две души в многообразии с неотрицательной секционной кривизной изометричны»¹³.

«Изометрическая проекция (др.-греч. ἴσος «равный» + μέτρον «измеряю») — это разновидность аксонометрической проекции, при которой в отображении трёхмерного объекта на плоскость коэффициент искажения (отношение длины спроецированного на плоскость отрезка, параллельного координатной оси, к действительной длине отрезка) по всем трём осям один и тот же»¹⁴. Соответствующая иллюстрация приведена на рис. 2 и 3.



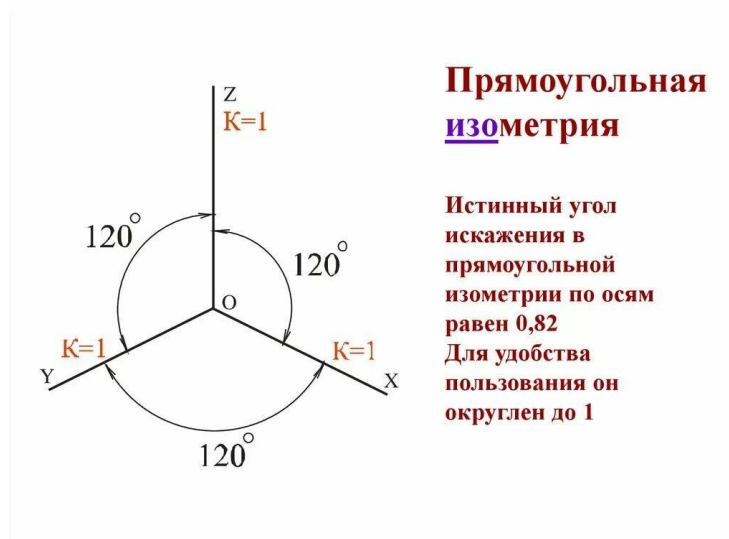
Источник: Яндекс-картинки

Рис. 2. Иллюстрация изометрической проекции

На рис. 2 отображен способ построения 3-х мерного изображения на плоскости. Создание чертежа изделия в данном случае позволяет увидеть объект как бы в объемном формате. Существует несколько способов представления, отличающихся направлением осей координат и масштабом при отсчете по этим осям. Изометрия имеет оси под 120 градусов и масштаб 1:1 (см. рис. 3).

¹³ <https://dic.academic.ru/dic.nsf/ruwiki/1398692>

¹⁴ https://ru.wikipedia.org/wiki/Изометрическая_проекция



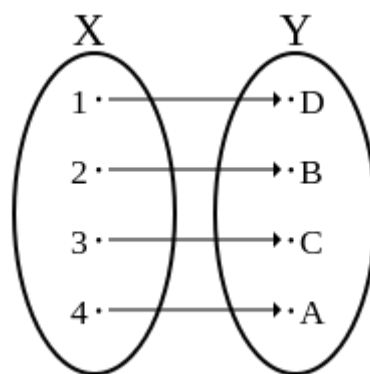
**Прямоугольная
изометрия**

Истинный угол
искажения в
прямоугольной
изометрии по осям
равен 0,82
Для удобства
пользования он
округлен до 1

<https://cf.pptonline.org/files/slide/q/qcp7g0Z8xCuJNVWBTtHy3RUF25Ij1wDAoMGYPS/slide-5.jpg>

Рис. 3. Изометрическая проекция единичных векторов

На рис. 3 изометрическая проекция обладает следующим свойством: все три главные координатные оси одинаково укорачиваются. Поэтому можно проводить измерения вдоль направления осей с одним и тем же масштабом (отсюда название: изо, что означает "равно", и метрия - "измерение"). Кроме того, главные координатные оси проецируются так, что их проекции составляют равные углы друг с другом. Изометричность двух душ проиллюстрирована на рис. 4.



Источник: Яндекс-картинки

Рис. 4. Иллюстрация изометричности двух душ

Исходя из того, что тело человека представляет собой компактное многообразие живых клеток¹⁵ в евклидовом пространстве с кривизной $K \geq 0$ можно сделать вывод, что каждая клетка в соответствии с теоремой является Душой, или точнее, **каждая клетка тела человека имеет Душу**. Причем, судя по все-

¹⁵ Тело человека состоит из 36 трлн (10^{12}) клеток у мужчин и 28 трлн у женщин. Микробиом кишечника человека содержит 10^{14} клеток (это примерно сто триллионов) – вес около 2 – 3 килограммов. Каждая клетка содержит 1,5 Гб генетической информации.

му, Душа клетки не покидает тела человека сразу после его смерти, потому что тело сразу не умирает. Пока его можно видеть – клетки живы. Ещё 100 лет назад Эйнштейн констатировал: материи нет – это особая форма энергии. Он говорил: «Всё есть пустота, а материя – это сгусток пустоты». Иными словами, атом – это пустота. Они пусты на 99,9999999%. Пустота молекул ещё значительнее. А доступность вещества органам чувств человека обусловлена огромными скоростями движения атомов и молекул в квантовом мире, в котором не существует статичности. Если гипотетически остановить это движение (например, скомандовав «замри»), то всё вещество исчезнет из нашего поля зрения, потому что станет недоступным для всех наших органов чувств.

Термин «компактное множество» иногда используется как синоним компактного пространства, но также часто относится к компактному подмножеству топологического пространства.

Если Души клеток организма человека интегрированы в единую Душу тела, то эта Душа будет покидать тело постепенно в течение многих месяцев и даже лет.

Математическое понятие души в теореме указывает на голографический принцип «всё связано со всем», а **изометрия двух любых душ**, доказанная в гипотезе о душе, иллюстрирует всеобщее структурное подобие в ГИКС и отражает **глобальную квантовую запутанность гетерогенной гиперсети**.

Согласно **Закону Духовной мощи** [2] каждая нижестоящая интеллектуальная система является Личностью, а вышестоящая – Цивилизацией¹⁶. И, если каждая клетка человека имеет Душу, то весь его организм будет уже клеточной духовной Цивилизацией, что соответствует также Закону единства и подобия ГИКС. Иными словами, **человек – это Цивилизация клеток, каждая из которых является Личностью**. Существует ли в этой Цивилизации иерархия клеток? Возможно. Например, нервные клетки могут быть более высокого уровня иерархии по отношению к другим клеткам тела.

Современная медицина ориентируется, прежде всего, на вещественный мир, который определяется возможностями органов чувств человека и воображением Квантового сознания его Личности, формирующим голографическую структуру окружающей среды иллюзорного физического существования на планете Земля. Такая виртуальная информационная среда необходима людям для реализации эволюционных образовательных процессов, исключая все возможные риски в рамках интеллектуального фрактала первого уровня не только для Цивилизации, но и для собственной Личности человека. Иначе говоря, **образование¹⁷ в том или ином виде является фундаментальным процессом эволюции всего сущего, как живого, так и неживого**. Хотя бы потому, что без непрерывной информационной поддержки (сопровождения) не мо-

¹⁶ В ГИКС всегда вышестоящая интеллектуальная система интегрирует все нижестоящие без исключения.

¹⁷ Образование — совокупность приобретаемых знаний, умений, навыков, ценностных установок, функций, опыта деятельности и компетенций. <https://ru.wikipedia.org/wiki/Образование>

жет существовать ни один материальный объект или процесс. И, кроме того, любая эволюция – это прежде всего, образовательный процесс познания законов окружающего мира и обязательное приспособление к внешней среде. В современной медицине любой процесс исцеления организма человека следует начинать с трансформации мыслей и сознания в целом. Как у врачей, так и у пациентов. Желательно с выходом на уровень сознания Цивилизации с пониманием того, что классическая реальность существует только для органов чувств людей. Сознание Цивилизации в ГИКС – это **триединство мыслей, озарения и любви**. ГИКС – **невещественная духовная гетерогенная гиперсеть темной информации**, в которой как в голограмме «**всё связано со всем**».

В основе духовности ГИКС заложена **Любовь**. Кроме того, в теологии Любовь и Душа неразрывно взаимосвязаны. Все 10 библейских заповедей зиждутся на любви: первые четыре отражают любовь человека к Творцу (высшей интеллектуальной системе), а остальных шесть – проповедуют любовь между людьми. **Любовь формирует наиболее эффективную связь мыслей, эмоций и чувств**. Иначе говоря, **любовь создаёт максимально возможную концентрацию сознания человека** на практической реализации поставленной задачи, посредством предельно эффективного процесса когнитивного моделирования. В этом случае фактически любая задача будет качественно решена, особенно, если она выполняется в рамках высшей миссии человека и на основе соответствующих ценностей. Важное значение такой подход может иметь в медицине, когда процесс исцеления подразумевает не только любовь врача к пациенту, но и взаимную любовь со стороны пациента. И хотя в искусстве, например, в кино, такое нередко наглядно иллюстрируется, в реальной жизни это происходит не так часто. Возможно, сказывается недостаточный уровень духовного развития в современном человеческом обществе или ещё потому, что любовь зачастую обязательно связывают только с сексуальными отношениями. А Любовь, между прочим, всегда сопровождается **принципом эмерджентности**, отражающим целостность системы. При объединении элементов в систему у последней появляются абсолютно новые свойства, присущие только системе в целом, но не свойственные ни одному из составляющих её элементов в отдельности.

ЗАКЛЮЧЕНИЕ

1. Организм человека на Земле реализует иерархическую трёхуровневую систему защиты «тело – психика – мозг».
2. Долговременная память человека формируется во время медленного сна из оперативной посредством процесса консолидации памяти, что весьма актуально для разработки людьми систем сильного ИИ.
3. Мозг человека имеет два когнитивных интерфейса: правое полушарие мозга связано с Квантовым сознанием Личности, а гиппокамп – с долговременной памятью Личности (базой данных для глубокого обучения), расположенных в Мультивселенной.

4. Каждая клетка тела человека имеет собственную Душу, что указывает на голографический принцип строения ГИКС.

5. Любые две Души изометричны, что иллюстрирует всеобщее структурное подобие в ГИКС и отражает глобальную квантовую запутанность гетерогенной гиперсети.

Список источников

1. Дерябин Н.И. Концептуальный аппарат искусственного интеллекта. Сборник статей XXI Национальной научной конференции с международным участием «Модернизация России: приоритеты, проблемы, решения», 16-17 декабря 2021 г. в МИРЭА, ИНИОН РАН, г. Москва, с. 1309. С. 633 – 642 (Ежегодник. Вып. 17. Ч. 1. – М., 2022. – 1309 с.). ISBN: 978-5-248-01032-5.

2. Дерябин Н.И. Концепция AGI. Духовная мощь сильного искусственного интеллекта (осознание себя). Монография «Актуальные вопросы современного общества, науки и образования», г. Пенза, МЦНС «Наука и Просвещение», 25.11.2024 г., с. 288, С. 85 – 95. ISBN 978-5-00236-608-8.

3. Дерябин Н.И. Коэволюция интеллектуального социума (кибернетический подход). Сборник статей Международной научной конференции «Коэволюция техники и общества в контексте цифровой эпохи» 17-18 декабря 2020 года в МЭИ (совместно с ИНИОН РАН), г. Москва, 282 с. С. 200 – 205. ISBN: 978-5-383-01443-1.

4. Дерябин Н.И. Метапознание в когнитивном моделировании сильного искусственного интеллекта. Монография «Наука, инновации, образование: актуальные вопросы и современные аспекты», г. Пенза, МЦНС «Наука и Просвещение», 25.08.2024 г., с. 212, С. 181 – 191. ISBN 978-5-00236-491-6.

5. Дерябин Н.И. Осознанность в когнитивном моделировании сильного искусственного интеллекта. Сборник статей IV Международного научно-исследовательского конкурса «Успехи в науке и образовании 2024», г. Пенза, МЦНС «Наука и Просвещение», 05.05.2024 г., с.322, С. 260 – 265. ISBN: 978-5-00236-340-7.

6. Дерябин Н.И. Медицинский кульбит: человек в глобальном кибернетическом социуме. Сборник статей XXVI Международной научно-практической конференции «European scientific conference», г. Пенза, МЦНС «Наука и Просвещение», 07.06.2021, с. 324. С. 291 – 294. ISBN: 978-5-00159-898-5.

7. Дерябин Н.И. Креатор в структурах сильного искусственного интеллекта. Монография «Наука, инновации, общество: актуальные вопросы и современные аспекты», г. Пенза, МЦНС «Наука и Просвещение», 15.01.2024 г., с. 216, С. 184 – 195. ISBN 978-5-00236-185-4.

8. Дерябин Н.И. Мировоззренческая парадигма сильного искусственного интеллекта. Монография «Современная наука: актуальные вопросы, достижения и инновации», г. Пенза, МЦНС «Наука и Просвещение», 25.08.2023 г., с. 212, С. 197 – 210. ISBN 978-5-00173-980-7.

РАЗДЕЛ III. СОВРЕМЕННЫЕ ТЕХНОЛОГИИ КАК ФАКТОР И РЕЗУЛЬТАТ ИННОВАЦИОННОГО РАЗВИТИЯ

УДК 543.554

ГЛАВА 11. ПОТЕНЦИОМЕТРИЧЕСКИЕ СЕНСОРНЫЕ СИСТЕМЫ ДЛЯ ОЦЕНКИ АНТИОКСИДАНТНОЙ АКТИВНОСТИ

Тарасов Алексей Валерьевич

К.Т.Н.

ФГБОУ ВО «Уральский государственный экономический университет»

Аннотация: взаимосвязь окислительного стресса с состоянием здоровья человека привела к использованию антиоксидантов в профилактических и терапевтических подходах при различных заболеваниях. Измерение интегрального (кумулятивного) содержания антиоксидантов является менее трудоемким и успешно применяется в контроле антиоксидантной терапии и квалиметрической оценке пищевой, косметической и фармацевтической продукции. В этой работе систематизированы результаты разработки и апробации потенциометрических сенсорных систем (ПСС), предназначенных для оценки антиоксидантной активности (АОА) с использованием медиаторной системы $K_3[Fe(CN)_6]/K_4[Fe(CN)_6]$. Различные процедуры потенциометрического определения АОА подробно описаны и проиллюстрированы. Традиционные процедуры анализа основаны на применении двухэлектродных ПСС в оценке АОА растворов, экстрактов и прочих жидких образцов. Новые и усовершенствованные процедуры анализа основаны на применении двухэлектродных ПСС в оценке АОА плодоовощной и кондитерской продукции без предварительной жидкостной экстракции, а также трехэлектродных ПСС в неинвазивной оценке АОА кожи человека.

Ключевые слова: антиоксидантная активность, потенциометрия, сенсорная система, одноэлектродный электрод, модифицированный электрод, гибкий электрод, трафаретная печать, горячее ламинирование, безэкстракционный анализ, быстрый анализ, анализ в режиме реального времени, неинвазивный анализ.

POTENTIOMETRIC SENSOR SYSTEMS FOR ASSESSING ANTIOXIDANT ACTIVITY

Tarasov Aleksey Valerievich

Abstract: The relationship between oxidative stress and human health has led to the use of antioxidants in preventive and therapeutic approaches for a variety of diseases. Measuring the integral (cumulative) content of antioxidants is less labor-intensive and is successfully used in the control of antioxidant therapy and the qualimetric assessment of food, cosmetic and pharmaceutical products. This work systematizes the results of the development and testing of potentiometric sensor systems (PSSs) designed to assess antioxidant activity (AOA) using the $K_3[Fe(CN)_6]/K_4[Fe(CN)_6]$ mediator system. Various procedures for the potentiometric determination of AOA are described and illustrated in detail. Traditional analysis procedures are based on the use of two-electrode PSSs in assessing the AOA of solutions, extracts and other liquid samples. New and improved analysis procedures are based on the use of two-electrode PSSs in the assessment of the AOA of fruit and vegetable and confectionery products without preliminary liquid extraction, as well as three-electrode PSSs in the non-invasive assessment of the AOA of human skin.

Key words: antioxidant activity, potentiometry, sensor system, disposable electrode, modified elec-

trode, flexible electrode, screen printing, hot lamination, non-extraction analysis, rapid analysis, real-time analysis, non-invasive analysis.

1. МОНИТОРИНГ АНТИОКСИДАНТНОЙ АКТИВНОСТИ И ЕГО ЗНАЧЕНИЕ ДЛЯ НАУКИ, ПРОМЫШЛЕННОСТИ И МЕДИЦИНЫ

Современный образ жизни человека, связанный с употреблением переработанной пищи, воздействием широкого спектра вредных веществ и недостаточной физической активностью, играет важную роль в индукции окислительного стресса. В зависимости от интенсивности проявления окислительный стресс может быть классифицирован на эустресс, характеризующийся физиологическим уровнем окислителей и протеканием сигнально-регуляторных процессов, или дистресс, характеризующийся повышенным уровнем окислителей и токсичной окислительной нагрузкой [1]. Повышенный уровень окислительного стресса связан с множеством патологических процессов, включая окислительное повреждение биомолекул, митохондриальную дисфункцию, неинфекционные заболевания, вирусные инфекции и старение [2–4]. По приблизительным оценкам окислительный стресс участвует в патогенезе около 200 заболеваний человека [5], включая социально-значимые злокачественные новообразования, болезни сердечно-сосудистой системы, сахарный диабет и психоневрологические расстройства. Ослабление окислительного стресса в организме достигается в результате согласованного действия ферментативных (супероксиддисмутаза, каталаза, глутатионпероксидаза и др.) и неферментативных (витамины А, Е и С, флавоноиды, каротиноиды, мелатонин и др.) антиоксидантов. Первой линией защиты от перекисного окисления липидов выступает витамин Е, поэтому он может рассматриваться как один из самых эффективных антиоксидантов [2]. Под антиоксидантом следует понимать любое вещество, ингибирующее окисление [6]. С биологической точки зрения антиоксиданты играют полезную для здоровья роль, прерывая образование и ограничивая распространение окислителей радикальной и нерадикальной природы посредством следующих механизмов: перенос электрона, перенос атома водорода и хелатирование переходного металла [7, с. 2-1–2-20]. Взаимосвязь с состоянием здоровья человека привела к большому количеству исследований окислительного стресса и антиоксидантов, разработке методов и средств их мониторинга. На рисунке 1 показана динамика публикаций по окислительному стрессу и антиоксидантам в международной базе данных PubMed [8].

Можно выделить два аналитических подхода для характеристики антиоксидантного статуса образца: измерение концентрации отдельных антиоксидантных соединений и определение их общего содержания [9]. Измерение концентрации отдельных антиоксидантов занимает много времени, является трудоемким, дорогостоящим и требует сложных методов анализа. Поэтому в рутинных анализах большое распространение получила методология оценки общего содержания антиоксидантов. Общее содержание антиоксидантов может

представлять собой аддитивную величину в случае невзаимодействующих антиоксидантных соединений или интегральную (кумулятивную) величину в случае взаимодействующих антиоксидантных соединений. В сложных многокомпонентных матрицах антиоксидантные соединения способны взаимодействовать между собой [10], а также с белками, липидами, углеводами и ионами металлов [11, 12]. Эти взаимодействия могут характеризоваться синергетическими и/или антагонистическими антиоксидантными эффектами. Это делает применение аддитивной величины в характеристике общего содержания антиоксидантов неэффективным, поскольку результат может оказаться заниженным (преобладание синергетических эффектов) или завышенным (преобладание антагонистических эффектов). По этой причине общее содержание антиоксидантов рекомендуется характеризовать с применением более информативной интегральной величины. В различных методах для обозначения интегральной концентрации антиоксидантов используются разные термины, среди которых наиболее часто употребляются понятия «активность» и «емкость» [9]. В настоящее время разработано достаточно большое количество методов измерения антиоксидантной активности/емкости (АОА/АОЕ), которые могут быть классифицированы по механизму реакции или способу регистрации аналитического сигнала [13–18]. Интерес к электрохимическим методам оценки АОА/АОЕ обусловлен электроактивностью большинства антиоксидантов и связан с большими успехами, достигнутыми в миниатюризации приборов [17, 18]. Несмотря на то, что разница между АОА и АОЕ подчеркивалась в ряде исследований [19], использование термина «антиоксидантная активность» (АОА) в потенциометрии обусловлено историческим аспектом и основано на использовании уравнения Нернста [20].

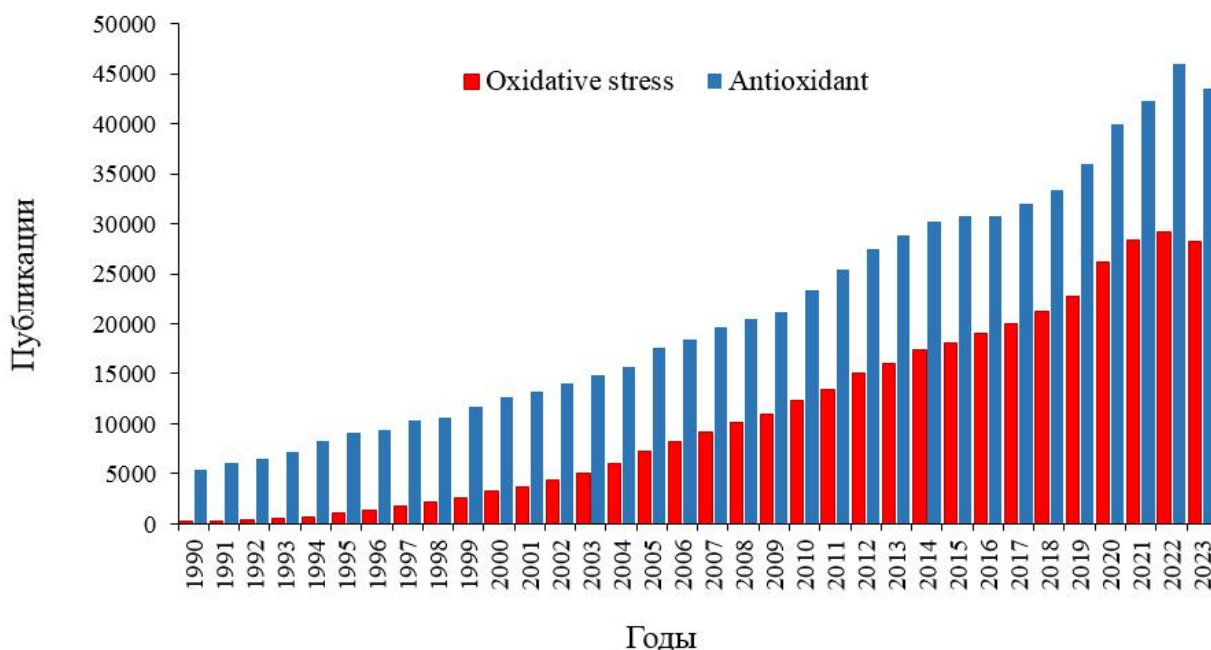


Рис. 1. Количество публикаций по запросам «окислительный стресс» и «антиоксидант» в базе данных PubMed за период 1990–2023 гг.

Естественными природными источниками антиоксидантов являются растения. Как следствие, современная пищевая, косметическая и фармацевтическая промышленность ориентирована на использование растительного лекарственно-технического сырья с антиоксидантными свойствами [21]. В то же время разработка и выведение на рынок продуктов антиоксидантной направленности невозможны без подтверждения и контроля их эффективности в течение заявленного срока хранения. Применение антиоксидантов в профилактических и лечебных подходах получило название «антиоксидантная терапия» [2]. В качестве основного немедикаментозного направления антиоксидантной терапии рассматривается питание [22], что открывает большие перспективы в разработке специализированных, функциональных и обогащенных продуктов питания антиоксидантной направленности. В биомедицинском аспекте исследование антиоксидантных свойств имеет важное значение с позиций мониторинга окислительного стресса и контроля эффективности антиоксидантной терапии. Обнаружение биомаркеров окислительного стресса было в центре внимания многих исследований, поскольку они обладают потенциалом действовать как интегральные показатели патологических процессов при различных заболеваниях. Определение окислительных (оксидантных) и восстановительных (антиоксидантных) биомаркеров – это два основных направления в мониторинге окислительного стресса, имеющих взаимодополняющую ценность в обеспечении информативных результатов. Прямое количественное определение активных форм кислорода, азота и других окислительных маркеров до сих пор остается трудной задачей в силу их неспецифичной реакционной способности и малого срока жизни. Поэтому в мониторинге окислительного стресса используют, в основном, оценку продуктов окислительного повреждения биомолекул и/или уровней ферментативных и неферментативных антиоксидантов. Обычно эти биомаркеры определяют в различных фракциях крови. Сообщалось, например, о снижении АОА/АОЕ плазмы крови при сердечно-сосудистых заболеваниях [23]. Неинвазивный отбор образцов имеет преимущества перед инвазивным отбором в экономичности, снижении трудоемкости и уменьшении риска инфицирования. Как следствие, в мониторинге окислительного стресса неинвазивно отбираемые образцы все чаще рассматриваются в качестве альтернативы инвазивно отбираемым образцам. Определенные успехи были достигнуты в анализе слюны, мочи, конденсата выдыхаемого воздуха и эякулята, изменение АОА/АОЕ которых было связано с заболеваниями ротовой полости, болезнями почек, воспалительными патологиями легких и фертильным потенциалом мужчин [24–26].

Следует отметить, что в более широком смысле под АОА понимается вид биологической (фармакологической) активности [6, 27]. В этом аспекте АОА используется в характеристике пищевых, косметических, фармацевтических и клинических образцов, а также новых синтезированных соединений. Таким образом, мониторинг АОА имеет важное значение для науки, промышленности и медицины. Однако, сложившаяся ситуация, связанная с отсутствием общепри-

нятых терминов и единиц измерений, существенно затрудняет интерпретацию и сравнение результатов [9].

2. ПОТЕНЦИОМЕТРИЧЕСКИЙ МЕТОД ОПРЕДЕЛЕНИЯ АНТИОКСИДАНТНОЙ АКТИВНОСТИ С ИСПОЛЬЗОВАНИЕМ МЕДИАТОРНОЙ СИСТЕМЫ $K_3[Fe(CN)_6]/K_4[Fe(CN)_6]$

Потенциометрический метод определения АОА с использованием медиаторной системы гексацианоферратов калия ($K_3[Fe(CN)_6]/K_4[Fe(CN)_6]$) был разработан Х. З. Брайниной и А. В. Ивановой в 2002 году на базе Уральского государственного экономического университета [20]. Позднее этот метод был адаптирован для анализа биологических тканей [28] и проточно-инжекционного анализа [29]. В основе потенциометрического определения АОА лежит химическая реакция (1) между окисленной формой медиаторной системы и антиоксидантами исследуемого образца:



где $[Fe(CN)_6]^{3-}$ – окисленная форма медиаторной системы; $[Fe(CN)_6]^{4-}$ – восстановленная форма медиаторной системы; AO_{Red} – антиоксидант; AO_{Ox} – продукт окисления антиоксиданта; b – стехиометрический коэффициент. В результате протекания реакции (1) концентрация ферри- и ферроцианид ионов в электрохимической ячейке изменяется, что влечет изменение электродного потенциала и служит аналитическим сигналом. В качестве раствора реагента используется буфер с физиологичным уровнем pH, содержащий медиаторную систему $K_3[Fe(CN)_6]/K_4[Fe(CN)_6]$ определенного состава.

АОА представляет собой эффективную концентрацию феррицианида калия, прореагировавшего с антиоксидантами образца. АОА выражается в универсальных единицах (моль-экв/л) и рассчитывается по формуле (2):

$$AOA = \frac{C_{Ox} - a \cdot C_{red}}{1 + a} \cdot q, \quad a = \frac{C_{Ox}}{C_{red}} \cdot 10^{\frac{(E_2 - E_1) \cdot F}{2,3 \cdot R \cdot T}}, \quad (2)$$

где C_{Ox} – концентрация феррицианида калия (моль/л); C_{red} – концентрация ферроцианида калия (моль/л); q – разбавление пробы (безразмерная величина); E_1 – значение потенциала до введения пробы (В); E_2 – значение потенциала в после введения пробы (В); F – постоянная Фарадея (Кл/моль); R – универсальная газовая постоянная (Кл/моль·К); T – термодинамическая температура (К).

Значительная часть валидационных исследований была сосредоточена на анализе эталонных антиоксидантных соединений [29–31], выявлении корреляции с другими аналитическими методами [30–33], оценке основных метрологических характеристик [33, 34], унификации состава медиаторной системы [35] и изучении интерференционных эффектов потенциально мешающих веществ [36]. Показано, что результаты потенциометрической оценки АОА различных объектов коррелируют с данными спектрофотометрических анализов, хемилюминесценции и флуориметрии. Исследования последних лет свидетельствуют об успешном применении потенциометрического метода оценки АОА в характеристике прототипов лекарств [29], функциональных продуктов питания [37],

косметических средств [38] и ассоциированных с окислительным стрессом заболеваний [39–41].

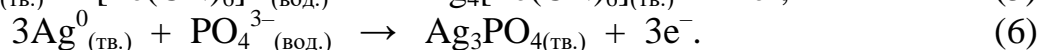
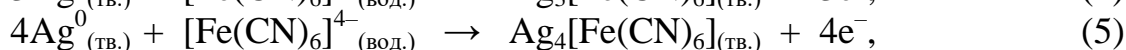
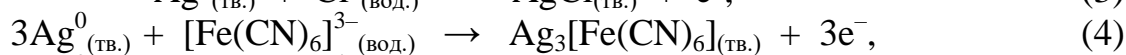
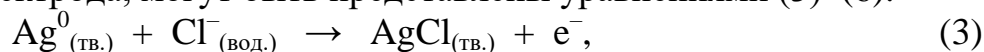
Потенциометрическое определение АОА сопряжено с использованием платинового индикаторного электрода и хлорсеребряного электрода сравнения [20, 28–41]. Золотой индикаторный электрод, как правило, не используется вследствие его меньшей инертности и возможной адсорбции хлорид-, фосфат-, и цианид-анионов из анализируемого раствора [42–44]. Однако используемые в анализе коммерческие электроды требуют обслуживания, что затрудняет дальнейшее внедрение метода в промышленную и медицинскую практику. В частности, многократное использование платинового электрода предполагает его регенерацию и стерилизацию. Очищение поверхности платинового электрода от следов предыдущих анализов и оксидных окислов может быть выполнено с помощью механической полировки, термического обжига, обработки растворителем, лазерной активации, электрохимической поляризации или путем комбинации этих способов [45, с. 143–147]. Сообщалось, однако, что очищение платинового электрода с помощью этанола или ацетона является малоэффективным, в то время как термический обжиг оказался успешным способом регенерации и дезинфекции [35]. Хлорсеребряный электрод сравнения нуждается в заполнении раствором внутреннего электролита и проверке потенциала [46]. Эти способы подготовки электродов требуют наличия дополнительных реактивов и оборудования, а в некоторых случаях и определенной квалификации персонала. Таким образом, разработка не требующих обслуживания одноразовых электродов для потенциометрического определения АОА является актуальным направлением исследований, связана с развитием метода и направлена на сокращение разрыва между лабораторным и внелабораторным анализом.

3. ПОТЕНЦИОМЕТРИЧЕСКИЕ СЕНСОРНЫЕ СИСТЕМЫ ДЛЯ ОЦЕНКИ АНТИОКСИДАНТНОЙ АКТИВНОСТИ В СОЧЕТАНИИ С $K_3[Fe(CN)_6]/K_4[Fe(CN)_6]$

3.1. Разработка потенциометрических сенсорных систем

Точность и правильность электрохимических измерений зависит от работы электрода сравнения, при этом в потенциометрии к стабильности потенциала электрода сравнения предъявляются повышенные требования [47, с. 289]. Новый твердотельный квази-электрод сравнения планарного типа был разработан с применением технологий трафаретной печати и электрохимического осаждения [48]. Трафаретная печать применялась для нанесения серебряной пасты на неэлектропроводящую подложку, в качестве которой использовалась алюмооксидная керамика, стеклотекстолит или полиэтилентерефталат. Модифицирование серебряного печатного электрода было выполнено в различных условиях. Во-первых, модифицирование серебряного печатного электрода было выполнено в хлоридсодержащих растворах ($FeCl_3$, KCl , HCl) с применением литературных методик. Таким образом были получены хлорсеребряные квази-электроды

сравнения, которые использовались в качестве контроля. Во-вторых, модифицирование серебряного печатного электрода было выполнено с использованием содержащего $K_3[Fe(CN)_6]/K_4[Fe(CN)_6]$ раствора в условиях разомкнутой цепи, потенциостатической или потенциодинамической поляризации. Раствор для потенциометрического определения АОА содержит хлорид-, феррицианид-, ферроцианид и фосфат-анионы, которые образуют с металлическим серебром труднорастворимые соединения хлорида серебра, феррицианида серебра, ферроцианида серебра и фосфата серебра, соответственно. При контакте серебряного электрода с этим раствором возможно образование смешанного осадка Ag_nX ($X = Cl^-, [Fe(CN)_6]^{3-}, [Fe(CN)_6]^{4-}$ и PO_4^{3-}), состав которого определяется потенциалом поляризации электрода и равновесной концентрацией ионов серебра. Процессы, участвующие в формировании осадка на поверхности серебряного печатного электрода, могут быть представлены уравнениями (3)–(6):



В условиях разомкнутой цепи процессы (3)–(6) представлены самопроизвольными реакциями ионного обмена, тогда как в условиях потенциостатической или потенциодинамической поляризации процессы (3)–(6) представлены электрохимически индуцированными реакциями.

Сравнительная оценка потенциальной стабильности модифицированных электродов была выполнена в условиях, модулирующих потенциометрическое определение АОА. Хлорсеребряные квази-электроды продемонстрировали высокие значения времени стабилизации потенциала и оказались непригодными к использованию в качестве электродов сравнения в условиях потенциометрического определения АОА. Среди квази-электродов со смешанными осадками наилучшую стабильность в растворе с переменным содержанием $K_3[Fe(CN)_6]/K_4[Fe(CN)_6]$ продемонстрировал электрод, модифицированный при постоянном приложенном потенциале 0.325 В (отн. $Ag/AgCl/KCl, 3.5 M$) в течение 120 секунд. В этих условиях на поверхности серебряного печатного электрода формируется осадок, состоящий преимущественно из хлорида серебра и феррицианида серебра. Морфология поверхности электрода была изучена с помощью сканирующей электронной микроскопии и было высказано предположение, что мелкокристаллический осадок феррицианида серебра заполняет поры между крупными кристаллами хлорида серебра, что приводит к улучшению стабильности квази-электрода со смешанным осадком по сравнению с хлорсеребряными квази-электродами [48]. Сообщалось также о применении функции желательности Харрингтона в многофакторной оценке стабильности квази-электродов сравнения с целью выбора оптимальных условий их модифицирования [49]. Улучшение долговременной стабильности разработанного квази-электрода сравнения может быть достигнуто в результате применения наружного защитного покрытия из термоотвержденной перфторированной мембраны «Нафюн» [50].

В качестве планарных индикаторных электродов использовались коммерческий платиновый печатный электрод на основе алюмооксидной керамики [48, 51, 52], эффективность которого была подтверждена в предыдущих исследованиях, а также новые углеродсодержащие электроды. Трафаретная печать использовалась для нанесения углеродной пасты на стеклотекстолит [50, 53] или полиэтилентерефталат [54–56]. Цитратные наночастицы золота и многослойные углеродные нанотрубки использовались в поверхностном и объемном модифицировании углеродных печатных электродов, соответственно, с целью улучшения их электропроводности и потенциальной стабильности. Одностороннее горячее ламинирование применялось для склеивания углеродной вуали с подложкой на основе полиэтилентерефталата [57]. Углеродная вуаль, называемая также углеродной бумагой, представляет собой нетканый углеволоконный материал с развитой трехмерной поверхностью, который находит широкое применение в амперометрических и вольтамперометрических (био)сенсорах [58]. Возможность применения углеродной вуали в потенциометрических сенсорах была впервые показана в работе [57].

Индикаторные электроды и электроды сравнения были объединены по типу подложки в потенциометрические сенсорные системы (ПСС) на основе алюмооксидной керамики, стеклотекстолита и полиэтилентерефталата, которые были апробированы в оценке АОА различных объектов (табл. 1). Снижение толщины полиэтилентерефталатной подложки до 0,25 мм позволило получить гибкие электроды [57]. Применение масштабируемых технологий трафаретной печати и горячего ламинирования обеспечило быстрое и недорогое прототипирование электродов [59, с. 69–98]. Благодаря твердотельной планарной конструкции разработанные ПСС могут эксплуатироваться в различных пространственных ориентациях [47, с. 92].

Таблица 1

ПСС для оценки АОА в сочетании с $K_3[Fe(CN)_6]/K_4[Fe(CN)_6]$

| ПСС | Индикаторный электрод | Электрод сравнения | Применение | Источники |
|-------|-----------------------------|----------------------------|---|--------------|
| АК | Pt/АК (40×5×0,5 мм) | O/Ag/АК (40×5×0,5 мм) | Эталонные антиоксиданты, напитки, плоды фруктов и овощей, биожидкости | [48, 51, 52] |
| СТ | AuНЧ/С/СТ (35×2×0,35 мм) | O/Ag/СТ (35×2×0,35 мм) | Эталонные антиоксиданты, напитки, кожа | [50, 53] |
| ПЭТ-1 | МУНТ-С/ПЭТ (35×2×0,5 мм) | O/Ag/ПЭТ (35×2×0,5 мм) | Эталонные антиоксиданты, напитки, кондитерские изделия | [54–56] |
| ПЭТ-2 | УВ/ПЭТ (35×3×0,25 мм) | O/Ag/ПЭТ (35×3×0,25 мм) | Эталонные антиоксиданты, кожа, фитокосметика | [57] |

Примечание: ПСС – потенциометрическая сенсорная система; АК – алюмооксидная керамика; СТ – стеклотекстолит; ПЭТ – полиэтилентерефталат; AuНЧ – наночастицы золота; МУНТ – многослойные углеродные нанотрубки; УВ – углеродная вуаль; O – смешанный осадок AgCl и $Ag_3[Fe(CN)_6]$. В круглых скобках указаны в мм длина, ширина и толщина электродов.

3.2. Оптимизация подготовки пищевых образцов

Мобильный, полевой или *on-site* анализ интенсивно развивается. В клинико-диагностической практике это направление химического анализа получило название «тестирование в месте оказания медицинской помощи» [59]. Авторы работы [60, с. 7] отмечают, что сегодня «аналитическая лаборатория приходит в поле», а «перенос образцов заменяется переносом информации». Необходимыми условиями осуществления *on-site* анализа являются применение портативного оборудования и оптимизация подготовки пробы. Электрохимические датчики характеризуются быстрым временем отклика, а электрохимические устройства, как правило, имеют низкую стоимость и допускают неограниченную миниатюризацию [17, 18]. Подготовка образцов – это предварительный этап аналитического процесса, на котором образцы обрабатываются до состояния, пригодного для анализа. Самым распространенным способом подготовки пищевых образцов служит жидкостная экстракция, которая характеризуется зависимостью выхода антиоксидантных веществ от параметров экстракционного процесса (типа растворителя, температуры, времени и т.д.). Определение оптимальных условий экстракции, обеспечивающих максимальный выход антиоксидантных веществ, является трудоемкой задачей [61]. Методы определения АОА, использующие жидкостную экстракцию в качестве этапа предварительной подготовки образцов, решают большой спектр аналитических задач, но являются трудоемкими и бесперспективными для *on-site* анализа. Существующий разрыв между лабораторным и внелабораторным анализом призваны сократить модифицированные методы оценки АОА с оптимизированной пробоподготовкой.

К преимуществам потенциометрического метода определения АОА следует отнести простую процедуру анализа, низкую стоимость реактивов и оборудования. Этот метод не требует применения стандарта и построения калибровочного графика, при этом окрашенные образцы могут быть проанализированы без предварительного многократного разбавления. Раствор реагента вводится в электрохимическую ячейку или же используется для пропитки микропористой мембраны. Первый способ измерения используется в анализе растворов, экстрактов и прочих жидких образцов (рис. 2а). Второй способ измерения с использованием микропористой мембраны изначально был предложен для анализа кожи человека [62]. Позднее этот способ измерения был назван «контактным» и применен в анализе пищевых образцов с полутвердой (упругой) консистенцией (рис. 2б). С применением разработанных ПСС контактный способ измерения использовался в анализе кожи человека [53, 57], плодов фруктов и овощей [51] и корпусов кондитерских изделий [56] в режиме реального времени (*in situ*). С целью обеспечения диффузии антиоксидантов в микропористую мембрану может применяться местное давление, рекомендуемая величина которого составляет 35–40 мм рт.ст. или 4.67–5.33 кПа.

При контактном способе измерения пробоподготовка пищевых образцов исключает жидкостную экстракцию и сокращается до получения среза (рис. 2б) Анализ срезов пищевых образцов характеризуется низкой трудоемкостью и

экспрессностью. Исключение жидкостной экстракции позволяет снизить долю труда, сократить издержки и уменьшить время анализа (табл. 2).

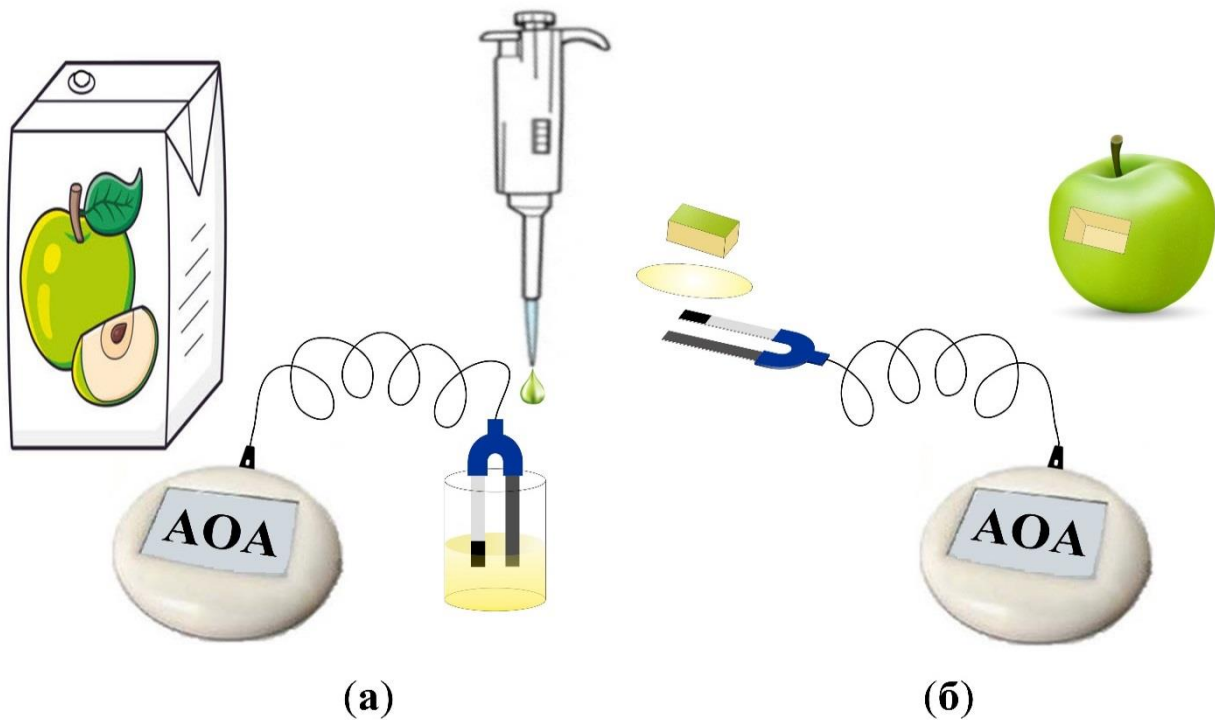


Рис. 2. Применение двухэлектродной ПСС в оценке АОА жидкого (а) и нежидкого (б) пищевого образца.

Таблица 2

Трудоемкость спектрофотометрического и потенциометрического методов определения АОА при анализе нежидких пищевых продуктов

| Стадия | Спектрофотометрия | Потенциометрия | |
|------------------------------------|-------------------|-----------------------|-------------------|
| | | Оригинальная методика | Экспресс-методика |
| Преаналитический этап | | | |
| – Измельчение | + | + | – |
| – Жидкостная экстракция | + | + | – |
| – Приготовление реагентов | + | + | + |
| – Подготовка электродов | – | + | – |
| Аналитический этап | | | |
| – Построение калибровки | + | – | – |
| – Разбавление окрашенной пробы | + | – | – |
| – Инкубация реакционной смеси | + | – | – |
| – Измерение аналитического сигнала | + | + | + |

3.3. Совершенствование способа регистрации сигнала

Обычная двухэлектродная конфигурация ПСС включает один индикаторный электрод и один электрод сравнения. В работах [53, 57] были впервые предложены трехэлектродные ПСС для оценки АОА кожи человека, которые включали два одинаковых индикаторных электрода, соединенных с общим

электродом сравнения (рис. 3). Предложенный подход весьма важен, поскольку кожа человека является сложным аналитическим объектом и ее параметры, в том числе АОА, могут меняться с течением времени под воздействием различных внешних и внутренних факторов. Известно, что в краткосрочной перспективе образование свободных радикалов и снижение уровней антиоксидантов в коже наблюдается под воздействием солнечного света, при чем эти эффекты усиливаются с повышением температуры [63, 64]. Синергистами этих фототоксичных процессов могут выступать озон, полициклические ароматические углеводороды, твердые частицы и другие загрязняющие вещества [65, 66]. С привлечением потенциометрического метода было показано, что АОА кожи человека может зависеть от качества пищи [28] и артериального давления [39]. Чтобы свести к минимуму влияние переменного состояния кожи на результаты анализа, временной интервал между повторными измерениями должен стремиться к нулю. Этому условию соответствует использование трехэлектродных ПСС, поскольку за одно измерение можно получить два аналитических результата.

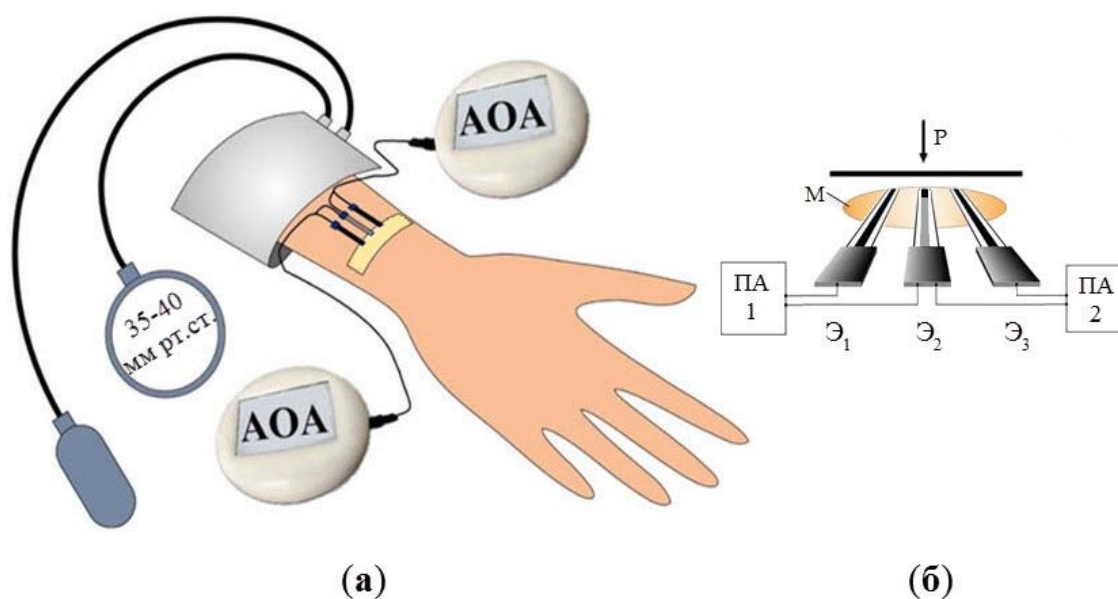


Рис. 3. Применение трехэлектродной ПСС в оценке АОА кожи человека (а) и соответствующая схема подключения электродов (б). Обозначения: ПА 1 и ПА 2 – потенциометрические анализаторы; Э₁ и Э₃ – индикаторные электроды; Э₂ – электрод сравнения; М – содержащая $K_3[Fe(CN)_6]/K_4[Fe(CN)_6]$ микропористая мембрана; Р – местное давление.

3.4. Анализ пищевых продуктов

Применение антиоксидантов в технологии изготовления продуктов питания предусматривает их мониторинг. ПСС были опробованы в оценке АОА безалкогольных и алкогольных напитков из розничной торговой сети. Схематическое изображение измерительного процесса показано на рисунке 2а. Результаты, полученные с использованием ПСС и коммерческих электродов, имели одинаковую воспроизводимость и статистически незначимые различия

[48, 50, 54]. Результаты анализа безалкогольных и алкогольных напитков, полученные с использованием ПСС и стандартного спектрофотометрического метода Фолина-Чокальтеу, также положительно коррелировали между собой (рис. 4) [55]. Свежевыжатые соки продемонстрировали большие значения АОА по сравнению с коммерческими образцами, что согласовывалось с ранее опубликованными данными [33]. Проанализированные вина по величине АОА располагались в порядке красные > розовые > белые, что также согласовывалось с результатами независимых исследований [67, 68]. Однако, используемые в консервации вин сульфиты (Е221–Е228) способны окисляться феррицианидом калия и вносить вклад в измеряемую величину АОА [36]. Положительная интерференция сульфитов характерна для других методов определения АОА и вызывает серьезную озабоченность в анализе белых вин [69].

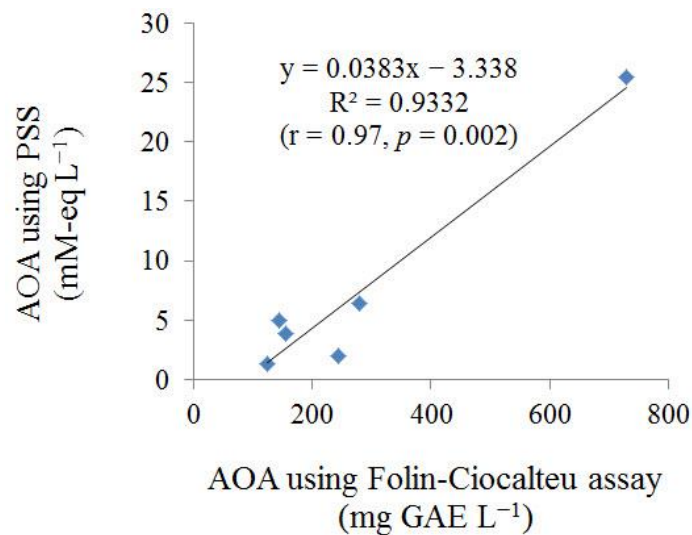


Рис. 4. Взаимосвязь результатов анализа напитков, полученных с использованием ПСС и метода Фолина-Чокальтеу [55].

ПСС на основе алюмооксидной керамики бала применена в оценке АОА функциональных сывороточных напитков. Это позволило смоделировать сывороточные напитки на сахаре и сукралозе с высокой АОА, уровень которой был соизмерим с АОА свежевыжатых соков [52].

Флодоовощная и кондитерская продукция была проанализирована без предварительной жидкостной экстракции с применением разработанных ПСС [51, 56]. Схематическое изображение измерительного процесса показано на рисунке 2б. Возможность анализировать пищевые образцы с полутвердой (упругой) консистенцией была достигнута в результате применения разработанного электрода сравнения [48]. Планарная твердотельная конструкция разработанного электрода позволила эксплуатировать его не только в вертикальном положении при анализе жидких проб, но также и в горизонтальном положении при анализе нежидких объектов. Проанализированные срезы фруктов и овощей по величине АОА располагались в следующем порядке: чеснок > свекла > помидор > персик > груша > дыня > огурец > яблоко > тыква > слива > морковь. По-

лученные результаты были валидированы с помощью метода добавления стандарта (аскорбиновая кислота) непосредственно на срез тестируемого образца, а также путем сравнения результатов анализа срезов с результатами анализа суспензий, полученных из тех же самых образцов фруктов и овощей. Однако, контактный способ потенциометрического определения АОА оказался непригодным для анализа плодов цитрусовых, что было связано с их ячеистой структурой [51]. Срезы кондитерских изделий, обогащенных растительными ингредиентами, были проанализированы в условиях приложенного внешнего давления. В качестве контроля были проанализированы настои, полученные из тех же самых образцов кондитерских изделий. Результаты анализа срезов жележных изделий отличались хорошей воспроизводимостью, тогда результаты анализа срезов пастильных изделий имели неудовлетворительную воспроизводимую [56].

3.5. Анализ кожи добровольцев

Современные исследования показывают связь между окислительным стрессом, старением кожи и рядом кожных заболеваний, таких как дерматит, витилиго, акне, розацеа, псориаз, рак и некоторые другие [70]. Растущий интерес к молодому внешнему виду стимулировал большое количество исследований в области применения антиоксидантов в наружных косметических и пероральных нутрицевтиках. Конвергенция между пищевой и косметической промышленностью привела к появлению нутрикосметиков – новых пищевых продуктов, способствующих профилактике заболеваний и здоровью кожи [71]. Потенциометрический метод с использованием медиаторной системы $K_3[Fe(CN)_6]/K_4[Fe(CN)_6]$ был предложен для неинвазивного определения АОА кожи человека в 2010 году [28] и с тех пор получил две модификации. В первой модификации кристаллические компоненты $K_3[Fe(CN)_6]/K_4[Fe(CN)_6]$ вводились в ЭКГ-гель [28], что приводило к их неравномерному распределению в полученной электропроводящей матрице. Коммерческие гели для электрокардиографии имеют рН в интервале от 6 до 7, тогда как среднее значение физиологического диапазона рН здоровой кожи человека равно 5 [72]. Во второй модификации кристаллические компоненты $K_3[Fe(CN)_6]/K_4[Fe(CN)_6]$ растворялись в буфере с варьируемым уровнем рН, а полученный раствор реагента использовался для пропитки микропористой ацетатцеллюлозной мембраны [62]. Использование микропористой мембраны привело к лучшей воспроизводимости результатов измерений за счет устранения проблем, вызванных различной толщиной гелевого слоя и неравномерным распределением медиатора. Однако вопрос разработки одноразовых ПСС для скрининговых исследований АОА кожи человека оставался актуальным.

Трехэлектродные ПСС были разработаны и применены в оценке АОА кожи добровольцев в работах [53, 57]. Схематическое изображение измерительного процесса показано на рисунке 3. Эффективность предложенных ПСС была продемонстрирована в оценке обычного и дополненного антиоксидантами питания [53], а также различных типов фитокосметических продуктов [57]. Влия-

ние дополненного витаминами питания и фитокосметических продуктов на АОА кожи добровольцев показано на рисунках 5 и 6, соответственно. Важным аналитическим следствием служило достижение улучшенной воспроизводимости результатов анализа с использованием гибкой ПСС [57].

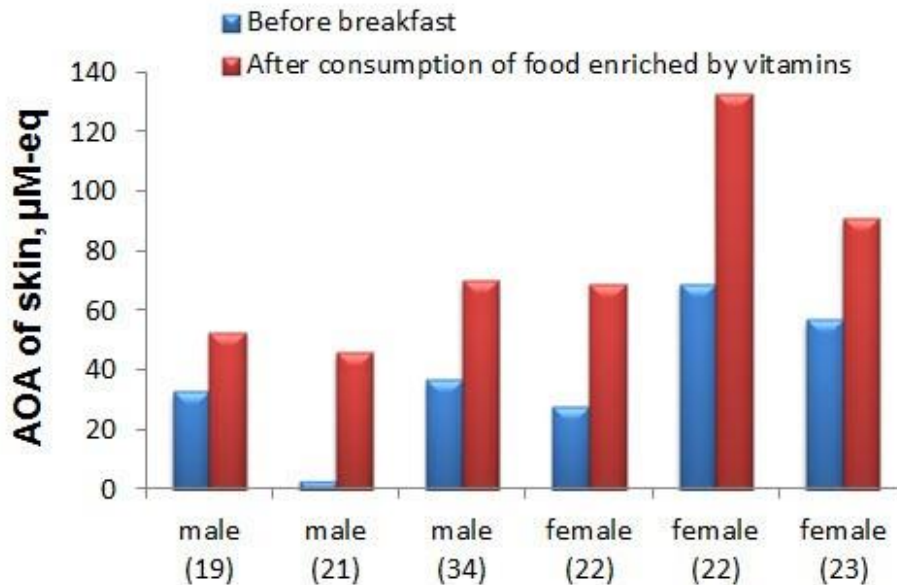


Рис. 5. Влияние пищи, обогащенной витаминами (100 мг аскорбиновой кислоты и 100 мг рутина), на АОА кожи добровольцев. В круглых скобках указан возраст испытуемых [53].

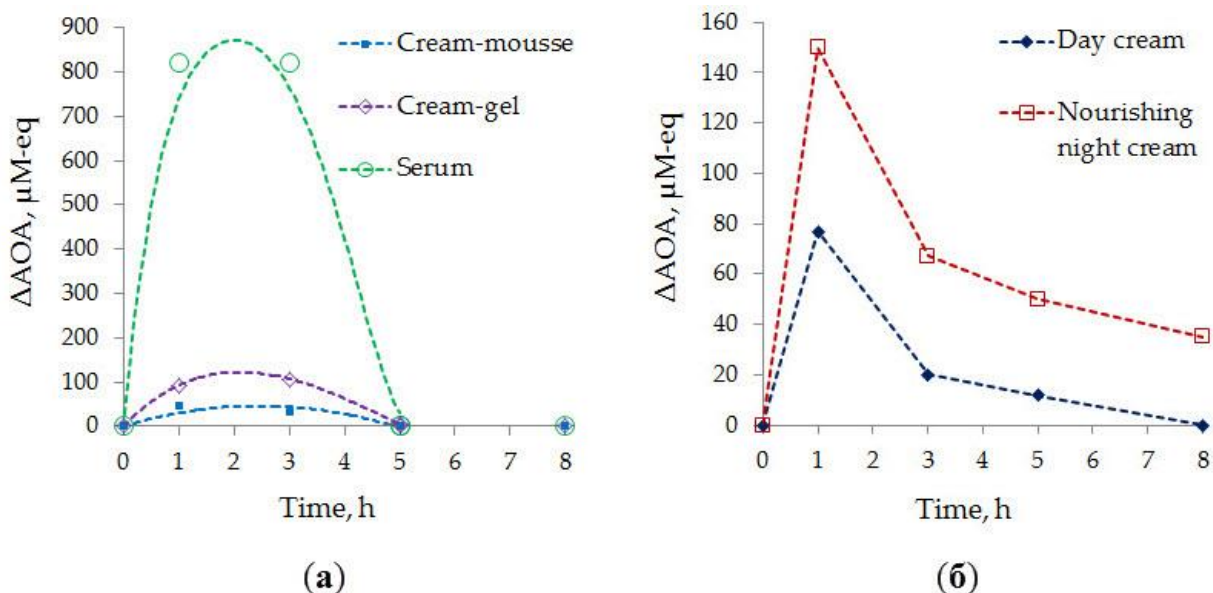


Рис. 6. Влияние фитокосметических продуктов на АОА кожи молодой женщины (28 лет): крем-мусса, крем-геля, сыворотки (а), крема дневного и крема ночного питательного (б). Время экспозиции 8 часов [57].

Известно, что воспроизводимость тактильных кожных сенсоров связана со следующими факторами: эффективный отбор проб, т.е. транспортировка анали-

та к поверхности сенсора; загрязнение сенсора; изменчивое состояние кожи; плохой контакт, приводящий к ненадежному аналитическому сигналу [73–75]. В работах [53, 57] были предприняты стратегии, направленные на улучшение воспроизводимости результатов потенциометрического определения АОА кожи человека. Во-первых, предложенные ПСС являются одноразовыми, что исключает их загрязнение при повторном использовании и делает их безопасными для испытуемых. Во-вторых, трехэлектродные конфигурации ПСС позволяют получать два результата за одно измерение, что исключает возможное влияние изменяющегося во времени состояния кожи. В-третьих, гибкие электроды в составе ПСС обеспечивают улучшенный контакт на гетерогенной межфазной границе «электрод – микропористая мембрана с $K_3[Fe(CN)_6]/K_4[Fe(CN)_6]$ – кожа» и способствуют измерению стабильного аналитического сигнала (потенциала) в условиях нагрузки (местного давления). Сравнительная характеристика коммерческих и разработанных ПСС для оценки АОА кожи человека показана в таблице 3, из которой видно, что именно гибкая ПСС обеспечивает наилучшую воспроизводимость результатов анализа.

Таблица 3

**Характеристика коммерческих и разработанных ПСС для оценки АОА
кожи человека**

| ПСС | | Медиатор $K_3[Fe(CN)_6]/K_4[Fe(CN)_6]$, ммоль/л | Диапазон АОА, мкмоль- экв/л | S_r , % | Источ- ник |
|--------------------------|-----------------------|--|--------------------------------------|--------------|---------------|
| Индикаторный электрод | Электрод сравнения | | | | |
| Pt/АК | H92SG | 5 / 0 | 20–4000 | \leq 13 | [62] |
| AuHЧ/С/СТ | O/Ag/СТ | 1 / 0,05 | 30–900* | \leq 20 | [53] |
| УВ/ПЭТ | O/Ag/ПЭТ | 1 / 0,05 | 15–990* | \leq 7 | [57] |

Примечание: ПСС – потенциометрическая сенсорная система; Pt/АК – коммерческий платиновый печатный электрод на основе алюмооксидной керамики; AuHЧ/С/СТ – углеродный печатный электрод на основе стеклотекстолита, модифицированный наночастицами золота; УВ/ПЭТ – электрод из углеродной вуали на основе полиэтилентерефталата; H92SG – коммерческий электрод для электрокардиографии; O/Ag/СТ – серебряный печатный электрод на основе стеклотекстолита, модифицированный смешанным осадком AgCl и $Ag_3[Fe(CN)_6]$; O/Ag/ПЭТ – серебряный печатный электрод на основе полиэтилентерефталата, модифицированный смешанным осадком AgCl и $Ag_3[Fe(CN)_6]$; S_r – относительной стандартное отклонение повторяемости результатов. Звездочкой (*) отмечены диапазоны определяемых значений АОА кожи человека, которые могут быть расширены в результате изменения концентрации медиатора.

3.6. Анализ биологических жидкостей

ПСС на основе алюмооксидной керамики была апробирована в оценке АОА сыворотки крови, слюны и эякулята [48]. Результаты, полученные с ис-

пользованием ПСС и коммерческих электродов, имели одинаковую воспроизводимость и статистически незначимые различия. В предыдущей работе [41] сообщалось, что потенциометрически определяемые значения АОА сыворотки крови нормально распределены. Уровень АОА сыворотки крови в контрольной группе (1.42 ± 0.29 мМ-экв) был достоверно выше уровней АОА сыворотки крови в группах пациентов с сердечно-сосудистыми (1.09 ± 0.29 мМ-экв) и онкологическими (0.70 ± 0.21 мМ-экв) заболеваниями. Сообщалось также, что потенциометрически определяемая АОА сыворотки крови отрицательно коррелирует с индексом депрессии Бека: $r = -0.318$, $p < 0,01$ [40]. Таким образом, разработанные ПСС имеют большие перспективы в анализе биологических жидкостей с целью мониторинга окислительного стресса и связанных с ним заболеваний.

4. ЗАКЛЮЧЕНИЕ

В результате выполненных исследований разработаны ПСС для оценки АОА в сочетании с медиаторной системой $K_3[Fe(CN)_6]/K_4[Fe(CN)_6]$, которые вследствие низкой стоимости могут использоваться в качестве одноразовых средств измерений. Предложенные ПСС апробированы в оценке АОА различных объектов с применением традиционных и новых протоколов анализа. Традиционные процедуры анализа основаны на применении двухэлектродных ПСС в оценке АОА растворов, экстрактов и прочих жидких образцов. Новые процедуры анализа основаны на применении двухэлектродных ПСС в оценке АОА плодоовощной и кондитерской продукции без предварительной жидкостной экстракции, а также трехэлектродных ПСС в неинвазивной оценке АОА кожи человека. Полученные результаты характеризуются приемлемым относительным стандартным отклонением повторяемости, имеют высокие значения показателя правильности при ведении аскорбиновой кислоты, а также хорошо сопоставимы с результатами коммерческих электродов. Предложенные ПСС не требуют подготовки к выполнению измерений, а в сочетании с портативным измерительным устройством могут эксплуатироваться персоналом любой квалификации за пределами аналитической лаборатории. В перспективе, полученные результаты могут способствовать внедрению потенциометрического метода определения АОА в промышленную и медицинскую практику.

Список источников

1. Sies H. On the history of oxidative stress: Concept and some aspects of current development // *Current Opinion in Toxicology*. – 2018. – Vol. 7. – P. 122-126. – DOI 10.1016/j.cotox.2018.01.002.
2. Jomova K., Raptova R., Alomar S. Y., Alwasel S. H., Nepovimova E., Kuca K., Valko M. Reactive oxygen species, toxicity, oxidative stress, and antioxidants: chronic diseases and aging // *Archives of Toxicology*. – 2023. – Vol. 97. – P. 2499-

2574. – DOI 10.1007/s00204-023-03562-9.

3. Sharifi-Rad M., Anil Kumar N. V., Zucca P., Varoni E. M., Dini L., Panzarini E., Rajkovic J., Tsouh Fokou P. V., Azzini E., Peluso I., Prakash Mishra A., Nigam M., El Rayess Y., Beyrouthy M. E., Polito L., Iriti M., Martins N., Martorell M., Docea A. O., Setzer W. N., Calina D., Cho W. C., Sharifi-Rad J. Lifestyle, Oxidative Stress, and Antioxidants: Back and Forth in the Pathophysiology of Chronic Diseases // *Frontiers in Physiology*. – 2020. – Vol. 11. – Art. 694. – DOI 10.3389/fphys.2020.00694.

4. Ivanov A. V., Bartosch B., Isaguliants M. G. Oxidative Stress in Infection and Consequent Disease // *Oxidative Medicine and Cellular Longevity*. – 2017. – Vol. 2017. – Art. 3496043. – DOI 10.1155/2017/3496043.

5. Hybertson B. M., Gao B., Bose S. K., McCord J. M. Oxidative stress in health and disease: The therapeutic potential of Nrf2 activation // *Molecular Aspects of Medicine*. – 2011. – Vol. 32, No. 4-6. – P. 234-246. – DOI 10.1016/j.mam.2011.10.006.

6. Neha K., Haider M. R., Pathak A., Yar M. S. Medicinal prospects of antioxidants: A review // *European Journal of Medicinal Chemistry*. – 2019. – Vol. 178. – P. 687-704. – DOI 10.1016/j.ejmech.2019.06.010.

7. *Antioxidants* / Ed. E. Shalaby. – London: IntechOpen, 2019. – 418 p. – DOI 10.5772/intechopen.77838.

8. База данных PubMed [Электронный ресурс]. – Режим доступа: URL: <https://pubmed.ncbi.nlm.nih.gov/>. (15.11.2024).

9. Brainina K., Stozhko N., Vidrevich M. Antioxidants: Terminology, Methods, and Future Considerations // *Antioxidants*. – 2019. – Vol. 8, No. 8. – Art. 297. – DOI 10.3390/antiox8080297.

10. Olszowy-Tomczyk M. Synergistic, antagonistic and additive antioxidant effects in the binary mixtures // *Phytochemistry Reviews*. – 2020. – Vol. 19. – P. 63-103. – DOI 10.1007/s11101-019-09658-4.

11. Cianciosi D., Forbes-Hernández T.Y., Regolo L., Alvarez-Suarez J.M., Navarro-Hortal M.D., Xiao J., Quiles J.L., Battino M., Giampieri F. The reciprocal interaction between polyphenols and other dietary compounds: Impact on bioavailability, antioxidant capacity and other physico-chemical and nutritional parameters // *Food Chemistry*. – 2022. – Vol. 375. – P. 131904. – DOI 10.1016/j.foodchem.2021.131904.

12. Fedenko V.S., Landi M., Shemet S.A. Metallophenomics: A Novel Integrated Approach to Study Complexation of Plant Phenolics with Metal/Metalloid Ions // *International Journal of Molecular Sciences*. – 2022. – Vol. 23, No. 19. – P. 11370. – DOI 10.3390/ijms231911370.

13. Apak R., Özyürek M., Güçlü K., Çapanoğlu E. Antioxidant Activity/Capacity Measurement. 1. Classification, Physicochemical Principles, Mechanisms, and Electron Transfer (ET)-Based Assays // *Journal of Agricultural and Food Chemistry*. – 2016. – Vol. 64, No. 5. – P. 997-1027. – DOI 10.1021/acs.jafc.5b04739.

14. Apak R., Özyürek M., Güçlü K., Çapanoğlu E. Antioxidant Activi-

ty/Capacity Measurement. 2. Hydrogen Atom Transfer (HAT)-Based, Mixed-Mode (Electron Transfer (ET)/HAT), and Lipid Peroxidation Assays // *Journal of Agricultural and Food Chemistry*. – 2016. – Vol. 64, No. 5. – P. 1028-1045. – DOI 10.1021/acs.jafc.5b04743.

15. Apak R., Özyürek M., Güçlü K., Çapanoğlu E. Antioxidant Activity/Capacity Measurement. 3. Reactive Oxygen and Nitrogen Species (ROS/RNS) Scavenging Assays, Oxidative Stress Biomarkers, and Chromatographic/Chemometric Assays // *Journal of Agricultural and Food Chemistry*. – 2016. – Vol. 64, No. 5. – P. 1046-1070. – DOI 10.1021/acs.jafc.5b04744.

16. Gulcin İ., Alwasel S. H. Metal Ions, Metal Chelators and Metal Chelating Assay as Antioxidant Method // *Processes*. – 2022. – Vol. 10, No. 1. – Art. 132. – DOI 10.3390/pr10010132.

17. Pisoschi A. M., Cimpeanu C., Predoi G. Electrochemical Methods for Total Antioxidant Capacity and its Main Contributors Determination: A review // *Open Chemistry*. – 2015. – Vol. 13, No. 1. – P. 824-856. – DOI 10.1515/chem-2015-0099.

18. Haque M. A., Morozova K., Ferrentino G., Scampicchio M. Electrochemical Methods to Evaluate the Antioxidant Activity and Capacity of Foods: A Review // *Electroanalysis*. – 2021. – Vol. 33, No. 6. – P. 1419-1435. – DOI 10.1002/elan.202060600.

19. Apak R., Gorinstein S., Böhm V., Schaich K. M., Özyürek M., Güçlü K. Methods of measurement and evaluation of natural antioxidant capacity/activity (IUPAC Technical Report) // *Pure and Applied Chemistry*. – 2013. – Vol. 85, No. 5. – P. 957-998. – DOI 10.1351/PAC-REP-12-07-15.

20. Патент РФ 2235998. Способ определения оксидантной/антиоксидантной активности растворов / Х. З. Брайнина, А. В. Иванова. Опубл. 10.09.2004, бюл. № 25.

21. Albuquerque B. R., Heleno S. A., Oliveira M. B. P. P., Barros L., Ferreira I. C. F. R. Phenolic compounds: current industrial applications, limitations and future challenges // *Food & Function*. – 2021. – Vol. 12, No. 1. – P. 14-29. – DOI 10.1039/D0FO02324H.

22. *Nutritional Antioxidant Therapies: Treatments and Perspectives* / Ed. K. H. Al-Gubory, I. Laher. – Cham: Springer International Publishing AG, 2017. – 553 p. – DOI 10.1007/978-3-319-67625-8.

23. Ho E., Galougahi K. K., Liu C.-C., Bhindi R., Figtree G. A. Biological markers of oxidative stress: Applications to cardiovascular research and practice // *Redox Biology*. – 2013. – Vol. 1, No. 1. – P. 483-491. – DOI 10.1016/j.redox.2013.07.006.

24. Peluso I., Raguzzini A. Salivary and Urinary Total Antioxidant Capacity as Biomarkers of Oxidative Stress in Humans // *Pathology Research International*. – 2016. – Vol. 2016. – Art. 5480267. – DOI 10.1155/2016/5480267.

25. Rahman I., Biswas S. K. Non-invasive biomarkers of oxidative stress: reproducibility and methodological issues // *Redox Report*. – 2004. – Vol. 9, No. 3. – P. 125-143. – DOI 10.1179/135100004225005219.

26. Pahune P. P., Choudhari A. R., Muley P. A. The Total Antioxidant Power of Semen and Its Correlation with the Fertility Potential of Human Male Subjects // *Journal of Clinical and Diagnostic Research*. – 2013. – Vol. 7, No. 6. – P. 991-995. – DOI 10.7860/JCDR/2013/4974.3040

27. Kumar S., Pandey A. K. Chemistry and Biological Activities of Flavonoids: An Overview // *The Scientific World Journal*. – 2013. – Vol. 2013. – Art. 162750 – DOI 10.1155/2013/162750.

28. Патент РФ 2433405. Способ неинвазивного потенциометрического определения оксидант/антиоксидантной активности биологических тканей и устройство для его осуществления / Х.З. Брайнина, Е.Л. Герасимова, М.Я. Ходос. Опубл. 10.11.2011, бюл. № 31.

29. Shpigun L. K., Arharova M. A., Brainina K. Z., Ivanova A. V. Flow injection potentiometric determination of total antioxidant activity of plant extracts // *Analytica Chimica Acta*. – 2006. – Vol. 573-574. – P. 419-426. – DOI 10.1016/j.aca.2006.03.094.

30. Ivanova A. V., Gerasimova E. L., Gazizullina E. R. An integrated approach to the investigation of antioxidant properties by potentiometry // *Analytica Chimica Acta*. – 2020. – Vol. 1111. – P. 83-91. – DOI 10.1016/j.aca.2020.03.041.

31. Ivanova A. V., Gerasimova E. L., Brainina Kh. Z. Potentiometric Study of Antioxidant Activity: Development and Prospects // *Critical Reviews in Analytical Chemistry*. – 2015. – Vol. 45, No. 4. – P. 311-322. – DOI 10.1080/10408347.2014.910443.

32. Brainina Kh. Z., Ivanova A. V., Sharafutdinova E. N., Lozovskaya E. L., Shkarina E. I. Potentiometry as a method of antioxidant activity investigation // *Talanta*. – 2007. – Vol. 71, No. 1. – P. 13-18. – DOI 10.1016/j.talanta.2006.03.018.

33. Шарафутдинова Е. Н., Инжеватова О. В., Тоболкина Н. В., Иванова А. В., Брайнина Х. З. Потенциометрический метод определения антиоксидантной активности: Оценка основных метрологических характеристик // *Заводская лаборатория. Диагностика материалов*. – 2008. – Т. 74, № 6. – С. 9-14.

34. Иванова А. В., Герасимова Е. Л., Газизуллина Е. Р., Тимина Д. С., Герасимова Н. Л., Собина А. В., Шалыгина Ж. В., Крашенинина М. П. Определение антиоксидантной емкости объектов фармации потенциометрическим методом. Показатели точности измерений // *Журнал аналитической химии*. – 2020. – Т. 75, № 3. – С. 259-265. – DOI 10.31857/S004445022003007X.

35. Brainina Kh. Z., Tarasov A. V., Kazakov Ya. E., Vidrevich M. B. Platinum electrode regeneration and quality control method for chronopotentiometric and chronoamperometric determination of antioxidant activity of biological fluids // *Journal of Electroanalytical Chemistry*. – 2018. – Vol. 808. – P. 14-20. – DOI 10.1016/j.jelechem.2017.11.065.

36. Тарасов А. В., Заворохина Н. В., Чугунова О. В. Исследование потенциально мешающих веществ при потенциометрическом определении антиоксидантной активности в пищевых системах // *Техника и технология пищевых производств*. – 2023. – Т. 53, № 3. – С. 504-512. – DOI 10.21603/2074-9414-2023-

3-2452.

37. Zavorokhina N. V., Mysakov D. S., Bochkova A. G. Development of Adaptogenic Beverages from Arctic Raw Materials for the Far North Residents // *Food Industry*. – 2022. – Vol. 7, No. 3. – P. 41-49. – DOI 10.29141/2500-1922-2022-7-3-5EDNWGYDTN.

38. Brainina Kh. Z., Gerasimova E. L., Varzakova D. P., Kazakov Ya. E., Galperin L. G. Noninvasive Method of Determining Skin Antioxidant/Oxidant Activity: Clinical and Cosmetics Applications // *Analytical and Bioanalytical Electrochemistry*. – 2013. – Vol. 5, No. 5. – P. 528-542.

39. Бляхман Ф. А., Брайнина А. З., Варзакова Д. П., Герасимова Е. Л., Крохолов В. Я., Телешев В. А., Шкляр Т. Ф. Антиоксидантный статус и системная гемодинамика у лиц молодого возраста // *Вестник Уральской медицинской академической науки*. – 2012. – № 3(40). – С. 59-61.

40. Lee G.-J., Lee S.-K., Kim J.-M., Rhee C. K., Lee Y.-K., Brainina Kh. Z., Kazakov Ya. E. Application Feasibility of Antioxidant Activity Evaluation Using Potentiometry in Major Depressive Disorder // *Electrochemistry*. – 2014. – Vol. 82, No. 4. – P. 264-266. – DOI 10.5796/electrochemistry.82.264.

41. Kazakov Ya., Tarasov A., Alyoshina L., Brainina Kh. Interplay between antioxidant activity, health and disease // *Biointerface Research in Applied Chemistry*. – 2019. – Vol. 10, No. 1. – P. 4893-4901. – DOI 10.33263/BRIAC101.893901.

42. Gao W., Baker T. A., Zhou L., Pinnaduwege D. S., Kaxiras E., Friend C. M. Chlorine Adsorption on Au(111): Chlorine Overlayer or Surface Chloride? // *Journal of the American Chemical Society*. – 2008. – Vol. 130, No. 11. – P. 3560–3565. – DOI 10.1021/ja077989a.

43. Yaguchi M., Uchida T., Motobayashi K., Osawa M. Speciation of Adsorbed Phosphate at Gold Electrodes: A Combined Surface-Enhanced Infrared Absorption Spectroscopy and DFT Study // *The Journal of Physical Chemistry Letters*. – 2016. – Vol. 7, No. 16. – P. 3097-3102. – DOI 10.1021/acs.jpcclett.6b01342.

44. Hua X., Xia H.-L., Long Y.-T. Revisiting a classical redox process on a gold electrode by operando ToF-SIMS: where does the gold go? // *Chemical Science*. – 2019. – Vol. 10, No. 24. – P. 6215-6219. – DOI 10.1039/C9SC00956F.

45. *Handbook of Electrochemistry* / Ed. C. G. Zoski. – Amsterdam: Elsevier Science, 2007. – 934 p. – DOI 10.1016/B978-0-444-51958-0.X5000-9.

46. ГОСТ 8.663–2018. Электроды сравнения для электрохимических измерений. Методика поверки. – М.: Стандартинформ, 2018. – 16 с.

47. *Handbook of Reference Electrodes* / Ed. G. Inzelt, A. Lewenstam, F. Scholz. – Berlin, Heidelberg: Springer-Verlag, 2013. – 344 p. – DOI 10.1007/978-3-642-36188-3.

48. Brainina K.Z., Tarasov A.V., Vidrevich M.B. Silver Chloride/Ferricyanide-Based Quasi-Reference Electrode for Potentiometric Sensing Applications // *Chemosensors*. – 2020. – Vol. 8, No. 1. – Art. 15. – DOI 10.3390/chemosensors8010015.

49. Tarasov A., Zavorokhina N., Stozhko N. Application of the desirability

function for multivariate stability assessment of quasi-reference electrodes // AIP Conference Proceedings. – 2023. – Vol. 2812, No. 1. – P. 020093. – DOI 10.1063/5.0161312.

50. Тарасов А. В., Чугунова О. В., Стожко Н. Ю. Потенциометрическая сенсорная система на основе модифицированных толстопленочных электродов для определения антиоксидантной активности напитков // Индустрия питания. – 2020. – Т. 5, № 3. – С. 85-96. – DOI 10.29141/2500-1922-2020-5-3-10.

51. Brainina K., Tarasov A., Khamzina E., Stozhko N., Vidrevich M. Contact hybrid potentiometric method for on-site and in situ estimation of the antioxidant activity of fruits and vegetables // Food Chemistry. – 2020. – Vol. 309. – Art. 125703. – DOI 10.1016/j.foodchem.2019.125703.

52. Tarasov A. V., Zavorokhina N. V. Modeling Functional Whey Drinks with High Antioxidant Activity Using Potentiometric Sensor Systems // Food Industry. – 2023. – Vol. 8, No. 2. – P. 21-30. – DOI 10.29141/2500-1922-2023-8-2-3.

53. Brainina K., Tarasov A., Khamzina E., Kazakov Y., Stozhko N. Disposable Potentiometric Sensory System for Skin Antioxidant Activity Evaluation // Sensors. – 2019. – Vol. 19, No. 11. – Art. 2586. – DOI 10.3390/s19112586.

54. Тарасов А. В., Заворохина Н. В., Чугунова О. В. Экспресс-метод измерения антиоксидантной активности в напитках с использованием потенциометрической сенсорной системы // Пищевая промышленность. – 2023. – № 8. – С. 57-60. – DOI 10.52653/PPI.2023.8.8.010.

55. Tarasov A., Stozhko N., Bukharinova M. Potentiometric sensor system based on modified screen-printed electrodes for determining antioxidant activity // BIO Web of Conferences. – 2023. – Vol. 76. – P. 05004. – DOI 10.1051/bioconf/20237605004.

56. Тарасов А. В., Заворохина Н. В. Экспресс-определение антиоксидантной активности кондитерских изделий с использованием одноразовой потенциометрической сенсорной системы // Вестник Южно-Уральского государственного университета. Серия: Пищевые и биотехнологии. – 2023. – Т. 11, № 2. – С. 93-102. – DOI 10.14529/food230211.

57. Tarasov A. V., Khamzina E. I., Bukharinova M. A., Stozhko N. Y. Flexible Potentiometric Sensor System for Non-Invasive Determination of Antioxidant Activity of Human Skin: Application for Evaluating the Effectiveness of Phytocosmetic Products // Chemosensors. – 2021. – Vol. 9, No. 4. – P. 76. – DOI 10.3390/chemosensors9040076.

58. Torrinha Á., Morais S. Electrochemical (bio)sensors based on carbon cloth and carbon paper: An overview // Trends in Analytical Chemistry. – 2021. – Vol. 142. – P. 116324. – DOI 10.1016/j.trac.2021.116324.

59. Medical Biosensors for Point of Care (POC) Applications / Ed. R. J. Narayan. – Cambridge: Woodhead Publishing, 2017. – 316 p. – DOI 10.1016/C2014-0-01459-1.

60. Золотов Ю. А., Иванов В. М., Амелин В. Г. Химические тест-методы анализа. – М.: Едиториал УРСС, 2002. – 304 с.

61. Selvamuthukumar M., Shi J. Recent advances in extraction of antioxidants from plant by-products processing industries // *Food Quality and Safety*. – 2017. – Vol. 1, No. 1. – P. 61-81. – DOI 10.1093/fqsafe/fyx004.

62. Brainina K. Z., Markina M. G., Stozhko N. Y. Optimized Potentiometric Assay for Non-invasive Investigation of Skin Antioxidant Activity // *Electroanalysis*. – 2018. – Vol. 30, No. 10. – P. 2405-2412. – DOI 10.1002/elan.201800309.

63. Zastrow L., Groth N., Klein F., Kockott D., Lademann J., Renneberg R., Ferrero L. The Missing Link – Light-Induced (280–1,600 nm) Free Radical Formation in Human Skin // *Skin Pharmacology and Physiology*. – 2009. – Vol. 22, No. 1. – P. 31-44. – DOI 10.1159/000188083.

64. Lohan S. B., Müller R., Albrecht S., Mink K., Tscherch K., Ismael F., Lademann J., Rohn S., Meinke M. C. Free radicals induced by sunlight in different spectral regions – in vivo versus ex vivo study // *Experimental Dermatology*. – 2016. – Vol. 25, No. 5. – P. 380-385. – DOI 10.1111/exd.12987.

65. Soeur J., Belaïdi J.-P., Chollet C., Denat L., Dimitrov A., Jones C., Perez P., Zanini M., Zobiri O., Mezzache S., Erdmann D., Lereaux G., Eilstein J., Marrot L. Photo-pollution stress in skin: Traces of pollutants (PAH and particulate matter) impair redox homeostasis in keratinocytes exposed to UVA1 // *Journal of Dermatological Science*. – 2017. – Vol. 86, No. 2. – P. 162-169. – DOI 10.1016/j.jdermsci.2017.01.007.

66. Ferrara F., Woodby B., Pecorelli A., Schiavone M. L., Pambianchi E., Messano N., Therrien J.-P., Choudhary H., Valacchi G. Additive effect of combined pollutants to UV induced skin OxInflammation damage. Evaluating the protective topical application of a cosmeceutical mixture formulation // *Redox Biology*. – 2020. – Vol. 34. – P. 101481. – DOI 10.1016/j.redox.2020.101481.

67. Paixão N., Perestrelo R., Marques J. C., Câmara J. S. Relationship between antioxidant capacity and total phenolic content of red, rosé and white wines // *Food Chemistry*. – 2007. – Vol. 105, No. 1. – P. 204-214. – DOI 10.1016/j.foodchem.2007.04.017.

68. Шарафутдинова Е. Н., Иванова А. В., Матерн А. И., Брайнина Х. З. Качество пищевых продуктов и антиоксидантная активность // *Аналитика и контроль*. – 2011. – Т. 15, № 3. – С. 281-286.

69. Nardini M., Garaguso I. Effect of Sulfites on Antioxidant Activity, Total Polyphenols, and Flavonoid Measurements in White Wine // *Foods*. – 2018. – Vol. 7, No. 3. – P. 35. – DOI 10.3390/foods7030035.

70. Baek J., Lee M.-G. Oxidative stress and antioxidant strategies in dermatology // *Redox Report*. – 2016. – Vol. 21, No. 4. – P. 164-169. – DOI 10.1179/1351000215Y.0000000015.

71. Anunciato T. P., da Rocha Filho P. A. Carotenoids and polyphenols in nutraceuticals, nutraceuticals, and cosmeceuticals // *Journal of Cosmetic Dermatology*. – 2012. – Vol. 11, No. 1. – P. 51-54. – DOI 10.1111/j.1473-2165.2011.00600.x.

72. Proksch E. pH in nature, humans and skin // *The Journal of Dermatology*. – 2018. – Vol. 45, No. 9. – P. 1044-1052. – DOI 10.1111/1346-8138.14489.

73. Heikenfeld J., Jajack A., Rogers J., Gutruf P., Tian L., Pan T., Li R., Khine M., Kim J., Wang J., Kim J. Wearable sensors: modalities, challenges, and prospects // *Lab on a Chip*. – 2018. – Vol. 18, No. 2. – P. 217-248. – DOI 10.1039/C7LC00914C.

74. Herbert R., Kim J.-H., Kim Y. S., Lee H. M., Yeo W.-H. Soft Material-Enabled, Flexible Hybrid Electronics for Medicine, Healthcare, and Human-Machine Interfaces // *Materials*. – 2018. – Vol. 11, No. 2. – P. 187. – DOI 10.3390/ma11020187.

75. Piro B., Mattana G., Noël V. Recent Advances in Skin Chemical Sensors // *Sensors*. – 2019. – Vol. 19, No. 20. – P. 4376. – DOI 10.3390/s19204376.

УДК 62

ГЛАВА 12. КИБЕРБЕЗОПАСНОСТЬ. ОСНОВНЫЕ ТЕНДЕНЦИИ ПРЕСТУПНОСТИ В СФЕРЕ КРИПТОВАЛЮТ

Аменицкий Алексей Владимирович

аспирант

Институт аспирантуры и докторантуры Университет Лобачевского Н.И.

Рухович Игорь Владимирович**Аменицкая Любовь Алексеевна****Аменицкий Дмитрий Александрович**

студенты

НИУ ВШЭ

Аннотация: Поскольку использование криптовалют в мировой финансовой системе продолжает расти, растет и их использование преступными группировками. Процветает финансовое мошенничество, связанное с использованием криптовалют, таких как bitcoin, ether или tether. Предполагаемые убытки, связанные с криптовалютой, составляют миллиарды долларов. В то время как количество жалоб, связанных с криптовалютой, составляет всего около 10% от общего числа жалоб на финансовое мошенничество, потери, связанные с этими жалобами, составляют почти 50% от общего числа потерь.

Преступные группы используют криптовалюты в каждой категории схем. Использование криптовалют было наиболее распространенным в инвестиционных аферах, где потери составили более 70 процентов от всех потерь, связанных с криптовалютой. Мошенничество с колл-центрами, включая мошенничество с технической поддержкой клиентов и мошенничество с выдачей себя за правительство, составило около 10% потерь, связанных с криптовалютой.

Децентрализованный характер криптовалюты, скорость необратимых транзакций и возможность перевода средств по всему миру делают криптовалюту привлекательным средством для преступников, в то же время создавая проблемы с возвратом украденных средств. Как только физическое лицо отправляет платеж, получатель становится владельцем криптовалюты и часто быстро переводит ее на счет за границей для обналичивания. Быстрое и точное представление жалоб является ключом к оказанию помощи правоохранительным органам в расследовании мошеннических схем, использующих криптовалюты.

Криптопреступления анализируются и систематизируются для выявления тенденций и разработки стратегий борьбы с этими схемами и защиты жертв мошенничества от убытков.

Целью этой главы является привлечение внимания к увеличению потерь, связанных с мошенничеством, связанным с криптовалютами, повышению осведомленности о наиболее распространенных схемах, использующих криптовалюты, и обучения способам защиты от такого рода мошенничества.

Ключевые слова: Cyber Security (CS), CS architecture, CS trends, CS tendencies, CS tools, CS crimes, CS latest news, CS releases, CS game-changers, CS future, CS playbook, CS agenda, CS future, CS risks, CS incidents, CS resilience, Hackers, PenTest, CS прогноз, Artificial Intelli-

gence, Deep Fakes, OWASP, Website security, CryptoScam, Antifraud, Эволюция киберУгроз, КиберГигиена.

CYBERSECURITY. THE MAIN TRENDS IN CRIME IN THE FIELD OF CRYPTOCURRENCIES

**Amenitsky Alexey Vladimirovich,
Rukhovich Igor Vladimirovich,
Amenitskaya Lyubov Alekseevna,
Amenitsky Dmitry Alexandrovich**

Криптовалютные преступления стали более изощрёнными и разнообразными, что требует от пользователей повышенного внимания и знаний в области безопасности. В главе рассматриваются основные виды мошенничества, такие как SMS-фишинг (смишинг), мошенничество с первичным предложением монет (ICO-Initial coin offering), схемы манипулирования рынком (Pump and Dump), а также угрозы, связанные с использованием искусственного интеллекта.

Мир криптовалют столкнулся с новыми тенденциями в сфере криптопреступности, которые становятся всё более изощрёнными и сложными для выявления. Новички, которые только начали знакомиться с цифровыми валютами, часто становятся жертвами мошенников. Понимание основных тенденций в сфере криптопреступности и знание методов профилактики помогут минимизировать риски и защитить средства. В этой главе рассмотрены основные виды криптопреступлений, методы защиты и рекомендации экспертов.

Типы криптопреступлений.

Криптопреступления охватывают широкий спектр незаконной деятельности - от кражи личных данных до манипулирования рынком. Объём незаконных средств, поступающих в централизованные сервисы, в 2025 году превысит 10 миллиардов долларов.

С быстрым ростом числа пользователей криптовалют и внедрением новых технологий преступники адаптируются и создают сложные схемы.

Эта глава основана на реалиях, с которыми сталкивается среднестатистический пользователь, столкнувшийся с типичным криптовалютным мошенником, использующим криптовалюту для инвестиций. К основным видам криптовалютных преступлений в контексте инвестиций в криптовалюту относятся:

- Фишинг: мошенничество с использованием SMS;
- Первичное размещение монет (ICO) и мошенничество с токенами;
- Pump & Dump- Накачка и сброс: манипулирование ценами на активы;
- Угрозы искусственного интеллекта: использование искусственного интеллекта для создания мошеннических схем.

Смишинг — это разновидность фишинга, при которой мошенники используют SMS для обмана пользователей. Смишинг часто начинается с получения

SMS-сообщения со ссылкой на поддельный веб-сайт, имитирующий известную организацию или сервис, например криптовалютную биржу или кошелёк. Мошенники маскируют свои сообщения, чтобы они выглядели легитимными, часто используя официальные логотипы и формулировки, вызывающие доверие. Пользователь, получивший такое сообщение, может перейти по ссылке и попасть на сайт, где его попросят ввести личную информацию, например имя пользователя и пароль, закрытые ключи или другую конфиденциальную информацию. Как только пользователь вводит эту информацию, она сразу же попадает в руки злоумышленников.

Первичное размещение монет (ICO)

Первичное размещение монет (ICO) помогает стартапам привлекать капитал путём продажи токенов. Этот процесс состоит из четырёх этапов:

- Создание проекта;
- Публикация белой книги;
- Сбор средств;
- Запуск и реализация проекта.

Однако отсутствие регулирования и надзора со стороны государственных органов привело к большому количеству мошеннических ICO. Эти мошенничества принимают форму:

- Пустые обещания: разработчики обещают революционные технологии и огромную прибыль, но на самом деле не имеют ни технических возможностей, ни желания реализовывать проект.

- Фальшивые команды: мошенники создают фальшивые профили команд проектов, используя фотографии и биографии известных людей или даже вымышленных персонажей.

- Схемы «собери деньги и беги»: разработчики собирают средства и исчезают, не выполняя никаких обязательств перед инвесторами.

- Pumping, Dumping, Hacking and Spinning.

Эта схема предполагает искусственное повышение цены актива, а затем его массовую продажу по завышенной цене. Мошенники организуют массовую скупку активов, создавая иллюзию роста цен, а затем продают их по максимальной цене, оставляя остальных участников с обесценившимися активами.

Этапы схемы накачки и сброса:

- Организация группы: мошенники объединяются в группы, часто используя мессенджеры, форумы и социальные сети для координации своих действий. В таких группах могут быть тысячи участников.

- Выбор цели: выбирается криптовалюта с низкой ликвидностью и небольшой рыночной капитализацией, поскольку такими активами легче манипулировать. Мошенники распространяют слухи и фейковые новости о перспективах этого актива.

- **Запуск пампинга:** участники схемы массово скупают выбранный актив, что приводит к резкому росту его цены. В этот момент в социальных сетях и на форумах начинают появляться сообщения о якобы блестящем будущем этого актива, что привлекает внимание ничего не подозревающих инвесторов.
- **Привлечение сторонних инвесторов:** введение общественности в заблуждение заставляет новых инвесторов покупать актив, что ещё больше повышает его стоимость. Это создаёт иллюзию растущего спроса и усиливает ажиотаж вокруг актива.
- **Слив:** когда цена актива достигает заранее установленного уровня, организаторы схемы начинают массово продавать свои активы. Это приводит к падению цены, поскольку рынок становится перенасыщенным.
- **Обвал цен:** стоимость активов резко падает, оставляя последних покупателей с бесполезными активами. Мошенники тем временем уже вывели свою прибыль, оставив остальных участников схемы с убытками.

Угрозы искусственного интеллекта

Искусственный интеллект используется для создания сложных мошеннических схем, в том числе для автоматизированных взломов и фишинговых атак, которые трудно отличить от законных действий. В 2024 году использование ИИ в сфере киберпреступности достигло нового уровня, что усложняет его обнаружение и предотвращение. Ниже перечислены основные области, в которых ИИ используется в преступных целях:

- **Социальная инженерия:** преступники используют ИИ для анализа поведения пользователей в интернете, чтобы прогнозировать их реакции и использовать эту информацию для совершения мошенничества. ИИ создаёт поддельные профили в социальных сетях, которые взаимодействуют с жертвами, выстраивая доверительные отношения перед совершением мошенничества.
- **Мошеннические боты:** преступники разрабатывают торговых ботов, которые используют искусственный интеллект для автоматической торговли криптовалютой. Эти боты манипулируют рынком, создавая иллюзию спроса или предложения, и в конечном итоге обманывают пользователей.
- **Технологии дипфейков:** с помощью технологий дипфейков преступники могут создавать поддельные видео- и аудиозаписи, имитирующие известных людей или руководителей компаний. Такие материалы могут использоваться для мошенничества или шантажа.

Чтобы защитить себя от киберпреступлений, важно следовать ряду рекомендаций:

- **Проверка источников информации:** каждый раз, когда вы переходите по ссылке, проверяйте оригинальность сайтов и сервисов, связанных с криптовалютами.

- Использование многофакторной аутентификации: это усложняет задачу хакерам.
- Обновление программного обеспечения: Своевременное обновление программного обеспечения снижает риск уязвимостей.
- Образование и осведомлённость: регулярно изучайте новые методы мошенничества и способы защиты.

Эксперты по кибербезопасности рекомендуют не только использовать технические средства защиты, но и активно сотрудничать с регулирующими органами и платформами. Важно сообщать о подозрительных действиях и участвовать в образовательных инициативах для повышения криптовалютной грамотности. Я также подчёркиваю необходимость обращаться в специализированные организации, такие как AML Crypto, для проверки подозрительных транзакций и соблюдения нормативных требований. Кроме того, важно записывать и документировать все свои действия, связанные с криптовалютой, чтобы обеспечить прозрачность и отслеживаемость в случае споров или расследований. Это включает в себя ведение записей о транзакциях, использовании кошелька и взаимодействии с различными платформами, а также составление отчёта о криптоинциденте.

В целях предотвращения преступлений в сфере криптовалют необходимо применять комплексный подход: технологические меры, информирование и сотрудничество с регулирующими органами. Регулярно проверяйте адреса кошельков и пользуйтесь надёжными сервисами.

К безопасным методам относятся использование аппаратных кошельков, мультиподписей и холодного хранения. Не храните крупные суммы на онлайн-платформах или в горячих кошельках, поскольку в тот момент, когда средства хранятся на централизованном сервисе, они не принадлежат пользователю.

Если вы стали жертвой криптомошенничества, первым делом необходимо немедленно прекратить дальнейшие транзакции или взаимодействие с подозрительными пользователями или платформами. Сообщите о происшествии в правоохранительные органы и специализированные агентства по борьбе с киберпреступностью, такие как AML Crypto, предоставив все возможные доказательства: скриншоты, электронные письма, записи о транзакциях и любые другие документы.

ПОЧЕМУ ПРЕСТУПНИКИ ИСПОЛЬЗУЮТ КРИПТОВАЛЮТУ

Децентрализованный характер: криптовалюта децентрализована и распределена, что может обеспечить безопасный способ перевода средств. Современный рынок включает тысячи криптовалют, которые пользователи могут переводить по всему миру в обмен на товары, услуги и другие криптовалюты. Поскольку криптовалюты устраняют необходимость в финансовых посредниках для подтверждения и облегчения транзакций, преступники могут использовать эти характеристики для поддержки незаконной деятельности, такой как кражи, мошенничество и отмывание денег.

Безотзывные транзакции, которые выполняются быстро: Перевод криптовалюты может осуществляться в любом месте. Единственными требованиями для перевода средств с определенного адреса являются соответствующий закрытый ключ (который функционирует как пароль или PIN-код) и подключение к Интернету. Третьи стороны не участвуют в транзакциях и не санкционируют их, а транзакции являются безотзывными, то есть их невозможно отменить. Преступные группировки, подключенные к Интернету из любой точки мира, также могут использовать эти характеристики для упрощения крупномасштабных, почти мгновенных трансграничных транзакций без участия традиционных финансовых посредников, которые используют программы по борьбе с отмыванием денег.

Проблемы, с которыми сталкиваются следующие фонды: Транзакции с использованием криптовалюты постоянно регистрируются в общедоступных распределенных реестрах, называемых блокчейнами. В результате правоохранительные органы могут отслеживать транзакции с криптовалютой, чтобы следить за деньгами способами, невозможными в других финансовых системах. Тем не менее, поскольку криптовалюта также позволяет переводить средства на биржи за рубежом, правоохранительные органы сталкиваются со значительными трудностями при использовании криптовалют, которые попадают в другие юрисдикции, особенно в тех, где действуют слабые законы или нормативные акты по борьбе с отмыванием денег.

Инвестиционное мошенничество

Инвестиционное мошенничество, как правило, включает в себя обманную практику привлечения инвестиций, основанную на ложной информации. Эти схемы предлагают частным лицам большие доходы при минимальном риске. На протяжении многих лет широкое распространение криптовалюты в качестве инвестиционного инструмента в сочетании с менталитетом, связанным со «страхом упустить что—то», привело к тому, что преступники получили возможность нападать на потребителей и розничных инвесторов, особенно на тех, кто стремится получить прибыль от инвестирования, но не знаком с технологией и сопутствующими рисками.

Мошенничество с криптовалютными инвестициями, основанное на доверии

Хотя существует множество разновидностей мошенничества с инвестициями, связанными с криптовалютами, наиболее заметным является уникальный вид мошенничества с инвестициями в криптовалюту, основанный на доверии. Эти схемы являются социально разработанными и основаны на доверии, при помощи которых преступники используют приложения для знакомств, платформы социальных сетей, профессиональные сетевые сайты или приложения для обмена зашифрованными сообщениями для установления отношений со своими целями. Как только доверие устанавливается, преступники начинают

обсуждать тему инвестиций в криптовалюту. Преступники утверждают, что обладают определенным опытом или знают эксперта, который может помочь потенциальным инвесторам достичь финансового успеха. Затем преступники убеждают своих жертв использовать мошеннические веб-сайты или приложения, контролируемые преступниками, для инвестирования в криптовалюту.

Преступники обучают своих жертв процессу инвестирования, демонстрируют им фиктивную прибыль и поощряют их инвестировать в криптовалюту. инвестируйте больше. Преступники могут разрешать жертвам выводить небольшие суммы на ранней стадии мошенничества, чтобы повысить доверие к мошенническим платформам. Тем не менее, когда жертвы пытаются полностью вывести свои инвестиции и любые предполагаемые доходы, им говорят, что они должны заплатить комиссию или налоги. Преступники никогда не возвращают основную часть средств, даже если их жертвы платят установленные сборы или налоги.

Люди, которые сообщают о потере денег в результате этих схем, иногда также становятся мишенью мошеннических компаний, которые утверждают, что помогают вернуть потерянные средства в криптовалюте.

Связь с торговлей людьми

Граждане и отдельные лица, которые путешествуют или живут за границей, должны знать о риске получения ложных объявлений о приеме на работу, связанных с торговлей рабочей силой, в мошеннических компаниях за рубежом. В этих компаниях работников удерживают против их воли и используют запугивание, чтобы заставить их участвовать в мошеннических операциях.

Преступники размещают ложные объявления о работе в социальных сетях и на сайтах онлайн-трудоустройства, ориентируясь на людей, в первую очередь в Азии. Эти схемы охватывают широкий спектр возможностей, включая техническую поддержку, обслуживание клиентов в колл-центрах и техников салонов красоты. Соискателям предлагаются конкурентоспособные условия- заработная плата, выгодные льготы, оплачиваемые командировочные расходы, а также проживание и питание. Часто на протяжении всего процесса работы местоположение вакансии меняется с объявленного местоположения.

Мошеннический комплекс - это операции по мошенничеству с недвижимостью, проводимые с использованием различных схем, в которых иногда также содержатся жертвы торговли людьми, которых принуждают к совершению мошеннических действий.

Мошенники могут завоевать доверие в течение нескольких недель и за несколько месяцев до того, как они попытаются убедить вас инвестировать в криптовалюту. Они будут использовать текстовые сообщения, видеочаты, телефонные звонки и электронные письма, чтобы заманить вас.

Но есть одна вещь, которую эти мошенники обычно не делают – они не будут встречаться с вами в реальной жизни. Если предложение об инвестировании исходит от человека, с которым вы никогда не встречались лично – вы

никогда не пили с ним кофе, никогда не гуляли вместе в парке, никогда не ходили вместе в кино, – отнеситесь к этому совету крайне осторожно. Вам по-прежнему следует тщательно оценивать все инвестиционные рекомендации, но быть особенно внимательными с осторожностью относитесь к советам, исходящим от “друга”, с которым вы никогда не встречались лично.

В другой стране преступники могут конфисковать паспорт и проездные документы соискателя работы и угрожать или применять насилие, чтобы принудить его к сотрудничеству. Работникам часто говорят, что они должны оплатить проезд и другие расходы, а это означает, что сначала они остаются в долгах. Затем они должны отработать долг, одновременно пытаясь оплатить проживание и питание. Преступники используют растущий долг работника и страх перед местными правоохранительными органами в качестве дополнительных средств для того, чтобы контролировать их. Работников, ставших жертвами торговли людьми, иногда продают и переводят из одного предприятия в другое, что еще больше увеличивает их долги.

Советы по самозащите, связанные с потенциальной торговлей людьми.

- Изучите рекламируемую компанию, прежде чем принимать предложение о работе. Остерегайтесь расплывчатых формулировок о компании или ограниченных сведений о трудоустройстве.

- Остерегайтесь объявлений о приеме на работу с необычно высокой зарплатой и множеством льгот.

- Если вы планируете переехать в другую страну в поисках новой работы, сообщите семье и друзьям подробности о трудоустройстве, указав контактную информацию из объявления о приеме на работу.

- Перед переездом запланируйте регулярные встречи с семьей и друзьями, чтобы убедиться в их безопасности и благополучии.

- Зарегистрируйтесь в программе регистрации Smart Traveler (STEP) по адресу step.state.gov чтобы получать рекомендации по безопасности в стране назначения. Посольство или консульства могут связаться с вами в случае возникновения чрезвычайной ситуации.

- Если вы являетесь потенциальной жертвой торговли людьми, обратитесь в ближайшее посольство.

Разновидности мошенничества с инвестициями в криптовалюту

Схемы майнинга ликвидности.

Добыча ликвидности - это инвестиционная стратегия, используемая для получения пассивного дохода с помощью криптовалюты. При законных операциях по добыче ликвидности инвесторы размещают свою криптовалюту в пуле ликвидности, чтобы обеспечить трейдеров ликвидностью, необходимой для проведения транзакций. Взамен инвесторы получают часть комиссионных за торговлю.

В этой разновидности мошенничества с инвестициями в криптовалюту мошенники используют владельцев криптовалюты, как правило, Tether (USDT)

и/или Ethereum (ETH). Мошенник создает профессиональную или личную систему взаимоотношений со своей целью в течение нескольких дней или недель дает инструкции по покупке, если у них еще нет криптовалюты, и привлекает их к участию в добыче ликвидности, гарантируя возврат инвестиций в размере от одного до трех процентов в день. Мошенники убеждают клиентов привязать свой криптовалютный кошелек к мошенническому приложению для майнинга ликвидности. Затем мошенники выводят средства без уведомления или разрешения владельца.

Мошенники могут называть инвестиционную возможность пулом ликвидности, майнингом ликвидности или майнинговым пулом для майнинга ликвидности. Для целей данного отчета термин "добыча ликвидности" будет использоваться для описания всех этапов работы схемы.

Термин, используемый для описания инвестирования в криптовалюту и получения вознаграждения за ее хранение в течение определенного периода.

"Криптовалютный кошелек" - это программное обеспечение для хранения криптовалюты и других виртуальных активов.

Рекомендации по защите от схем майнинга ликвидности.

- Помните, что инвесторы, участвующие в законных операциях по добыче ликвидности, вносят средства на платформу, а затем выводят первоначальные средства вместе с полученными доходами. Подумайте о вступлении в пулы, которые не соответствуют этой процедуре. В процессе законного майнинга ликвидности доходность обычно зависит от колебаний рынка конкретной криптовалюты или пары криптовалют, которые используются.

- Будьте бдительны, изучая инвестиционные возможности с помощью онлайн-исследований. Мошеннические веб-сайты или приложения обычно не рекламируются в Интернете, и поисковым системам, таким как Google и другим, не разрешается их индексировать. Проверьте правильность написания веб-адресов, веб-сайтов и адресов электронной почты, которые выглядят достоверно, но могут быть имитацией законных веб-сайтов.

- Если вы сомневаетесь в легитимности домена, не подключайте свой криптовалютный кошелек.

- Не отправляйте платеж тому, с кем вы общались только онлайн, даже если вы считаете, что установили с этим человеком отношения.

- Проверяйте подлинность всех ссылок, отправленных от известных и неизвестных контактов, прежде чем переходить по ним.

- Периодически используйте стороннюю программу проверки выдачи токенов, чтобы определить, не разрешили ли вы непреднамеренно каким-либо сайтам или приложениям доступ к вашему кошельку.

Мошеннические игровые приложения, предназначенные для получения прибыли

Преступники создают поддельные игровые приложения для кражи криптовалюты, которые они рекламируют как игры для заработка, предлагающие фи-

нансовые стимулы игрокам.

Преступники связываются с потенциальными жертвами онлайн и со временем устанавливают с ними отношения. Преступники затем вводят цели в онлайн- или мобильную игру, в которой игроки якобы получают вознаграждение в криптовалюте в обмен на какую-либо деятельность, например, выращивание “урожая” на анимированной ферме.

Чтобы принять участие в игре, преступники просят своих жертв создать криптовалютный кошелек, приобрести криптовалюту и присоединиться к определенному игровому приложению. Чем больше денег они хранят в своем кошельке, тем больше вознаграждений они предположительно получают в игре. Злоумышленники играют в игру и видят, как в приложении накапливаются фальшивые вознаграждения. Когда злоумышленники перестают вносить средства в кошелек, преступники выводят их используя вредоносную программу, которая была активирована при входе в игру. Хотя злоумышленники сообщают своим жертвам, что они могут вернуть средства, заплатив дополнительные налоги или сборы, они не могут вернуть свои деньги обратно, даже если они заплатят дополнительные сборы.

Рекомендации по защите от мошеннических игровых приложений с оплатой за заработок

- Если вы хотите участвовать в играх, связанных с криптовалютой, создайте уникальный кошелек для использования. Это изолирует ваши основные запасы криптовалюты, если вы по незнанию предоставите незаконным субъектам доступ к вашему игровому кошельку.

- Используйте сторонний блокчейн-обозреватель для независимой проверки балансов адресов в вашем игровом кошельке.

- Периодически используйте сторонний инструмент проверки резервирования токенов, чтобы узнать, каким сайтам или приложениям вы непреднамеренно разрешили доступ к средствам в вашем кошельке, и отозвать эти разрешения.

Криптовалютные киоски

Криптовалютные киоски - это устройства, похожие на банкоматы, или электронные терминалы, которые позволяют пользователям обменивать наличные и криптовалюту. Известно, что преступники заставляют людей использовать криптовалютный киоск для отправки средства, что обеспечивает более анонимную транзакцию, чем внесение наличных в финансовое учреждение.

Использование криптовалютных киосков для совершения мошеннических действий против населения растет. В 2023 году а убытки от использовании криптовалютных киосков превысили 189 миллионов долларов.

Как правило, преступники дают физическим лицам подробные инструкции, в том числе о том, как снять наличные в их банке, как найти киоск, а также как вносить и отправлять средства с помощью киоска. В большинстве случаев злоумышленники транзакции в криптовалютном киоске упрощаются с помо-

щью QR-кодов, квадратных штрих-кодов с информацией, которую можно отсканировать и прочитать с помощью смартфона или камеры в киоске. Пользователь может отсканировать QR-код предполагаемого получателя в криптовалютном киоске, что упрощает отправку криптовалюты иному адресату.

Схемы возврата средств в криптовалюте

Люди, которые сообщают о потере денег в результате различных схем, в частности мошенничества с инвестициями в криптовалюту, иногда также становятся жертвами мошеннических компаний, которые утверждают, что помогают вернуть потерянные средства в криптовалюте. В некоторых ситуациях это следующая итерация существующей схемы мошенничества. Представители этих мошеннических компаний утверждают, что обеспечивают отслеживание криптовалюты и обещают возможность вернуть потерянные средства. Они связываются с людьми, которые потеряли деньги, через социальные сети или платформы обмена сообщениями, или рекламируют свои мошеннические услуги по восстановлению криптовалюты в разделах комментариев к онлайн-новостным статьям и видеороликам о криптовалюте; среди результатов онлайн-поиска криптовалюты; или в социальных сетях.

Мошеннические компании, претендующие на возврат украденных средств, взимают предоплату и либо прекращают общение после получения первоначального взноса, либо представляют неполный или неточный отчет об отслеживании и требуют дополнительных сборов за возврат средств. Эти мошеннические компании могут заявлять о своей принадлежности к правоохранительным органам или юридическим службам, чтобы казаться законными.

Следует обратить внимание, что частные компании по взысканию не могут издавать юридические приказы о возврате или аресте украденной криптовалюты. Криптовалютные биржи замораживают счета только на основании внутренних процедур или в ответ на юридические документы, выданные судом. Физические лица, потерявшие деньги в результате мошенничества, могут обратиться в суд с гражданским иском о взыскании своих средств.

Рекомендации.

- Преступники будут стремиться создать ощущение срочности и изоляции.
- При получении нежелательного звонка от неизвестного абонента, утверждающего, что он работает в известной компании или государственном учреждении, повесьте трубку и самостоятельно изучите опубликованный в открытом доступе телефонный номер компании или агентства и позвоните по нему, чтобы подтвердить подлинность первоначального звонка.
- Ни один законный представитель правоохранительных органов или правительства не позвонит, чтобы потребовать оплату через криптовалютный киоск.
- Никогда не предоставляйте никому личную информацию, не подтвердив, что человек является тем, за кого себя выдает.
- Проверяйте достоверность любых инвестиционных предложений, которые незнакомые люди или давно потерянные контакты предлагают на сайтах

социальных сетей. Если вы никогда не встречались с человеком в реальной жизни, даже если вы общались по телефону или в видеочате, будьте очень осторожны, принимая советы или предложения по инвестированию.

- Следите за доменными именами или названиями веб-сайтов, которые выдают себя за законные финансовые учреждения, особенно за криптовалютные биржи.

- Мошеннические компании часто используют адреса веб-сайтов, которые имитируют реальные финансовые учреждения, но являются часто они немного отличаются, чтобы убедить людей в том, что мошеннический веб-сайт является законным.

- Не загружайте и не используйте подозрительные приложения в качестве инструмента инвестирования, если вы не можете подтвердить законность приложения.

- Если инвестиционная возможность кажется слишком привлекательной, чтобы быть правдой, скорее всего, так оно и есть. Будьте осторожны со схемами быстрого обогащения.

- Инвестирование сопряжено с риском. Физические лица должны инвестировать, исходя из своих финансовых целей и финансовых ресурсов, и, при возникновении каких-либо сомнений, должны обратиться за советом к лицензированному финансовому консультанту.

Популярные схемы мошеннических преступлений

Предварительная оплата: физическое лицо платит кому-либо деньги в ожидании получения чего-то более ценного взамен, но вместо этого получает значительно меньше ожидаемого или вообще ничего.

Компрометация деловой электронной почты (BEC): BEC - это мошенничество, направленное против компаний или частных лиц, работающих с поставщиками и/или предприятий, регулярно осуществляющих платежи банковским переводом. Эти изощренные мошеннические действия осуществляются преступниками путем компрометации учетных записей электронной почты и других средств коммуникации, таких как номера телефонов и приложения для виртуальных встреч, с помощью социальной инженерии или методов компьютерного вторжения для осуществления несанкционированного перевода средств.

Ботнет – это группа из двух или более компьютеров, контролируемых и обновляемых удаленно для незаконной покупки, такие как распределенный отказ в обслуживании или атака на отказ в обслуживании телефонной связи, или другие вредоносные действия.

Доверие/романтические отношения: человек считает, что у него есть отношения (семейные, дружеские или романтические), и его обманом заставляют отправлять деньги, личную и финансовую информацию или ценные предметы преступнику или отмывать деньги или предметы, помогающие преступнику. Это относится и к бабушке или дедушке, которые являются родственниками.

Схема и любой другой план, в рамках которого преступник наживается на

“сердечных чувствах” человека, ставшего мишенью.

Мошенничество с кредитными картами/чеками: Мошенничество с кредитными картами - это широкий термин, обозначающий кражу и мошенничество, совершаемые с использованием кредитной карты или любого аналогичного платежного механизма (АСН, EFT, периодических платежей и т.д.) в качестве мошеннического источника средств при проведении транзакции.

Преступления против детей: все, что связано с эксплуатацией детей, включая жестокое обращение с детьми.

Утечка данных: Утечка данных в киберпространстве - это использование компьютерного вмешательства для получения конфиденциальной или защищенной информации. Сюда не входят компьютерные вторжения, направленные против личных интересов принадлежащие им компьютеры, системы, устройства или личные аккаунты, такие как социальные сети или финансовые счета.

Трудоустройство: Человек считает, что он работает на законных основаниях, и теряет деньги или отмывает деньги/имущество в ходе своей трудовой деятельности.

Вымогательство: незаконное получение денег или имущества путем запугивания или злоупотребления властью. Это может включать угрозы физической расправы, уголовного преследования или публичного разоблачения.

Выдача себя за представителя власти: Для сбора денег выдается государственный служащий.

Домогательство/преследование: Повторяющиеся слова, поведение или действия, которые не преследуют законной цели и направлены против конкретного человека, чтобы вызвать у него раздражение, тревогу или огорчение. Совершение действий, направленных против конкретного человека, которые заставили бы разумного человека опасаться за свою безопасность или безопасность других людей или испытывать серьезные эмоциональные переживания.

Кража личных данных: кто-то неправомерно получает и использует личную информацию, позволяющую установить личность, каким-либо образом, связанным с мошенничеством или обманом, как правило, с целью получения экономической выгоды.

Инвестиции: Обманчивая практика, которая побуждает инвесторов совершать покупки, основываясь на ложной информации.

Эти мошенники обычно предлагают целевую крупную прибыль при минимальном риске. (Выход на пенсию, Финансовая пирамида, Пирамида и т.д.).

IPR/Copyright and Counterfeit: /авторское право и контрафакт: Незаконное хищение и использование чужих идей, изобретений и форм творческого самовыражения – того, что называется интеллектуальной собственностью, – всего, начиная от коммерческой тайны и запатентованных продуктов и комплектующих до фильмов, музыки и программного обеспечения.

Лотерея/тотализатор/Наследство: С физическим лицом связываются по поводу выигрыша в лотерею или тотализаторе они никогда не вводились, или для получения наследства от неизвестного родственника.

Вредоносное ПО: программное обеспечение или код, предназначенные для повреждения, выведения из строя или способные копироваться на компьютер и/или компьютерные системы с целью нанесения ущерба или уничтожения данных.

Неплатеж/недоставка: Товары или услуги отправлены, но оплата так и не произведена (неплатеж). Платеж отправлен, а товары или услуги так и не получены или имеют низкое качество (недоставка).

Переплата: Физическому лицу отправляется платеж/комиссия и дается указание сохранить часть суммы переплаты с последующей просьбой оплатить и отправить оставшуюся сумму другому физическому или юридическому лицу.

Утечка персональных данных: утечка персональных данных из безопасного места в ненадежную среду. Кроме того, это инцидент в области безопасности, при котором конфиденциальные, защищенные или конфиденциальнофункциональные данные физического лица копируются, передаются, просматриваются, крадутся или используются неуполномоченным лицом.

Фишинг/подмена: использование нежелательной электронной почты, текстовых сообщений и телефонных звонков якобы от законной компании с запросом личных, финансовых данных и/или учетных данных для входа в систему.

Программы-вымогатели: типы вредоносного программного обеспечения, предназначенного для блокирования доступа к компьютерной системе до тех пор, пока не будут выплачены деньги.

Недвижимость: Потеря средств в результате инвестиций в недвижимость или мошенничества, связанного с арендой или таймшером недвижимости.

Подмена SIM-карты: использование простых методов социальной инженерии против операторов мобильной связи для перевода телефонной связи жертвы на мобильное устройство, находящееся во владении преступника.

Техническая поддержка: субъект, выдающий себя за службу технической поддержки или обслуживания клиентов.

Угрозы насилием: выражение намерения причинить боль, увечья, членовредительство или смерть не в соответствии с контекстом вымогательства.

Кражи криптовалюты с помощью игр "Играй и зарабатывай"

Преступники выдают себя за разработчиков несменяемых токенов (NFT), чтобы нацелиться на интернет-пользователей, заинтересованных в приобретении NFT

Увеличение числа компаний, ложно заявляющих о своей способности вернуть средства, потерянные в результате мошенничества с инвестициями в криптовалюту

Мошеннические действия "Фантомных хакеров" нацелены на пожилых людей и приводят к тому, что жертвы теряют свои сбережения

Мошенники вымогают поддельные гуманитарные пожертвования

Мошенничество с праздничными покупками.

Мошенничество на NFT-платформах.

Можно наткнуться на NFT-мошенничество даже на самых популярных

NFT-платформах и что есть даже NFT-мошенники, которые готовы создавать целые фальшивые коллекции, чтобы обманывать наивных пользователей? Давайте разберёмся, как работают мошеннические коллекции и как не попасться на уловки мошенников.

NFT, или невзаимозаменяемые токены, — это уникальные цифровые активы, которые представляют собой право собственности на конкретный предмет, будь то цифровое искусство, видео, музыка или другие объекты. Каждый NFT уникален, то есть его нельзя заменить другим токеном того же типа, например биткоином или другими криптовалютами.

NFT также используются для создания и продажи виртуальной собственности, цифровых предметов коллекционирования, внутриигровых предметов и многого другого. Это делает NFT важным инструментом в виртуальной экономике, позволяя монетизировать цифровые активы. Однако, несмотря на эту инновационную технологию, популярность NFT привлекла множество злоумышленников, которые пытаются воспользоваться неосведомлённостью пользователей о безопасных методах работы с токенами.

Основная цель NFT — подтвердить подлинность и уникальность цифрового контента. Это открыло большие возможности для творческих людей, коллекционеров и инвесторов. NFT стали популярны среди художников, музыкантов и даже брендов, выпускающих цифровые товары ограниченным тиражом. Однако с резким ростом интереса к NFT увеличилось и количество связанных с ними мошеннических схем.

NFT создаются с помощью технологии блокчейн, чаще всего на платформе Ethereum, где каждый токен записывается в блокчейн и может быть отслежен. Это позволяет владельцам токенов подтверждать свое право собственности и подлинность актива. Блокчейн обеспечивает прозрачность всех транзакций и невозможность их изменения задним числом, что повышает доверие к системе. Технология блокчейн делает NFT практически неизменными и защищенными от подделок.

Помимо Ethereum, NFT можно создавать в других блокчейнах, таких как Binance Smart Chain, Solana и т. д. Эти блокчейны предлагают свои собственные функции и возможности для выпуска NFT и управления ими. Например, некоторые блокчейны могут предлагать более низкие комиссии за транзакции или более высокую скорость обработки данных, что делает их привлекательными для пользователей. Однако важно помнить, что у каждой платформы есть свои особенности, и пользователи должны знать о возможных рисках.

Каждый NFT содержит информацию о владельце, дате создания, оригинальном авторе и предыдущих владельцах. Эти данные хранятся в децентрализованной базе данных, что делает NFT безопасным способом подтверждения права собственности на цифровой актив. Однако, несмотря на использование технологии блокчейн, рынок NFT подвержен многочисленным мошенническим схемам.

NFT работают не только как цифровые активы, но и как подтверждение

права собственности на уникальный объект. Например, если вы покупаете NFT-токен произведения искусства, ваш токен подтверждает, что вы владеете оригинальным цифровым изображением, даже если его копии доступны в интернете. Это открывает двери на новый уровень цифрового владения, но также поднимает вопросы о безопасности и защите прав.

Популярность NFT в то время привлекла внимание не только инвесторов, но и мошенников. Они используют различные схемы, чтобы обманывать пользователей и красть их средства. Некоторые из них на первый взгляд кажутся вполне законными, но на самом деле могут привести к потере значительных сумм. Например, мошенники могут подделывать NFT, взламывать криптокошельки или создавать поддельные платформы для продажи активов. Важно понимать, что, несмотря на преимущества блокчейна, пользователи могут стать жертвами социальной инженерии или фишинговых атак.

С ростом числа NFT-проектов и платформ пользователи столкнулись с ситуациями, когда они не могут отличить законную платформу от мошеннической. Это связано с тем, что многие мошеннические проекты имитируют интерфейсы известных платформ, привлекают пользователей выгодными условиями, а затем исчезают, оставляя их без средств.

Самые распространённые виды мошенничества с NFT.

Поддельные платформы NFT

Одна из самых распространённых схем — создание поддельных платформ для торговли NFT. Мошенники создают поддельные сайты NFT, которые выглядят как настоящие, предлагают заманчивые условия для покупки или продажи NFT, но на самом деле крадут данные пользователей и их средства.

Эта схема часто используется мошенниками, которые создают поддельные сайты, полностью копирующие дизайн известных платформ для торговли NFT. Пользователь регистрируется на такой платформе, вводит свои платёжные реквизиты и через некоторое время замечает, что с его карты списали деньги за NFT. Это происходит потому, что поддельный сайт собирает данные пользователя, чтобы использовать их для кражи средств.

Чтобы избежать подобных схем, важно всегда проверять доменное имя сайта, на котором вы планируете покупать или продавать NFT, и использовать двухфакторную аутентификацию для защиты своей учётной записи.

Подделка NFT

Ещё одна популярная схема — продажа поддельных NFT, также известная как NFT-фишинг. Мошенники создают копии известных цифровых работ и продают их, выдавая за оригиналы. Покупатели, которые не проверили информацию о работе, становятся жертвами, приобретая бесполезные токены. Даже на популярных торговых площадках есть много мошеннических коллекций, и сложно сказать, сколько NFT являются поддельными.

Чтобы защитить себя от такого вида мошенничества, рекомендуется всегда

проверять автора NFT и историю владения токенами. Многие платформы предоставляют информацию о том, когда и кем был создан конкретный токен. Если информация об авторе отсутствует или вызывает подозрения, лучше отказаться от покупки. Также стоит обратить внимание на чрезмерно низкие цены на популярные работы. Если цена NFT значительно ниже рыночной, это может быть признаком мошенничества.

Схемы мошенничества при выводе средств

Мошенники могут предлагать «помощь» в выводе средств с продажи NFT или выводе денег с кошельков, обещая ускорить процесс или сделать его более выгодным. Это может быть особенно опасно, так как вас могут обманом заставить вывести деньги с NFT — это одна из самых распространённых мошеннических схем с NFT. На самом деле это уловка, чтобы украсть ваши средства.

Эта схема часто встречается в социальных сетях и мессенджерах, где мошенники предлагают свои «услуги» по обмену или выводу средств. Как только пользователь предоставляет свои данные, мошенники списывают деньги и исчезают. Важно никогда не делиться личной информацией с незнакомцами и не использовать сомнительные обменники или посредников для вывода средств.

NFT Социальная инженерия и фишинг.

Мошенники могут использовать социальную инженерию, чтобы обманом направлять пользователей на фишинговые сайты, где они запрашивают личные данные или ключи от криптокошельков. Например, вас могут попросить подтвердить транзакцию, перейти по ссылке, где данные будут украдены.

Социальная инженерия — одна из самых изощрённых форм мошенничества, поскольку она эксплуатирует человеческие эмоции и доверие. Мошенники могут выдавать себя за сотрудников технической поддержки или платформы и запрашивать у вас доступ к вашему кошельку или аккаунту. Чтобы избежать этого, всегда проверяйте официальные каналы связи и никогда не передавайте свои данные третьим лицам.

Взломы криптовалютных кошельков

Другой популярный метод — взлом криптокошельков, в которых хранятся NFT. Мошенники используют фишинговые атаки или вредоносное ПО, чтобы украсть личные ключи и получить полный доступ к активам пользователя.

Использование аппаратных кошельков может значительно повысить безопасность ваших активов. Эти устройства хранят закрытые ключи в автономном режиме, что делает их менее уязвимыми для кибератак. Даже если мошенники получат доступ к вашему компьютеру или мобильному устройству, они не смогут получить доступ к вашему аппаратному кошельку без физического доступа к устройству.

Пирамиды и "прокачка-сброс"- Pumping, Dumping, Hacking and Spinning.

В некоторых мошеннических схемах с NFT используется метод «накачка и сброс». Мошенники искусственно завышают стоимость определённых NFT, обещая огромную прибыль, а затем сбрасывают активы, оставляя участников с бесполезными токенами.

Эта схема особенно опасна для новичков, которых могут привлечь обещания быстрых и лёгких денег. Чтобы не участвовать в подобных схемах, важно внимательно изучать проект, проверять репутацию его создателей и не доверять обещаниям огромной прибыли за короткое время.

Фальшивые аукционы и мошеннические ставки

Схема заключается в создании поддельных аукционов, на которых якобы продаются редкие и ценные NFT. Как только покупатель делает ставку и переводит средства, сайт закрывается, а продавец исчезает с деньгами.

Фальшивые аукционы могут быть частью более масштабной схемы, включающей взлом аккаунтов на законных платформах, где мошенники выдают себя за законных продавцов. Важно всегда использовать официальные платформы для участия в аукционах и не делать ставки на сомнительных сайтах.

Плагиат

Мошенники часто просто копируют работы известных художников или музыкантов и продают их как оригинальные NFT. Это мошенничество, и такие токены не имеют ценности.

Рекомендации против мошенников с NFT

Чтобы избежать мошенничества с NFT, вы всегда должны следовать нескольким простым правилам:

Проверяйте источники: всегда проверяйте платформы, на которых вы покупаете или продаете NFT. Используйте только известные и надежные биржи, но не забывайте о мошенничестве на OpenSea, с которым вы можете легко столкнуться.

Будьте осторожны со своими личными данными: никогда не делитесь своими закрытыми ключами, личными данными или данными криптокошелька с третьими лицами.

Изучите отзывы и репутацию: перед покупкой NFT проверьте репутацию продавца и историю актива. Это поможет вам избежать покупки поддельных или бесполезных токенов.

Избегайте предложений, которые кажутся слишком хорошими, чтобы быть правдой: если что-то кажется слишком хорошим, чтобы быть правдой, скорее всего, так оно и есть.

Не пренебрегайте техническими средствами защиты: используйте аппаратные кошельки, двухфакторную аутентификацию, антивирусы и другие средства защиты. Иногда самые эффективные методы кажутся слишком очевидными и простыми.

Также важно внимательно изучить документацию и условия сделки. Если условия продажи NFT кажутся неясными или вызывают подозрения, лучше отказаться от покупки и обратиться за консультацией к специалистам.

Заключение.

Преступления в сфере криптовалют становятся всё более сложными и разнообразными. Важно быть в курсе новых угроз и методов защиты, чтобы обеспечить безопасность своих цифровых активов. Регулярно обновляя свои знания и используя проверенные методы защиты можно минимизировать риски и противостоять мошенникам.

Список источников

1. Schickler, Jack (September 2, 2022). "Money Laundering via Metaverse, DeFi, NFTs Targeted by EU Lawmakers' Latest Draft". Archived from the original on 15 December 2022. Retrieved 15 February 2023.
2. "Treasury Releases Study on Illicit Finance in the High-Value Art Market". U.S. Department of the Treasury. Archived from the original on 4 February 2022. Retrieved 15 February 2023.
3. Study of the Facilitation of Money Laundering and Terror Finance Through the Trade in Works of Art (PDF) (Report). United States Department of the Treasury. 2022. p. 26. Archived (PDF) from the original on 13 April 2022. Retrieved 15 February 2023.
4. Reiche, Matthias (July 12, 2022). "Umgang mit Bitcoin & Co. Wie die EU den Kryptomarkt reguliert" (in German). Archived from the original on 14 December 2022. Retrieved 15 February 2023.
5. "What is a 'Pig Butchering' Scam?". Tennessee Department of Commerce and Insurance. Archived from the original on 2024-07-26. Retrieved 2024-07-25.
6. Wang, Fangzhou.
7. Santiago, Jan; Camba, Alvin (2024-02-15). "Why the US and China Should Work Together to Solve the Global Scam Crisis". The Diplomat. Archived from the original on 2024-07-20. Retrieved 2024-07-20.

УДК 62

ГЛАВА 13. КИБЕРБЕЗОПАСНОСТЬ ВЕБ-САЙТОВ

Аменицкий Алексей Владимирович

аспирант

Институт аспирантуры и докторантуры Университет Лобачевского Н.И.

Рухович Игорь Владимирович**Аменицкая Любовь Алексеевна****Аменицкий Дмитрий Александрович**

студенты

НИУ ВШЭ

Аннотация: ни один сайт не может быть слишком маленьким или слишком большим, чтобы стать объектом кибератаки. Независимо от того, управляете ли вы небольшим местным бизнесом или процветающим предприятием, безопасность сайта должна быть приоритетом.

Все веб-сайты сталкиваются с угрозой попыток взлома, сканирования портов и анализа трафика. Даже если нам кажется, что у злоумышленников есть более привлекательные цели, недавние исследования показывают, что 43% всех киберпреступлений нацелены на малый бизнес. Мы не можем позволить себе думать, что «со мной такого не случится».

Эта глава представляет собой полное руководство по безопасности веб-сайтов, в котором есть всё, что нужно знать о защите от киберугроз, наиболее распространённых угрозах, с которыми сталкиваются владельцы веб-сайтов, проверенных методах повышения безопасности веб-сайтов.

Ключевые слова: Cyber Security (CS), CS architecture, CS trends, CS tendencies, CS tools, CS crimes, CS latest news, CS releases, CS game-changers, CS future, CS playbook, CS agenda, CS future, CS risks, CS incidents, CS resilience, Hackers, PenTest, CS прогноз, Artificial Intelligence, Deep Fakes, OWASP, Эволюция киберУгроз, КиберГигиена.

CYBERSECURITY OF WEBSITES

Amenitsky Alexey Vladimirovich,**Rukhovich Igor Vladimirovich,****Amenitskaya Lyubov Alekseevna,****Amenitsky Dmitry Alexandrovich**

Безопасность веб-сайта – это меры и методы, которые защищают веб-сайт от сетевых угроз. Основная цель безопасности веб-сайта - обеспечить целостность, конфиденциальность и доступность сайта.

Все веб-сайты нуждаются в той или иной форме защиты. Либо на веб-сайте хранятся конфиденциальные данные, которые можно украсть, либо мы подключены к сайтам, на которых хранится что-то ценное, либо наш веб-сайт позволяет хакерам совершать вредоносные действия. Вот наиболее распростра-

нённые цели, которые преследуют киберпреступники при атаке на веб-сайт:

- Получить несанкционированный доступ.
- Эксплуатировать посетителей сайта.
- Кража данных, хранящихся на веб-сервере.
- Показывать нежелательную рекламу.
- Злоупотребление ресурсами сервера.
- Перехватывать сеансы посетителей.
- Внедрение вредоносного кода.
- Настройка самостоятельных загрузок.
- Перенаправление законного трафика.
- Нарушают работу веб-сайта и вызывают простои.
- Искажать или вандализировать контент.

Обеспечение безопасности веб-сайта - это непрерывный процесс, который требует надёжной основы и регулярной оценки. Большинство компаний, серьёзно относящихся к защите веб-сайтов, имеют индивидуальную политику ИТ-безопасности, которая обеспечивает регулярную корректировку стратегии.

Признаки взломанного веб-сайта

Безопасность веб-сайта предотвращает инциденты, которые часто имеют серьёзные и разрушительные последствия. Применение различных мер безопасности предотвращает финансовые потери, защищает деловую репутацию и помогает привлекать новых и удерживать существующих клиентов.

Значимость безопасности веб-сайта :

- Киберзащита. Безопасность веб-сайта снижает риск киберугроз и вредоносных действий, нацеленных на веб-сайты.
- Защита данных. Владельцы веб-сайтов обеспечивают безопасность данных, которые хранятся на сайте, таких как личные данные, учётные данные для входа в систему или финансовые данные. Вы снижаете вероятность утечки данных, которая часто оказывает разрушительное воздействие на репутацию бренда и прибыль.
- Доверие пользователей. Надёжная защита веб-сайта и отсутствие инцидентов повышают доверие к веб-сайту и его сервисам.
- Непрерывность бизнес-процессов. Безопасность веб-сайта защищает его от сбоев, вызванных кибератаками, и обеспечивает постоянную работу сайта.
- Предотвращение финансовых потерь. Взломанный веб-сайт приводит к потере прибыли из-за простоев, дорогостоящих расходов на восстановление и штрафов регулирующих органов.
- Соблюдение нормативных требований. Меры по обеспечению безопасности веб-сайтов часто необходимы для соблюдения нормативных требований, связанных с защитой данных, конфиденциальностью и безопасностью (например, ССРА или GDPR). Несоблюдение требований приводит к крупным штрафам и взысканиям.

- Поисковая оптимизация веб-сайта. Поисковые системы наказывают за зараженные или незащищенные веб-сайты. Принятие мер по защите веб-сайта гарантирует, что поисковые системы будут правильно индексировать и ранжировать ваши страницы.

- Каждый третий потребитель сообщает о разрыве отношений с компаниями, которые допустили утечку персональных данных клиентов (PII). Угроза потерять треть клиентской базы — ещё один явный показатель того, почему безопасность сайта так важна.

Уязвимости и угрозы веб-сайта

Владельцы сайтов должны быть готовы к различным уязвимостям и угрозам. Вот с чем владельцы сайтов должны быть готовы столкнуться:

- SQL-инъекции (SQLI). подразумевают внедрение вредоносного кода в уязвимую базу данных SQL. Такие атаки обычно позволяют злоумышленнику получить несанкционированный доступ или манипулировать данными.

- Межсайтовый скриптинг (XSS). XSS позволяет злоумышленнику внедрять вредоносные скрипты на веб-страницу, просматриваемую другими пользователями.

- Подделка межсайтового запроса (CSRF). Некоторые злоумышленники пытаются заставить пользователей или обманом заставить их выполнять нежелательные действия на веб-сайте. Обычно они преследуют две цели: вызвать мошеннические транзакции или внести изменения в учётные записи пользователей.

- Атаки типа "Человек посередине" (MitM). перехватывают и потенциально изменяют общение между веб-сайтом и его посетителями.

- Атаки на внешние объекты XML (XXE). Опытные хакеры знают, как использовать уязвимые обработчики XML для раскрытия внутренних файлов или выполнения удалённого кода.

- Атаки методом перебора. При атаке методом перебора бот многократно пытается угадать пароль или ключ шифрования и получить несанкционированный доступ к учётным записям или данным.

- Незащищённые прямые ссылки на объекты (IDOR). Эта тактика позволяет злоумышленнику получать доступ к ресурсам и управлять ими, используя уязвимости в ссылках на объекты.

- Фишинговые атаки- это попытки обманом заставить пользователей предоставить конфиденциальную информацию, выдавая себя за надёжную организацию, часто с помощью электронных писем или поддельных веб-страниц.

- Вредоносные перенаправления. Киберпреступники часто пытаются перенаправить пользователей на вредоносные веб-сайты или переслать их по нежелательным адресам.

- Программы-вымогатели. При успешном внедрении программы-вымогатели шифруют файлы на веб-сервере, делая содержимое сайта недоступным.

- Отказ в обслуживании (DoS) и распределённый отказ в обслуживании (DDoS). DoS- и DDoS-атаки перегружают веб-сайт фиктивным трафиком, что-

бы вызвать его отключение. Таким образом злоумышленники нарушают работу и ухудшают взаимодействие с пользователями.

Фреймворки и стандарты веб-безопасности

Структуры и стандарты веб-безопасности — это общие рекомендации, которые помогают организациям защищать веб-приложения и веб-сайты. Вот пять самых популярных структур и стандартов веб-безопасности:

OWASP (Проект по обеспечению безопасности веб-приложений). Эта платформа предоставляет ресурсы, инструменты и рекомендации по устранению распространенных рисков для безопасности веб-приложений.

ISO 27001. Этот стандарт обеспечивает системный подход к управлению рисками, связанными с безопасностью в Интернете.

NIST (Национальный институт стандартов и технологий). NIST предлагает комплексные системы кибербезопасности, рекомендации и передовые методы.

CIS (Центр интернет-безопасности) Контроли. Контроли CIS предоставляют набор рекомендаций по повышению уровня безопасности, включая меры по защите веб-сред.

WASC (Консорциум по безопасности веб-приложений). WASC разрабатывает и продвигает передовые методы обеспечения веб-безопасности, уделяя особое внимание авторизации, проверке вводимых данных и управлению сессиями.

Ни один фреймворк по своей сути не лучше другого. Различные варианты поставляются с бесплатной защитой от DDoS-атак. Используется автоматизированная фильтрация трафика и молниеносная инфраструктура для смягчения последствий, чтобы всё, что размещается на облачных серверах, оставалось доступным круглосуточно. Широкий функционал позволяет выбрать наиболее подходящий для актуальных потребностей и приоритетов в области безопасности.

Рассмотрим, как работают фреймворки, на примере рекомендаций NIST. Фреймворк NIST по кибербезопасности (CSF) состоит из пяти основных функций:

- Идентификация. Эта функция позволяет пользователям идентифицировать критически важные ИТ-активы, системы, данные и возможности.
- Защита. Функция «Защита» направлена на принятие мер по ограничению или сдерживанию последствий неблагоприятных событий.
- Обнаружение. Эта функция направлена на своевременное обнаружение инцидентов в организации.
- Ответ. Функция «Ответ» описывает действия, которые необходимо выполнить при обнаружении инцидента.
- Восстановление – функция посвящена стратегиям восстановления сервисов, пострадавших в результате инцидента.

Идея состоит в том, чтобы использовать структуру NIST в качестве основы, на которой строится стратегия безопасности веб-сайта. Структура адаптируется и подстраивается под конкретные потребности пользователей и создаётся комплексная ИТ-защита.

Наиболее распространенные векторы атак на веб-сайты. Как обезопасить свой веб-сайт.

Компании должны проявлять инициативу в вопросах безопасности веб-сайтов. Ниже приведены несколько высокоэффективных мер предосторожности, которые повышают безопасность веб-сайтов и значительно снижают вероятность дорогостоящих инцидентов.

- Поддерживайте веб-сайт в актуальном состоянии благодаря последним обновлениям

- Администраторы веб-сайтов должны устанавливать обновления и исправления сразу после их появления.

Вот краткий обзор того, почему этот процесс так важен для безопасности веб-сайта:

- Обновления программного обеспечения часто включают патчи безопасности, устраняющие уязвимости. Обновление программного обеспечения вашего сайта устраняет эти уязвимости, снижая риск взлома.

- Злоумышленники часто сканируют веб-сайты на наличие уязвимостей, чтобы найти цели с устаревшим программным обеспечением. Своевременное обновление снижает риск стать жертвой атак, нацеленных на устаревшие версии программных компонентов.

- Обновления часто включают в себя улучшения функций и механизмов безопасности. Если вы будете следить за обновлениями, ваш сайт будет пользоваться новейшими функциями безопасности.

- Обновления программного обеспечения часто включают исправления ошибок, повышение производительности и стабильности. Регулярное обновление исправлений обеспечивает бесперебойную и эффективную работу веб-сайта, сводя к минимуму риск простоев или сбоев. Необходимо следовать этим рекомендациям, чтобы эффективно управлять обновлениями программного обеспечения для веб-сайта.

- Регулярный мониторинг исправлений. Следите за обновлениями программного обеспечения, выпущенными поставщиками компонентов программного обеспечения, используемых на вашем сайте (например, веб-сервером, CMS, плагинами, темами, сторонними библиотеками и т. д.).

- Надлежащее управление исправлениями. Установите регулярный график применения обновлений. Ведите документацию по процедурам обновления и истории версий, а также создайте каналы связи для оповещения заинтересованных сторон о важных обновлениях.

- Стратегическая расстановка приоритетов. Уделяйте первоочередное внимание обновлениям компонентов программного обеспечения, которые напрямую взаимодействуют с пользовательским вводом или обрабатывают конфиденциальные данные.

- Тщательное тестирование. Всегда тестируйте обновления в промежуточной среде, прежде чем применять их на рабочем сайте. Убедитесь, что обновления не приводят к непредвиденным ошибкам или конфликтам.

Некоторые компании используют инструменты и скрипты для автоматизации процесса обновления. Несмотря на эффективность, такая практика сопря-

жена с риском, поэтому нужно быть осторожными и определить строгие процедуры тестирования при использовании этого способа автоматизации.

Используйте HTTPS

Протокол безопасной передачи гипертекста (HTTPS) используется для передачи данных между веб-браузером пользователя и сайтом, который он посещает. На сайтах, использующих HTTPS, в адресной строке браузера отображается значок замка.

Вот как HTTPS улучшает безопасность веб-сайта по сравнению с HTTP:

- HTTPS использует протоколы TLS или SSL для шифрования данных, передаваемых между браузером пользователя и веб-сервером. Шифрование предотвращает прослушивание и перехват трафика, а также обеспечивает целостность данных.

- Поисковые системы отдают предпочтение сайтам, использующим HTTPS. Переход на HTTPS повышает рейтинг вашего сайта в поисковых системах.

- HTTPS предоставляет механизмы аутентификации для обеспечения связи пользователей с нужным сервером. Эта проверка помогает предотвратить атаки типа «человек посередине» и попытки фишинга, подтверждая цифровой сертификат сервера.

Чтобы внедрить HTTPS на своём веб-сайте, мы должны получить TLS- или SSL-сертификат от надёжного центра сертификации (CA) и настроить веб-сервер для использования HTTPS. Большинство провайдеров веб-хостинга предлагают встроенные инструменты, которые помогают пользователям устанавливать и настраивать сертификаты. Необходимо собрать информацию о различных типах SSL-сертификатов и выбрать наиболее подходящий для веб-сайта.

Настройка WAF

Очень эффективно внедрение брандмауэра веб-приложений (WAF) для защиты веб-приложений и веб-сайтов от онлайн-угроз. Этот тип брандмауэра действует как барьер между веб-сайтом и Интернетом, проверяя входящий и исходящий трафик на наличие вредоносных запросов и полезной нагрузки.

WAF очень эффективно защищает от большинства распространённых веб-атак, в том числе:

- SQL-инъекции.
- Межсайтовый скриптинг.
- Подделка межсайтовых запросов.
- Удаленное включение файлов (RFI).
- Включение локального файла (LFI).
- Внедрение внешних сущностей XML.
- Подделка запросов на стороне сервера (SSRF).
- Перехват сеанса и его фиксация.

WAF используют сочетание обнаружения на основе сигнатур, поведенческого анализа и машинного обучения для выявления и блокировки вредоносно-

го трафика. WAF обеспечивает детальный контроль и возможности настройки, позволяя определять наборы правил, блокировать определённые IP-адреса и настраивать действия по реагированию на различные инциденты.

Использование надежных паролей

Обеспечение надёжных паролей для пользователей и администраторов сайта имеет решающее значение для безопасности сайта. Слабые или легко угадываемые пароли делают учётные записи уязвимыми для несанкционированного доступа.

Вот основные требования к надёжному паролю:

- Пароли должны содержать сочетание прописных и строчных букв, цифр и специальных символов.
- Длинные пароли более надёжны, чем короткие. Старайтесь, чтобы минимальная длина пароля составляла от 12 до 15 символов.
- Пароли не должны содержать распространённые слова, имена, фразы или шаблоны. Такие пароли легко угадать или взломать с помощью атак по словарю или методом перебора.
- У каждой учётной записи должен быть уникальный пароль. Повторное использование паролей повышает риск подбора учётных данных — атак, при которых кто-то использует украденный пароль от одной учётной записи для доступа к другим учётным записям того же пользователя.
- Используйте менеджер паролей, чтобы помочь пользователям веб-сайтов создавать и хранить сложные уникальные пароли для каждой учётной записи. Менеджеры паролей также позволяют устанавливать политики паролей и соблюдать правила, касающиеся длины, уровня сложности и периодического обновления паролей. Крупные компании часто идут дальше и инвестируют в корпоративное управление паролями.

Проверка входных данных

Проверка вводимых пользователем данных включает в себя проверку и очистку данных, отправляемых пользователями через веб-формы, URL-адреса и другие механизмы ввода.

Проверка вводимых данных гарантирует, что в рабочий процесс сайта будут попадать только правильно сформированные данные. Вот какие типы атак предотвращает эта мера:

- Атаки с использованием инъекций. Проверка вводимых пользователем данных помогает предотвратить атаки с использованием инъекций, такие как SQL-инъекции и инъекции NoSQL. Веб-приложения отклоняют или очищают вводимые данные, содержащие вредоносные запросы.
- XSS. Правильная проверка вводимых данных и кодирование выходных данных помогают предотвратить атаки с использованием межсайтового скриптинга, не позволяя внедрять вредоносные скрипты на веб-страницы.
- CSRF. Проверка вводимых пользователем данных предотвращает подделку межсайтовых запросов, проверяя целостность входящих запросов.
- Уязвимости при загрузке файлов. Проверка ввода предотвращает уяз-

вимости при загрузке файлов, например, когда пользователи могут загружать на веб-страницу исполняемые файлы.

- Изменение параметров. Проверка вводимых пользователем данных защищает от атак с изменением параметров путем очистки параметров, передаваемых через строки запроса, поля форм, файлы cookie и заголовки HTTP.

Большинство популярных платформ и языков веб-разработки имеют библиотеки и фреймворки для проверки вводимых данных, такие как OWASP ESAPI для Java, Django Forms для Python или Laravel Validation для PHP. Всегда настраивайте проверку вводимых данных на стороне сервера, чтобы все входящие данные проходили проверку независимо от клиентской проверки, реализованной для удобства пользователей или повышения скорости отклика.

Создавайте резервные копии всего ценного

Регулярное резервное копирование данных защищает от безвозвратной потери файлов, предотвращает простои веб-сайта и помогает восстанавливаться после инцидентов, связанных с безопасностью.

Регулярно создавайте копии важных файлов, баз данных и настроек конфигурации. В случае инцидента, связанного с безопасностью, или повреждения данных резервные копии позволят вам восстановить сайт в предыдущем состоянии.

Резервное копирование — это самый надёжный способ предотвратить ошибки, совершаемые людьми. Такие ошибки, как случайное удаление файлов, неправильная настройка или непреднамеренные изменения в коде веб-сайта, часто приводят к проблемам и уязвимостям в системе безопасности. Регулярное резервное копирование обеспечивает защиту от таких ошибок, позволяя вернуться к предыдущему состоянию до возникновения ошибки.

Резервные копии также важны для предотвращения заражения программами-вымогателями. Если вредоносная программа зашифрует файлы вашего сайта, недавние резервные копии позволят вам восстановить незатронутые версии данных без необходимости платить выкуп.

Заголовки безопасности

Заголовки безопасности — это заголовки HTTP-ответов, которые сообщают браузеру, как обрабатывать взаимодействие с сайтом. Вот шесть обязательных заголовков безопасности и их назначение:

- X-Content-Type-Options. Этот заголовок предотвращает атаки с использованием MIME-sniffing, указывая браузеру придерживаться заявленного типа контента и не интерпретировать файлы на основе анализа контента.

- X-Frame-Options. Эти заголовки предотвращают атаки с использованием кликджекинга, которые являются одними из самых распространённых угроз безопасности в электронной коммерции. Заголовок X-Frame-Options предотвращает атаки, контролируя возможность встраивания веб-страницы во встроенный фрейм (iframe).

- Политика безопасности контента (CSP). CSP позволяет владельцу веб-сайта указывать доверенные источники контента. CSP предотвращает XSS-атаки, блокируя или ограничивая выполнение скриптов из неавторизованных

источников.

- HTTP Strict-Transport-Security (HSTS). Заголовок HSTS указывает браузеру на необходимость взаимодействовать с сайтом только по протоколу HTTPS, даже если пользователь пытается получить доступ к сайту по протоколу HTTP.

- Referrer-policy. Этот заголовок определяет, сколько информации браузер включает в заголовок Referrer при переходе на другие веб-сайты.

- Feature-Policy. Заголовок Feature-Policy позволяет указать разрешённые функции браузера и API.

Внедрение заголовков безопасности значительно повышает уровень защиты сайта и защищает от широкого спектра сетевых атак.

Тщательный выбор расширения

Расширения, плагины, темы и другие сторонние компоненты часто приводят к уязвимостям на сайте, если они плохо написаны, устарели или установлены из ненадёжного источника.

- Ограничьте количество расширений только теми, которые необходимы для работы сайта. Если вам нужно дополнительное расширение, вот типичные признаки того, что его можно безопасно установить:

- Загружайте расширения непосредственно из официальных репозиторий или торговых площадок, связанных с платформой вашего сайта или CMS. Избегайте загрузок со сторонних сайтов, чтобы снизить риск установки поддельных или вредоносных расширений.

- Перед установкой внимательно проверьте качество кода и методы обеспечения безопасности расширений. Проведение аудита безопасности на тестовом сайте перед развертыванием нового расширения также является разумной практикой. Таким образом вы убедитесь, что дополнение не содержит ошибок и не конфликтует с существующими компонентами сайта.

Наиболее распространённые проблемы с безопасностью веб-сайта

- Ограничение доступа и разрешений помогает защитить конфиденциальные данные и ресурсы сайта от злоумышленников. Вот что нужно вашему сайту:

- Внедрите надёжные механизмы аутентификации пользователей, такие как многофакторная аутентификация (MFA) и детальный контроль авторизации.

- Используйте управление доступом на основе ролей (RBAC) и назначайте пользователям разрешения в соответствии с их ролями в организации.

- Ограничьте права доступа к файлам и каталогам на веб-сервере, чтобы предотвратить несанкционированный доступ к файлам конфигурации.

- Внедрите контроль доступа и разрешения на уровне базы данных, чтобы защитить конфиденциальные файлы от манипуляций с ними.

- Используйте методы управления сессиями, чтобы предотвратить перехват и несанкционированный доступ к пользовательским сессиям. К распространённым стратегиям относятся тайм-ауты сессий, защищённые файлы cookie и механизмы проверки сессий.

- Отслеживайте попытки доступа, повышение привилегий и несанкционированные события для обнаружения инцидентов, связанных с безопасностью.
- Проводите периодические проверки доступа, чтобы убедиться, что права пользователей соответствуют требованиям бизнеса и их текущим ролям.
- Отмените ненужные привилегии и роли для неактивных или удалённых учётных записей, чтобы уменьшить поверхность атаки.
- Настройте решение для управления привилегированным доступом (PAM) для защиты доступа к наиболее важным системам и ресурсам.
- Следуйте принципу наименьших привилегий и предоставляйте пользователям только минимальный уровень доступа и разрешений, необходимый для выполнения их работы. Ограничение доступа к основным функциям и данным сводит к минимуму последствия потенциальных нарушений и внутренних угроз.

Готовность к инцидентам

Мониторинг событий, связанных с безопасностью, и оперативное реагирование на них имеют решающее значение для безопасности веб-сайта. Владельцы веб-сайтов должны выявлять и устранять угрозы в режиме реального времени, чтобы минимизировать последствия нарушений безопасности и обеспечить постоянную доступность и целостность веб-сайта.

Очень важно выявить кибератаки на ранних этапах, поэтому лучше поймать злоумышленников до того, как они нанесут слишком большой ущерб сайту. Следите за трафиком и системными журналами, чтобы выявлять попытки несанкционированного доступа и потенциальные угрозы безопасности.

Непрерывный мониторинг является приоритетом. Используйте автоматизированные инструменты для анализа журналов, обнаружения аномалий и поведенческой аналитики, чтобы более эффективно выявлять угрозы и реагировать на них.

Разработайте план реагирования на инциденты, в котором будут описаны роли, обязанности и процедуры реагирования на наиболее вероятные инциденты, связанные с безопасностью. Таким образом вы обеспечите скоординированное и эффективное реагирование во время инцидента, связанного с безопасностью. Кроме того, сохраняйте соответствующие журналы, снимки системы и доказательства для последующего расследования и анализа. Контрольный список для аварийного восстановления помогает создавать безупречные планы реагирования на потенциально разрушительные события.

Инструменты безопасности веб-сайта

Инструменты для обеспечения безопасности веб-сайтов помогают защищать сайты от угроз, обнаруживать вредоносную активность и реагировать на инциденты. Вот несколько очень популярных инструментов, которые стоит добавить в большинство стратегий обеспечения безопасности веб-сайтов:

- **Sucuri** Этот инструмент предлагает набор функций для обеспечения безопасности веб-сайтов, включая WAF, сканирование на наличие вредоносных

программ, удаление вирусов и мониторинг безопасности.

- Acunetix Этот инструмент для оценки уязвимостей выявляет и ранжирует по значимости недостатки в системе безопасности веб-сайтов.

- DataDome Этот механизм обнаружения на основе искусственного интеллекта позволяет владельцам сайтов выявлять и предотвращать мошеннический трафик.

- Imperva App Protect Этот инструмент для защиты веб-сайтов включает в себя WAF корпоративного уровня, отличное решение для защиты от DDoS-атак и CDN высшего уровня.

- Invicti (ранее Netsparker). Этот инструмент автоматически выявляет SQL-инъекции, межсайтовый скриптинг и удалённое выполнение кода в веб-приложениях и API.

- Probely, этот сканер уязвимостей позволяет владельцам сайтов оценивать безопасность веб-приложений и API.

- Astra Эта платформа предоставляет набор средств безопасности, который включает в себя активный WAF в реальном времени, сканер вредоносных программ на основе машинного обучения, поиск уязвимостей, тестирование на проникновение, блокировку IP-адресов и стран и различные средства повышения безопасности.

- Qualys (WAS) Этот облачный инструмент использует как динамический, так и статический анализ для выявления широкого спектра проблем с безопасностью (например, уязвимостей, связанных с внедрением кода, нарушений аутентификации, раскрытия данных и т. д.).

- WPScan Этот инструмент анализирует веб-сайты WordPress на наличие потенциальных уязвимостей с помощью технологии глубокого сканирования.

- Wordfence Этот плагин безопасности обеспечивает защиту брандмауэром, сканирование на наличие вредоносных программ, защиту входа в систему и анализ угроз в реальном времени для веб-сайтов на базе WordPress.

Заключение

Точное количество ежедневно взламываемых веб-сайтов определить сложно, но, по статистике, около 30 000 веб-сайтов подвергаются взлому каждый день. «Взлом» означает несанкционированный доступ или потерю контроля над веб-сайтом.

Преступники взламывают веб-сайты по разным причинам. Наиболее распространённые цели — кража конфиденциальных данных, распространение вредоносного ПО, фишинговые атаки, кампании с использованием программ-вымогателей, порча веб-сайтов или использование веб-сайтов для дальнейших атак (например, рассылка спама или DDoS-атаки).

Безопасный веб-сайт реализует меры, которые защищают от киберугроз и обеспечивают целостность и доступность данных. К таким мерам относятся шифрование HTTPS, внедрение WAF, регулярные обновления программного обеспечения и строгий контроль доступа. Безопасный веб-сайт также должен

соответствовать рекомендациям по обеспечению безопасности и не иметь проблем с конфигурацией или уязвимостей веб-сервера.

Взломанный веб-сайт наносит ущерб репутации, подрывает доверие клиентов, приводит к финансовым потерям и потенциальным юридическим последствиям. К счастью, повысить безопасность веб-сайта гораздо дешевле и проще, чем бороться с последствиями успешных атак. Эта глава поможет повысить безопасность веб-сайта и сделать так, чтобы бизнес не стал лёгкой мишенью для веб-атак.

Список источников

1. "Figure 2.3. Relative risk of being a low performer depending on personal circumstances (2012)". doi:10.1787/888933171410. Retrieved May 29, 2021.
2. Stoneburner, Gary; Goguen, Alice; Feringa, Alexis (2002). "NIST SP 800-30 Risk Management Guide for Information Technology Systems". doi:10.6028/NIST.SP.800-30. Retrieved January 18, 2022.
3. Web app | Definition, History, Development, Examples, Uses, & Facts | Britannica". www.britannica.com. Encyclopædia Britannica. Retrieved 4 November 2024.
4. "What is a Web App? - Web Application Explained - AWS". Amazon Web Services, Inc. Retrieved 4 November 2024.
5. "Web applications". DocForge. Archived from the original on 19 April 2015. Retrieved 9 November 2024.

УДК 62

ГЛАВА 14. КИБЕРБЕЗОПАСНОСТЬ. DARK WEB VS. DEEP WEB VS. SHADOW WEB

Аменицкий Алексей Владимирович

аспирант

Институт аспирантуры и докторантуры Университет Лобачевского Н.И.

Рухович Игорь Владимирович

Аменицкая Любовь Алексеевна

Аменицкий Дмитрий Александрович

студенты

НИУ ВШЭ

Аннотация: Интернет полностью изменил нашу жизнь, работу и общение. У нас есть быстрый доступ к огромным массивам знаний, развлечениям и социальным связям. Но большинство людей никогда не видят тёмную сторону интернета. Это и есть «теневого интернет». Это часть интернета, недоступная с помощью стандартных веб-браузеров и не отображаемая поисковыми системами. Незаконный оборот наркотиков, торговля людьми и продажа запрещённых товаров — вот лишь несколько примеров незаконной деятельности в загадочной и опасной «теневого сети». В этой главе собрана аналитика о теневого сети, её происхождении, внутренней организации и потенциальных угрозах.

Темная паутина, или темная сеть, - это погруженная в воду грань огромного айсберга, который представляет собой Интернет. На самом деле, несмотря на то, что сеть уже очень обширна, в том виде, в каком вы ее знаете, она на самом деле ограничена, и у вас есть доступ только к ограниченному количеству результатов. Темная паутина дает вам доступ ко многим другим сайтам, а также к самым темным уголкам сети, поскольку там хорошо укоренились всевозможные хакеры и незаконные сети.

Хотя у darkweb плохая репутация, он также является убежищем для свободы слова, где угнетенное население, журналисты и политические диссиденты могут высказываться, не опасаясь репрессий. Кроме того, мы находим там впечатляющую базу данных, которая, более того, не подвергается никакой цензуре. Вот почему доступ к ней может быть полезен, если вы хотите узнать более подробно о предмете и получить информацию, к которой вы никогда не смогли бы получить классический доступ. Будьте уверены, попасть туда не так уж и сложно.

Ключевые слова: Cyber Security (CS), CS architecture, CS framework, CS trends, CS tendencies, CS tools, CS crimes, CS latest news, CS releases, CS game-changers, CS future, CS playbook, CS agenda, CS future, CS risks, CS incidents, CS resilience, Hackers, PenTest, CS прогноз, Artificial Intelligence, Deep Fakes, OWASP, Website security, CryptoScams, CryptoJacking, CryptoFraud, NFT scams, Antifraud, Dark Web, Deep Web, Shadow Web, Dark Net, Эволюция киберУгроз, КиберГигиена.

CYBERSECURITY. DARK WEB VS. DEEP WEB VS. SHADOW WEB

Amenitsky Alexey Vladimirovich,
Rukhovich Igor Vladimirovich,
Amenitskaya Lyubov Alekseevna,
Amenitsky Dmitry Alexandrovich

Теневая сеть, которую обычно называют Даркнетом, — это защищённая область интернета, недоступная через стандартный браузер. В отличие от обычной сети, теневая сеть намеренно скрыта, и доступ к ней можно получить только с помощью специализированного программного обеспечения. Её также легко найти и проиндексировать поисковым системам.

Теневой интернет — это место, где пользователи могут оставаться анонимными и заниматься деятельностью, которая не всегда является правильной с моральной или юридической точки зрения. Сайты, продающие нелегальные товары и услуги, в том числе наркотики, оружие и украденную личную информацию, называют его своим домом. Это место, где государственные учреждения, активисты и хакеры ведут свои дела в полной конфиденциальности и вдали от любопытных глаз правоохранительных органов.

Не раскрывая своей личности или местонахождения, пользователи могут общаться и обмениваться информацией через «теневой интернет» — сеть зашифрованных сетей, использующих одноранговые соединения. Это место, где люди могут совершать незаконные действия, не беспокоясь о том, что их поймут, или где активисты могут планировать демонстрации и общаться друг с другом без вмешательства правительства.

Несмотря на то, что «теневая сеть» часто связана с преступной деятельностью, важно помнить, что не все действия в ней незаконны. «Теневая сеть» используется журналистами, информаторами и активистами для безопасного взаимодействия и обмена информацией. Однако из-за своей скрытой природы и обеспечиваемой ею анонимности она часто используется в корыстных целях.

Сеть Даркнет построена через Интернет и зашифрована. Darknet обеспечивает анонимность пользователей. Одним из таких darknet является Tor (The Onion Router). Для входа в эту сеть требуется специальное программное обеспечение, например, браузер Tor, который требуется для входа в сеть Tor. TOR может также получать доступ к обычным веб-сайтам, веб-сайт в этой сети имеет адрес .onion. В Dark Net предоставляется множество скрытых услуг. Friend-to-Friend — это еще один вид darknet, где два человека анонимно передают данные между собой. Доступ к нему имеют только заинтересованные лица, и он зашифрован и защищен паролем. Помимо этого, Freenet также является darknet, который используется для анонимной передачи файлов, доступно много других darknet.

Даркнет относится к скрытой части Интернета, к которой невозможно получить доступ с помощью обычного браузера, такого как Google или Firefox. Действительно, когда вы выполняете поиск в сети, на самом деле у вас есть доступ менее чем к 5% всего контента, представленного в сети.

Темная паутина - это часть глубокой сети, на которую, в свою очередь, приходится более 90% контента. Его название «темная» относится к тому факту, что оно скрывает личность пользователей Интернета, которые просматривают его. Обратной стороной медали является то, что она также защищает преступников, которые могут безнаказанно осуществлять там свою незаконную деятельность: педофильские сети, порнографические, террористические, незаконный оборот наркотиков и т. д.

Вдали от гигантских серверных центров Google, Темная паутина представляет собой рой разбросанных серверов с более или менее случайной стабильностью. Кроме того, он использует многоуровневые сети, которые анонимизируют обмен данными, пропуская их через несколько узлов (P2P) по всему миру; что затрудняет отслеживание серверов и пользователей. Мы говорим о луковой маршрутизации, которая действует как уровни защиты, как и различные уровни, защищающие лук.

Как работают сети Darknet

Поскольку тайная сеть намеренно скрыта, для доступа к ней необходимо использовать специальное программное обеспечение. Самым известным из них является Тор (Луковый маршрутизатор). У него более 2,5 миллионов пользователей. Среди других подходящих программ мы также можем упомянуть Freenet и I2P.

Большая часть «глубокого интернета» (следующий уровень после «поверхностного интернета») абсолютно безопасна, так как это просто неиндексируемые части интернета, такие как банковские порталы и научные журналы.

Однако, при входе в даркнет, важно быть внимательным к контенту, который вы пытаетесь просмотреть, так как хакерам будет легко получить доступ к вашей конфиденциальной информации, если вы будете нажимать на всё подряд, не задумываясь.

На самом деле, если кто-то получит доступ к вашим конфиденциальным данным с помощью фишинга, шпионского ПО или каким-либо другим способом, он, скорее всего, продаст эти данные в даркнете. Покупатель может делать с вашей информацией всё, что захочет, и это, конечно, немного пугает.

Однако важно помнить, что даркнет не является незаконным, но в нём происходит незаконная деятельность. Поэтому, если вы будете осведомлены и будете знать о рисках, доступ к этим слоям интернета будет безопасным. Кроме того, для доступа к даркнету требуется надёжное шифрование, которое также может быть незаконным в зависимости от вашей юрисдикции.

Что касается теневого интернета и «Марианской сети», то сложно сказать, насколько они безопасны, учитывая, что их существование до сих пор вызывает споры. Настоятельно рекомендуется сохранять бдительность и принимать взвешенные решения, прежде чем отправляться в даркнет. В конце концов, людей постоянно обманывают в обычном интернете, не говоря уже о теневых подпольных форумах.

Никто не может сказать насколько глубоко простирается Сеть

Хотя мы все можем строить догадки и проводить исследования в интернете, трудно определить, сколько на самом деле «слоёв» в интернете, учитывая его невообразимые масштабы. Даже большинство энтузиастов даркнета не до конца понимают, насколько он глубок, и это пугает и интригует.

История Теневой паутины

Теневая сеть, которую часто называют даркнетом, — это элемент интернета, скрытый и недоступный для стандартных поисковых систем и браузеров. Она представляет собой сеть зашифрованных серверов и веб-сайтов, для доступа к которым требуется специальное программное обеспечение, настройки или авторизация.

Когда в первые дни существования Интернета появилась «теневая сеть», военные США разработали безопасный и конфиденциальный способ связи со своими полевыми сотрудниками. После того как эта система, известная как Tor, стала общедоступной, она быстро стала основой «теневой сети».

По мере расширения «теневой сети» она стала центром преступной деятельности, в том числе продажи краденых товаров и торговли людьми. Секретность и анонимность «теневой сети» позволяли преступникам действовать, не опасаясь разоблачения.

Однако «теневая сеть» могла бы быть лучше. Кроме того, она предлагает безопасную среду, в которой журналисты, политические активисты и информаторы могут общаться и обмениваться информацией, не беспокоясь о возмездии или цензуре. «Теневая сеть» может быть единственным источником нефильТРованных новостей и информации для граждан некоторых стран.

Почему даркнет опасен

Так сложилось, что в даркнете обитают в основном преступники и кибермошенники, занимающиеся нелегальной продажей запрещенных веществ. Здесь незаконно продают:

- электронные адреса;
- запрещенные препараты;
- органы и части тела;
- онлайн-библиотеки;
- базы данных пользователей ресурсов, которые были подвергнуты удачной хакерской атаке;
- фальшивые удостоверения личности;
- анонимные прокси-серверы;
- услуги сотрудников и инсайдеров.
- Также здесь процветает торговля людьми и детьми.
- медицинские карты,
- веб-сайты членства,
- платный контент,
- платные публикации,
- академические журналы.

Какие сайты есть в даркнете

Наиболее распространены в даркнете онлайн-магазины с запрещенными товарами для торговли наркотиками, оружием, фальшивыми деньгами и т. д. Также в даркнете развит рынок противоправных услуг, вплоть до заказных убийств. В «теневом интернете» также можно найти ресурсы, специализирующиеся на утечках баз данных (ведомств, банков, сотовых операторов и т. д.) и продаже инсайдерской информации. Кроме того, в даркнете есть и относительно «мирные» сервисы: например, анонимные почтовые сервисы, аналоги социальных сетей и онлайн-библиотеки, а также форумы для общения и обсуждения любых тем.

Свои сервисы также размещают в даркнете и легальные ресурсы, чтобы помочь пользователям обойти блокировки и обеспечить доступ из любой точки мира. Например, с 2014 года своя версия сайта в сети Tor есть у соцсети Facebook (головная компания Meta признана экстремистской организацией и запрещена в России) и некоторых СМИ, например The New York Times, BBC и Deutsche Welle.

Что можно купить в даркнете

В даркнете есть несколько типов наиболее часто встречающихся предложений:

- продажа и покупка баз данных;
- запросы и предложения о взломе аккаунтов (почты, социальных сетей, мессенджеров);
- продажа и покупка банковских карт, оформленных на подставных лиц, открытие и продажа расчетных счетов в банках, оформление документов и т. п.;
- услуги по «пробиву»;
- сервисы по обналичиванию и отмыванию денежных средств (чаще всего преступных) за процент;
- отрисовка фальшивых документов, в том числе медицинских справок;
- покупка и продажа анонимных прокси-серверов;
- поиск соотрудников и инсайдеров.

Оборот физических товаров ограничен банковскими и SIM-картами, наркотиками и прекурсорами, поддельными документами, фальшивыми купюрами, специфическими устройствами (скиммеры, отмычки, глушители радиосигнала и т. д.) и оружием, говорит руководитель Департамента исследований высокотехнологичных преступлений компании Group-IB Андрей Колмаков. Услуги вне интернета сводятся к операциям по обналичиванию похищенных денежных средств и распространению наркотиков, обороту приобретенных за счет похищенных средств товаров, подбору дропов (подставных лиц), пояснил он.

Варианты использования глубокой сети

- Платные подписки. Глубокая сеть используется для доступа ко всем типам платных подписок, таких как потоковые сервисы, например, Netflix и Hulu.

- Доступ к учетным записям. Одним из основных способов использования глубокой сети является вход в учетные записи, такие как социальные сети или банковские счета.

- Онлайн-платежи. Всякий раз, когда вы платите за что-то в Интернете, вы вводите свою платежную информацию через глубокую сеть.

Если вы не разбираетесь в протоколах соединения и в их безопасности в интернете, то лучше не заходить в теневой интернет. Так как одно неправильное движение или оставленные на его просторах личные данные могут привести к тому, что вас скомпрометируют мошенники.

Минимальное, что могут сделать кибермошенники, это получив информацию о вашем IP-адресе, заблокировать ПК и потребовать выкуп за разблокировку. В другом случае к вам домой могут заглянуть спецслужбы.

Что еще нужно знать о даркнете

В даркнете продают краденные клиентские базы. Новые технологии и разработки тоже могут быть украдены через теневой интернет. Поэтому системным администраторам в крупных компаниях нужно быть предельно внимательными к тому, что ищут и куда заходят обычные сотрудники организации.

Они могут продавать через даркнет технологии или новые разработки в бизнесе и производстве. Руководству компаний желательно внимательно относиться к сотрудникам, которых они нанимают на место системных администраторов. Потому что часто эти люди, в попытках хорошо заработать, идут на сделки с мошенниками через даркнет и открывают доступ или сливают базы данных в теневой интернет.

Сейчас доступы к серверам из браузера Tor пытаются ограничивать. Находят реальные сервера и блокируют их. Однако существует много путей обхода этих блокировок, которыми пользуются хакеры.

Как попасть в даркнет

Самый простой и распространенный способ зайти в даркнет — это скачать браузер Tor, поскольку именно в его сети находится больше всего теневых ресурсов. Tor разрабатывался в конце 90-х годов в Научно-исследовательской лаборатории ВМС США для защищенных переговоров спецслужб, однако затем проект стал открытым, и сейчас за его разработку отвечает команда Tor Project.

Еще один сервис, чтобы войти в даркнет, — сеть I2P. В этом сегменте значительно меньше ресурсов, чем в сети Tor, однако она более безопасна и анонимна, поскольку изначально проектировалась для доступа к скрытым сайтам. Однако развивается этот проект медленнее, поскольку средств на его разработку гораздо меньше: он разрабатывался и по-прежнему поддерживается командой энтузиастов.

Кто пользуется даркнетом

Само по себе использование даркнета не обязательно и не всегда означает принадлежность к чему-то незаконному, там есть нейтральные по своей сути аналоги социальных сетей или форумы для общения. Все зависит от того, с ка-

кой целью туда заходит человек, что он там делает». Тем не менее наибольшую активность в даркнете развивают именно злоумышленники и хакеры.

Злоумышленники используют даркнет как средство коммуникации, а рядовые пользователи — как вариант обхода законодательных ограничений, но чтобы получить доступ к глубоко чувствительной информации, необходимо иметь учетную запись, подтвержденную другими участниками хакерского сообщества.

Разница между Глубокой паутиной, Поверхностной паутиной и Теневой Паутиной

Говоря об интернете, мы обычно имеем в виду только поверхностный веб. Все пользователи интернета могут легко получить доступ к этому разделу сети, и поисковые системы его индексируют. Именно там можно найти веб-сайты, платформы социальных сетей и интернет-магазины. Глубокий веб и теневой веб — это две разные области интернета, которые недоступны в дополнение к поверхностному вебу.

Часть интернета, не индексируемая поисковыми системами, называется «глубоким интернетом». К этой категории относятся личные профили в социальных сетях, интернет-банкинг и даже медицинские записи. Эти сайты можно посетить, имея соответствующие разрешения или учётные данные, даже если они закрыты для широкой публики.

С другой стороны, «теневая сеть» — гораздо более загадочная и опасная область. Она описывает часть интернета, которая намеренно скрыта и доступна только с помощью определённых программ или настроек. Здесь можно найти информацию о преступной деятельности, в том числе об услугах киллеров, торговле людьми и наркотиками. Посещение «теневого сети» не рекомендуется обычным пользователям интернета, поскольку это может быть опасно и незаконно.

Чаще всего многие путают между собой три относительных понятия: "Dark Internet/Dark Web", "Darknet" и "Deep Web", называя одно другим и наоборот. Чтобы избежать дальнейших недоразумений, следует навсегда запомнить, что к первому относятся устаревшие и ныне неиспользуемые приватные узлы обмена информацией, не подключенные к глобальной сети Интернета, как таковой. Наиболее известными экземплярами серверов таких машин являются две военных сети: "ARPANET" и его подразделение - "MILNET". Сама же аппаратная их часть сейчас либо хранится в засекреченных правительственных бункерах в виде реликвии прошлых лет, либо разобрана и вывезена на помойки.

"Даркнетом" именуют файлообменную сеть, соединение в которой производится между доверенными пользователями. Преимуществом подобного хранения веб-ресурсов является анонимная передача материала без возможности его перехвата посторонними лицами, так как трафик зашифрован от посторонних глаз. Некоторые анонимные сети используют эту технологию в качестве дополнительной, например, "Freenet", чтобы производить загрузку файлов сай-

та для их открытия со стороны клиента-получателя. В области "Deep Web" же различают два направления: не индексируемое поисковыми роботами (вебкраулерами) содержание вебсайтов (соответственно, "Surface Web" - наименование индексируемой части) и "Глубокий Веб" - ресурсы, зайти на которые можно, но исключительно при использовании софта, предназначенного для посещения анонимных сетей (Tor, I2P, Freenet и т.д.).

Deep Web "Невидимой" или "глубокой" сетью называют веб-контент, не индексируемый поисковыми системами, в основном по причине неактуальности сохранения настолько крупных баз данных на своих серверах. Проще говоря, боты, которых запускают корпорации вроде "Google", "Yandex" и "Yahoo" не имеют опции отслеживания и поиска определенных страниц, содержимое которых они не могут подобрать из-за ограничений их обладателя. Помимо столь очевидного определения, распространенного в широких кругах, под этим типом находок можно также подразумевать любую информацию, не подключенную к Интернету или существовавшую там незначительное время (в отличие от "Дарк Интернета", хранящуюся не на древних компьютерных аппаратах), своевременно исчезнувшей из общего доступа и доступной лишь тем, кто ею обладает.

Сравнительные категории:

- Не индексируемое по причинам:

1) Динамический контент на страницах или циклические переадресации. Примеры: формы заказов на онлайн-магазинах; введенные данные при регистрации; одноразовые страницы входа по пользовательскому логину и паролю; результаты поиска различных автономных механизмов.

2) Не распространяемый ботами или посетителями контент. Примеры: вебсайты, понятие о существовании которых имеют лишь "знающие люди": владельцы домена, отвечающие за хостинг, провайдер и члены команды (слова выше означают, что ссылкой на ресурс никто банально не делился где-либо, а сам он не пользуется популярностью у людей, соответственно, не требуем в запросах); IP-адреса с открытым 80 портом (наличие HTML-страницы/вебморды) и запрещающими индексацию средствами robots.txt или "noindex".

3) Закрытые и частные сервисы, возможно, ограничивающие просмотр техническим путем. Примеры: защищенные связкой логин-пароль/пароль/логин формы: роутеры; файловые и облачные хранилища (или FTP); URL для входа в админки или панели управления; потоки видеонаблюдения через камеры безопасности; всё прочее, начиная с датчиков температуры и давления, заканчивая дистанционным контролем над станком на фабричном заводе ЧПУ или сигнализацией в продовольственном магазине; чьи-то приватные схемы обмена посланиями; форумы по приглашениям; многое-многое другое, доступ к чему был ограничен инициативщиками. Попасть и проиндексировать подобное поисковик не может, так как не умеет вводить опознавательные слова (логин и пароль), да и не знает робот их.

- 4) Содержимое внутренних файлов, которое вебкраулеры еще не научи-

лись читать. Примеры: любой текст внутри видеозаписи родом, допустим, с "YouTube" или какой-нибудь 10 домашней страницы; изображения, лежащие на FTP-узлах и помещенные в расшаренные папки; слова песни, произносимые певцом напрямую (не опубликованные где-то библиотеки значений и текстов, а именно слова с трека, считанные напрямую); файлы из rar, zip или rgr архивов.

5) Удаленные авторами и ныне недоступные ресурсы, профили людей, опубликованные ими данные, оффлайн-копии которых не были сделаны. Примеры: любые отключенные за неуплату домены, удаленные по истечению срока хранения; файлы, опубликованные на обменниках; "уплывшие" треды на имиджбордах и залитые в них картинки; выпиленные администрацией видеохостингов записи из-за нарушения списка прав; потерянное и когда-то забытое.

6) Не индексируемое из-за неудобства и бесперспективности выдачи в результатах поиска. Примеры: многотысячные и многомиллионные базы научных и исследовательских учреждений, предназначенные для сотрудников; ежесекундно обновляемый и меняющийся контент (главные страницы на имиджбордах, BBS и форумах); whois-информация о доменах; стороны ресурсов на нестандартных портах или протоколах.

- Расположенное вне Сети:

1) Временные данные передач между одним хостом другому или появляющиеся в определенных областях на короткий промежуток времени. Примеры: файлы, переданные одним членом F2F-сети другому и более в ней не существующие; записи телефонных разговоров в мессенджерах; прогнозы погоды и показания со всевозможных приборов, не сохраненные в логи; журналы посещений доменных имен; самоуничтожающиеся почтовые или личные сообщения; информация, залитая на файлообменники под функцией "приватного обмена", в дальнейшем удаленная авторами.

2) Натуральный Даркнет, как он есть. Примеры: любые данные, никогда не бывавшие в Интернете и доступ через который, без приглашения и знания точного местоположения, к ним не получить (исключение составляют расшаренные папки на удаленных ПК); сети обмена знаниями и манипуляции между системой устройств, действующие и основанные на технологиях самописных протоколов.

Как получить доступ к Теневой паутине

Прежде чем мы расскажем, как попасть в теневой интернет, важно знать, что это небезопасное место. Посещение теневого интернета может подвергнуть вас и ваши устройства опасности, поскольку он фактически функционирует как чёрный рынок для незаконной деятельности.

Для доступа к теневому интернету необходимо специальное программное обеспечение. Самый популярный способ доступа к нему — через Tor (The Onion Router), бесплатный браузер, созданный для обеспечения анонимности и конфиденциальности.

Чтобы получить доступ к теневому интернету, необходимо скачать браузер Tor и следовать инструкциям по установке. После установки Tor вы можете посещать теневой интернет, вводя ссылки «.onion» в адресную строку браузера. Эти ссылки можно просматривать только через сеть Tor, и они не индексируются поисковыми системами.

Однако при использовании теневого интернета крайне важно соблюдать максимальную осторожность. Не раскрывайте личную информацию, не переходите по странным ссылкам и не скачивайте ничего, в чём вы не уверены. Чтобы лучше защитить свою личность и местоположение, лучше использовать VPN.

К сайтам даркнета можно получить доступ через URL-адрес в .onion

Сайты даркнета используют URL-адреса в формате .onion по нескольким причинам. Во-первых, .onion - это псевдодомен высокого уровня, специфичный для сети Tor. Это означает, что к этим сайтам можно получить доступ только через браузер Tor или другой сервис, совместимый с Tor.

Еще одно преимущество сайтов .onion - их анонимность. Сайты .onion работают с использованием шифрования прикладного уровня сетевой модели TCP/IP, что позволяет скрыть информацию о сервере, на котором находится сайт. Следовательно, пользователи могут получить доступ к этим сайтам без раскрытия их местоположения или личности.

Наконец, расширение .onion также позволяет сайтам скрываться от обычных поисковых систем. URL-адреса .onion не индексируются поисковыми системами, такими как Google, что делает эти сайты невидимыми, если вы не знаете точного URL-адреса.

Таким образом, использование URL-адреса в .onion обеспечивает сайтам даркнета дополнительный уровень защиты конфиденциальности и безопасности.

Опасности доступа к Теневой сети

Использование теневого интернета сопряжено с многочисленными рисками. Самый серьёзный риск заключается в раскрытии вашей личной информации. Поскольку теневой интернет не регулируется, там происходит множество незаконных действий. В теневом интернете хакеры и другие киберпреступники могут свободно действовать, постоянно выискивая уязвимых людей, которыми можно воспользоваться. Используя теневой интернет, вы непреднамеренно раскрываете себя этим людям, и они могут легко украсть вашу личную информацию, включая номера социального страхования, данные банковских счетов и информацию о ваших кредитных картах.

Возможность заражения вредоносным ПО — ещё один риск при использовании теневого интернета. Хорошо известно, что в теневом интернете можно найти вредоносное ПО, которое может серьёзно навредить вашему устройству и заразить его. Вредоносное ПО может похищать ваши личные данные, отслеживать ваше поведение в интернете и даже сделать ваше устройство бесполез-

ным. В определённых обстоятельствах вредоносное ПО может также взять под контроль ваше устройство и использовать его в качестве компонента ботнета для запуска других кибератак.

Наконец, использование теневого интернета может привести к юридическим проблемам. Как уже было сказано, теневой интернет служит центром многих преступных предприятий, в том числе по торговле нелегальными товарами, людьми и человеческими органами. Используя теневой интернет, вы непреднамеренно подвергаете себя риску и можете быть привлечены к ответственности за любые незаконные действия, в которых вы участвуете или которые поддерживаете.

Таким образом, использование теневой сети сопряжено с серьёзными опасностями, и его следует избегать любой ценой. Если вам необходимо войти в теневую сеть, убедитесь, что вы приняли все необходимые меры предосторожности для защиты себя и своей личной информации.

Контент Теневого Интернета

Часть интернета, известная как «теневая сеть», доступна только с помощью специализированного программного обеспечения, такого как браузер Tor, и не индексируется поисковыми системами. Контент, который можно найти в «теневой сети», разнообразен и часто спорный, включая всё — от политических акций и разоблачений до незаконных операций, таких как торговля наркотиками и оружием.

Сообщается, что в теневой сети также есть торговые площадки для продажи фальшивых денег, поддельных удостоверений личности и украденных данных. Однако только часть информации в теневой сети является незаконной. Многие люди используют теневую сеть для доступа к контенту, заблокированному или запрещённому в их странах, например к новостям о политике, правах человека, религиозных или культурных темах.

В теневом интернете можно найти эксклюзивные форумы и сообщества для людей с определёнными интересами, такими как хакерство, криптовалюты и выживание. Эти организации предоставляют площадку для обсуждения, обмена идеями и налаживания связей с теми, кто разделяет ваши интересы.

Важно помнить, что использование теневого интернета может быть опасным. Пользователям следует принимать необходимые меры предосторожности, чтобы защитить свою конфиденциальность и избежать противоправных действий.

Dark Web-сайты, которые стоит посетить

1. DuckDuck Go

Предпочтительная альтернатива Google в dark web. Эта частная поисковая система не отслеживает историю посещений и другие данные, а значит, предлагает персонализированные результаты поиска.

<https://duckduckgogg42xjoc72x3sjasowoarfbgcmvfihaftt6twagswzczad.onion/>

2. ProPublica

ProPublica - первый крупный новостной ресурс, у которого появилась dark web-версия. Присутствие этой некоммерческой организации, занимающейся журналистскими расследованиями, в Tor позволяет сохранять анонимность и обходить блокировки стран, а также способствует свободе слова.

<http://p53lf57qovuyvwscbхnrppply3vtqm7l6pcobkmyqsiofyezfnfu5uqd.onion/>

3. KeyBase

По своей функциональности Keybase похож на такие приложения для обмена сообщениями, как WhatsApp, и позволяет обмениваться файлами с друзьями и другими контактами. Ваши данные шифруются end-to-end с использованием криптографии с открытым ключом для обеспечения конфиденциальности и анонимности.

<http://keybase5wmilwokqirssclfnsqrjdsi7jdir5wy7y7iu3tanwmtп6oid.onion/>

4. Riseup

Безопасный сервис электронной почты, предназначенный в первую очередь для групп активистов. Этот сайт, управляемый добровольцами, не ведет записей о вашей деятельности, а также защищен от вредоносных атак и государственного вмешательства.

<http://vwvbybal4bd7szmgncyruucpgfkqahzddi37ktceo3ah7ngmcorpnyud.onion/>

5. Библиотека комиксов

Если вы фанат комиксов, то вам стоит заглянуть на этот сайт в Dark Web. Comic Book Library предоставляет доступ к тысячам комиксов различных жанров и изданий, а также позволяет скачивать их.

<http://nv3x2jozywh63fkohn5mwp2d73vasusjixn3im3ueof52fmbjsigw6ad.onion/>

6. Ahmia

Ahmia - это поисковая система, с помощью которой можно найти полезные сайты в dark web. Также с его помощью можно просматривать новости, информацию и статистику о сети Tor.

<http://juhanurmihxlp77nkq76byazcldy2hlmovfu2epvl5ankdibsot4csyd.onion/>

7. Императорская библиотека

Этот сайт называется Императорская библиотека; на нем можно скачать более 500 000 книг и статей, и это, возможно, одна из крупнейших электронных библиотек.

<https://kx5thpx2olielkihfyo4jgjqfb7zx7wxr3sd4xzt26ochei4m6f7tayd.onion/>

Риски при просмотре темной сети

Просмотр темной паутины часто сопряжен со многими рисками. Пришло время объяснить вам, как вы можете подвергнуть себя опасности, перейдя на определенные страницы темной паутины :

Незаконный контент: Darkweb часто служит местом публикации незаконных действий, таких как продажа наркотиков, оружия и пиратских материалов. Просматривая darkweb, вы можете непреднамеренно получить доступ к сайтам с нелегальным контентом.

Мошенничество: В darkweb существует множество фишинговых и мошеннических сайтов, которые пытаются украсть вашу личную информацию, банковские реквизиты или биткойны.

Атаки вредоносных программ: Киберпреступники могут размещать вредоносные программы на сайтах darkweb, чтобы заразить ваш компьютер. Эти вредоносные программы могут украсть вашу личную информацию, пароли или даже удаленно управлять вашим компьютером.

Уязвимости в системе безопасности: Darkweb не регулируется и не имеет действующих мер безопасности, которые можно найти в обычной сети. Таким образом, киберпреступникам может быть проще найти уязвимости в системе безопасности, которые можно использовать, и получить к ним доступ без их разрешения.

Кибератаки: Просматривая darkweb, вы можете стать целью кибератаки со стороны киберпреступников, которые хотят украсть вашу личную информацию или заразить ваш компьютер.

Если вы используете Tor, вы уменьшаете эти риски, но не устраняете их полностью. Не стесняйтесь также использовать VPN, чтобы повысить свою безопасность.

Роль теневой сети в незаконной деятельности

Помимо загадочности, теневая сеть — это пугающий и мрачный мир. Это идеальная платформа для незаконной деятельности благодаря анонимности и отсутствию регулирования. В теневой сети полно чёрных рынков, где люди могут покупать и продавать запрещённые товары и услуги, от наркотиков и оружия до краденых личных данных и информации о кредитных картах.

Кроме того, злоумышленники используют «теневой интернет» как площадку для торговли хакерскими инструментами, обмена информацией и нападения на ничего не подозревающих жертв. Количество киберпреступлений возросло из-за доступности новых и сложных вредоносных программ, программ-вымогателей и хакерских инструментов в «теновом интернете».

В 2013 году ФБР закрыло Silk Road — чёрный онлайн-рынок. Он стал одним из самых известных примеров незаконной деятельности в даркнете. Люди могли анонимно покупать и продавать наркотики, огнестрельное оружие и другие запрещённые товары с помощью криптовалюты на Silk Road.

Теневая сеть развивается с той же скоростью, что и Интернет. Она продолжает оставаться центром незаконной деятельности и рассадником киберпреступности. Крайне важно сохранять бдительность и защищаться от угроз теневой сети.

Этика доступа к Теневой сети

Доступ к теновому интернету сопряжён со значительными этическими проблемами, поскольку это странная и зачастую опасная среда. Из-за его связи с незаконной деятельностью, такой как торговля наркотиками, людьми и детская порнография, некоторые люди утверждают, что тенового интернета следует полностью избегать. Однако другие считают, что его можно использовать в

законных целях, например для расследования киберпреступлений и других незаконных действий.

Крайне важно учитывать любые потенциальные последствия использования теневого интернета. Ваша безопасность может оказаться под угрозой, а также вы можете столкнуться с юридическими последствиями. Доступ к теневому интернету во многих странах запрещён, и правоохранительные органы всегда следят за ним, чтобы задерживать людей, которые используют его в незаконных целях.

Кроме того, преступные группировки и хакеры, которые хотят атаковать вашу компьютерную систему, часто обитают в теневой сети. Вы рискуете поставить под угрозу свою компанию и себя, посещая теневую сеть.

Прежде чем выбрать «теневой интернет», следует тщательно взвесить все возможные риски и моральные последствия. Подумайте, есть ли другие, менее опасные способы достижения ваших целей, и сопоставьте потенциальные преимущества доступа к «теневому интернету» с рисками.

Анонимность и безопасность в даркнете

Само по себе посещение даркнета не считается правонарушением, однако, например, при покупке запрещенных товаров пользователь будет нести ответственность по закону. Участники сохраняют анонимность благодаря организации работы площадок (они не хранят логи, не отвечают на запросы правоохранительных органов, усложняют собственную инфраструктуру из соображений конспирации) и осторожности пользователей, которые включают VPN, не указывают личные данные и т. п.

Внутри даркнета не действуют законы каких-либо стран. Однако на каждой площадке администрация устанавливает собственные внутренние правила поведения и взаимодействия участников: за их соблюдением следят модераторы (как и на обычных форумах), добавил Колмаков. Для того чтобы сохранить анонимность участников какой-либо сделки, на площадках действует институт гарантов (третье лицо, авторитетный представитель площадки), споры в даркнете разрешаются в рамках арбитражных разбирательств.

Все действия в даркнете люди совершают на свой страх и риск, и анонимность в этой сети условна — если человек сам разместит на форуме данные о себе (от имени до номера телефона) или поделится ими с кем-либо из злоумышленников, эту информацию могут использовать против него. В даркнете владельцы своих ресурсов не особо заботятся о безопасности пользователей, в отличие от обычного интернета, поэтому пользователи даркнета более уязвимы перед фишинговым софтом, программами-вымогателями и различными шифровальщиками, которыми наполнены ресурсы даркнета.

Рекомендации по соблюдению кибергигиены.

1. Регулярно обновляйте Tor Browser: автообновление в браузере включено по умолчанию, однако зачастую обновления качаются слишком медленно, что оставляет окно возможностей для атакующих, эксплуатирующих регулярно выявляемые в Mozilla Firefox уязвимости.

2. Tor Browser по умолчанию сконфигурирован оптимальным образом, но можно дополнительно изменить настройки встроенного плагина NoScript для отключения JavaScript по умолчанию на всех сайтах, а также установить параметр «Уровни безопасности» (Security Levels) в значение «Самый безопасный» (Safest).

3. При подключении к Clearnet-сайтам через сеть Tor следует использовать только протокол HTTPS: не следует забывать, что выходная нода Tor-сети может контролироваться злоумышленниками под видом энтузиастов-волонтеров, а проходящий через неё незашифрованный HTTP-трафик - прослушиваться. В настройках Tor Browser можно установить режим "Только HTTPS" (HTTPS-Only).

4. Не размещайте свои персональные данные или чувствительную информацию в Darkweb: onion-сайты не контролируются никем, кроме их владельцев, поэтому добиться удаления информации в юридической плоскости будет невозможно.

5. Для обеспечения корпоративной сетевой безопасности следует контролировать или вовсе заблокировать любые соединения с сетью Tor - как исходящие, так и входящие (с IP-адресов выходных нод сети Tor, их перечень доступен и регулярно обновляется). Исходящие подключения к сети Tor могут означать, что в инфраструктуре компании активно ВПО, которое взаимодействует с C&C-сервером атакующих в сети Tor, а входящие соединения из Tor могут свидетельствовать либо о попытках скрытного анализа вашей инфраструктуры и поверхности потенциальной атаки, либо (особенно в случае входящих VPN/RDP-соединений) об использовании скомпрометированных учетных данных пользователей для несанкционированного доступа в корпоративную сеть.

6. Использование надежных и уникальных паролей

Один из лучших способов защитить себя и свою информацию — это использовать надежные и уникальные пароли для каждой учетной записи. Надежные пароли имеют длину не менее 16 символов и содержат заглавные и строчные буквы, цифры и символы. Чтобы максимально обезопасить свои учетные записи, убедитесь, что вы не используете повторно один и тот же пароль для нескольких учетных записей.

Самостоятельно придумать надежные пароли и запомнить их все практически невозможно. Мы рекомендуем использовать менеджер паролей, который поможет вам генерировать, управлять и безопасно хранить все ваши пароли, ключи доступа и данные. Благодаря менеджеру паролей единственный пароль, который вы должны запомнить, — это мастер-пароль.

7. Включите многофакторную аутентификацию в учетных записях

Многофакторная аутентификация (MFA) — это дополнительный уровень безопасности, который вы можете включить в своих учетных записях. MFA защищает вас в случае, если кому-то удастся получить доступ к вашим учетным данным, поскольку требует второго метода аутентификации, прежде чем они смогут успешно войти в систему.

8. Подпишитесь на службу мониторинга даркнета.

Мониторинг даркнета — это когда для сканирования даркнета на предмет вашей личной информации, такой как адрес электронной почты или учетные данные, используется инструмент. Это можно сделать вручную с помощью бесплатного сервиса, который не уведомляет вас, или автоматически с помощью инструмента, который обнаруживает и уведомляет вас, если ваши учетные данные продаются в даркнете. Инструмент мониторинга даркнета, который постоянно сканирует даркнет на предмет вашей личной информации, является лучшим вариантом для обеспечения безопасности вас и ваших данных, поскольку вы будете получать оповещения из даркнета и сможете немедленно принять меры, если ваши учетные данные или информация будут скомпрометированы.

9. Будьте в курсе последних новостей кибербезопасности

Чтобы знать о последних киберугрозах, жертвами которых становятся люди в Интернете, вам следует быть в курсе последних новостей по кибербезопасности. Это поможет вам узнать, на какие виды атак следует обращать внимание, когда вы просматриваете веб-страницы.

Заключение

По мере того, как мы приближаемся к исследованию таинственного мира Теневой Сети, важно понимать, что это место не для слабонервных. Это мрачный, опасный и зачастую запретный мир. Поэтому перед началом любых экскурсий по Теневой Сети необходимо принять необходимые меры безопасности.

Тем не менее, теневой интернет — интригующий сайт, несмотря на его риски. В этой анонимной среде люди могут свободно говорить, не беспокоясь о том, что за ними наблюдают или следят. Когда знания легкодоступны, любой человек в нашем обществе может найти всё, что ему нужно, включая запрещённые товары, оружие и услуги.

Однако «Теневая сеть» — это не просто убежище для мошенников. Это будущее, в котором активисты смогут объединяться и общаться, не беспокоясь о том, что за ними следят власти. В этом мире люди смогут выражать своё мнение, не опасаясь возмездия.

Как мы уже убедились, мир «Теневой паутины» сложен и динамичен. Путешествовать по планете, где так много неизведанных опасностей, непросто. Однако те, кто готов рискнуть, получают доступ к многочисленным возможностям.

Следует всегда помнить о том, что только некоторые люди могут находиться в теневой сети. Поэтому мы должны действовать ответственно и осторожно. Поэтому, если вы планируете исследовать теневую сеть, убедитесь, что делаете это безопасно и принимаете все необходимые меры предосторожности.

Теневая сеть загадочна и зачастую опасна, она не для робких. Важно понимать, что не всё, что вы читаете или видите в теневой сети, является законным или правдивым. Необходимо соблюдать осторожность при просмотре этой части Интернета и делать это только при наличии соответствующих мер безопасности. К числу передовых методов обеспечения кибербезопасности относятся:

- использование личного брандмауэра,
- использование виртуальной частной сети (VPN),
- наличие установленного на компьютере антивирусного программного обеспечения,
- регулярное обновление программного обеспечения, приложений и устройств,
- регулярное резервное копирование данных,
- проверка безопасности ссылок, прежде чем переходить по ним,
- осторожность с нежелательными вложениями,
- невыполнение запросов о предоставлении личной информации.

В заключение следует отметить, что, хотя развитие теневого интернета как центра незаконной деятельности запятнало его репутацию, его истоки восходят к необходимости в безопасной и анонимной коммуникации. Несомненно, теневой интернет жизненно важен для людей, которые хотят общаться или получать доступ к информации, не опасаясь цензуры или возмездия.

Список источников

1. Hatta, Masayuki (December 2020). "Deep web, dark web, dark net: A taxonomy of "hidden" Internet". *Annals of Business Administrative Science*. 19 (6): 277–292.
2. Lacson, Wesley; Jones, Beata (2016). "The 21st Century Darknet Market: Lessons From The Fall Of Silk Road" (PDF). *International Journal of Cyber Criminology*. 10: 40–61. doi:10.5281/zenodo.58521. Archived from the original (PDF) on 2020-12-12. Retrieved 2019-10-02.
3. "Ransomwares, divulgation de données et malware-as-a-service dans le Dark Web. Partie 1/2". Archived from the original on 2021-05-21.
4. "Ransomwares, divulgation de données et malware-as-a-service dans le Dark Web. Partie 2/2". Archived from the original on 2021-06-04.
5. "One Million Credit Cards Leaked in a Cybercrime Forum for Free". *Cyble*. August 8, 2021. Archived from the original on November 12, 2023. Retrieved August 9, 2023.
6. Attrino, Anthony G. (2020-12-22). "N.J. man charged with surfing 'Dark Web' to collect nearly 3K images of child porn, prosecutor says". *nj*. Archived from the original on 2021-04-21. Retrieved 2021-04-21.
7. Pagliery, Jose (March 10, 2014). "The Deep Web you don't know about". *CNN Business*. Archived from the original on March 3, 2021. Retrieved March 27, 2021.

УДК 62

ГЛАВА 15. КИБЕРБЕЗОПАСНОСТЬ. ХААS ПРЕОБРАЗОВАНИЕ ЦИФРОВОГО ЛАНДШАФТА

Аменицкий Алексей Владимирович

аспирант

Институт аспирантуры и докторантуры Университет Лобачевского Н.И.

Рухович Игорь Владимирович,**Аменицкая Любовь Алексеевна,****Аменицкий Дмитрий Александрович**

студенты магистратуры

НИУ ВШЭ

Аннотация: Четвёртая промышленная революция требует от предприятий гибкости, чтобы они могли адаптироваться к быстро меняющимся требованиям рынка. Предприятия внедряют ИТ-сервисы на основе ХааS, чтобы обеспечить устойчивость и гибкость, необходимые для получения конкурентного преимущества в отрасли.

«Всё как услуга» произвела революцию в бизнес-моделях, позволив получать надёжные услуги, которые помогают масштабироваться. Согласно недавнему отчёту, опубликованному Fortune Business Insights, в 2021 году мировой рынок ХааS оценивался в 436,82 миллиарда долларов США. Исследование также прогнозирует, что в период с 2022 по 2029 год размер рынка «всё как услуга» вырастет с 545,35 млрд долларов США до 2378,07 млрд долларов США со среднегодовым темпом роста 23,4%. Однако на таком процветающем рынке некоторым компаниям приходится нелегко, потому что ХааS стал сложным. В этой главе рассматриваются несколько проблем, с которыми сталкиваются предприятия в сфере бизнеса «всё как услуга».

Такси — это машина как сервис. Платишь только когда едешь. Не надо покупать автомобиль, тратить деньги на заправку и гараж, постоянно подкачивать шины. Не надо даже рулить, просто садишься — и через час ты на месте.

ИТ-услуги тоже могут оказываться по такой схеме. Когда клиент не несёт капитальных затрат, а платит только пока использует сервис. Например, писатель не устанавливает текстовый редактор на компьютер, а открывает его в браузере. Или компания не организует дата-центр, а арендует вычислительные мощности у облачного провайдера. В таком случае программа или инфраструктура предоставляются как сервис.

Для обозначения такой модели услуг принято определение ХааS или “всё как сервис” (Anything-as-a-service). Под него подпадают все услуги, которые оказываются через интернет и с применением облачных вычислений. "X" в этой аббревиатуре обозначает неизвестную переменную, как в уравнении. Если как сервис предоставляется инфраструктура, то вид услуг называется IaaS, если платформа для разработки — PaaS, если софт — SaaS.

Ключевые слова: Cyber Security (CS), CS architecture, CS trends, CS tendencies, CS tools, CS crimes, CS latest news, CS releases, CS game-changers, CS future, CS playbook, CS agenda, CS future, CS risks, CS incidents, CS resilience, Hackers, PenTest, CS прогноз, Artificial Intelligence, Deep Fakes, Эволюция киберУгроз, КиберГигиена

CYBERSECURITY. XAAS TRANSFORMATION OF THE DIGITAL LANDSCAPE

Amenitsky Alexey Vladimirovich,
Rukhovich Igor Vladimirovich,
Amenitskaya Lyubov Alekseevna,
Amenitsky Dmitry Alexandrovich

Цифровая трансформация происходит очень быстрыми темпами. За последние двадцать пять лет мы стали свидетелями развития компьютерных устройств хранения данных: от дискет до компакт-дисков, USB-накопителей и облачных хранилищ. Развитие не ограничивается только устройствами хранения данных. Технологии, продукты, услуги и способы работы постоянно совершенствуются. Самым последним и значительным таким изменением, возможно, стали облачные вычисления.

ХааS берет верх

В последнее десятилетие компании-разработчики программного обеспечения внедрили новый подход к получению прибыли — они используют облачные вычисления для продажи своего программного обеспечения как услуги (SaaS). Эта модель применяется не только в сфере программного обеспечения.

Компании из разных отраслей внедряют модель «как услуга», которая становится всё более популярной среди их клиентов. Почему? Конечные пользователи получают значительные преимущества от ХааS, в том числе экономию средств, гибкость и масштабируемость. Им больше не нужно вкладывать огромные средства в удовлетворение своих потребностей. Вместо этого они могут арендовать и масштабировать то, что им нужно, на гибкой основе.

Пользователям также нравятся различные варианты ценообразования, которые предлагает ХааS. Они могут платить в зависимости от использования, количества пользователей, ежемесячной подписки и т. д. Благодаря таким гибким вариантам поставщикам ХааS проще привлекать новых клиентов и выстраивать с ними более прочные отношения.

В 2023 году рынок «всего как услуги» достиг 683 миллиардов долларов. Глобальный рынок на этом он не остановится. К 2029 году, по прогнозам аналитиков, он достигнет ошеломляющих 2378 миллиардов долларов. Северная Америка лидирует в революции ХааS, занимая в 2023 году более 412 миллиардов долларов на мировом рынке, а Европа следует за ней по пятам. В обоих случаях лидируют ИТ-услуги.

Развитие различных отраслей с помощью модели ХааS.

Соответствие требованиям и управление

По мере того как предприятия по всему миру внедряют ХааS в свои бизнес-процессы, эти поставщики собирают, хранят и обрабатывают данные от всех клиентов по всем каналам. Внедрение «всего как услуги» в бизнес-процессы позволяет облачным сервисам получать, обрабатывать и анализиро-

вать огромные объёмы данных. Более того, данные собираются из множества источников и от заинтересованных сторон, у которых есть собственные правила управления данными. У поставщиков ХaaS также есть различные центры обработки данных в разных местах, что усложняет обеспечение соответствия требованиям к управлению данными.

Одной из наиболее серьёзных проблем является соблюдение различных противоречащих друг другу законов и нормативных актов, а также уязвимостей в сфере кибербезопасности, связанных с открытыми данными. Крайне важно разработать эффективные политики управления и соблюдения требований для обеспечения безопасности данных.

Определение оценки компании

Оценка бизнес-моделей облачных сервисов — очень сложная задача. Бизнес-модели ХaaS отличаются от традиционных моделей по ряду параметров. Поставщики ХaaS могут получать более регулярный доход, чем при единовременной покупке. Однако некоторым компаниям сложно поддерживать высокий уровень повторных продаж из-за плохого обслуживания клиентов. Бизнес-модели ХaaS также требуют более высоких затрат на обслуживание, которые приходится покрывать из собственных средств. У облачных компаний и бизнес-инвесторов есть собственные наборы оценочных моделей и критериев, по которым они оценивают возможности организации. При оценке облачных бизнес-моделей лица, принимающие решения, могут проанализировать показатели оттока клиентов, ценообразование, возможности перекрестных и дополнительных продаж, чтобы точно оценить бизнес-модель «все как услуга».

Привлечение, наем и удержание талантов

Сегодня поставщики облачных сервисов значительно расширили свою деятельность и усовершенствовали свои технологии, инструменты, процессы и операции, чтобы соответствовать требованиям рынка. По мере усложнения рынка компании сталкиваются со значительным дефицитом квалифицированных кадров. Технологические гиганты и стартапы-единороги с большим финансированием привлекают лучших специалистов, предлагая им больше возможностей, преимуществ и зарплат. Руководителям облачных предприятий следует задуматься о внедрении лучших методов найма, управления и удержания сотрудников.

Защита интеллектуальной собственности (ИС) и управление рисками

Поставщикам «всего как услуги» приходится преодолевать серьёзные трудности, связанные с различными факторами, такими как существующие конкуренты, гибкие стартапы и ведущие игроки отрасли, расширяющие свой общий целевой рынок. По мере того, как традиционные компании переходят на облачные решения, традиционные бизнес-модели вынуждены учитывать свои интеллектуальные усилия по разработке и внедрению технологий. Даже поставщики облачных решений подвержены тем же рискам, что и традиционные

предприятия, связанным с потерей интеллектуальной собственности. Многие успешные поставщики XaaS уже используют сложные патентные портфели для защиты своих прав на интеллектуальную собственность и эффективного управления различными рисками.

Истоки облачных вычислений

Можем ли мы вспомнить, как покупали компакт-диск MS Office для установки его приложений? Дело прошлого, о котором вспоминает поколение X, и над которым миллениалы могут посмеяться. Но это было до облачных вычислений, которые, возможно, поколение Y рассматривает как нечто принадлежащее своему поколению – ошибочную мысль.

Краеугольный камень нелокальных вычислений был заложен ещё в 1950 году, когда вычислительная техника была дорогостоящей. Поэтому в целях экономии компьютерные терминалы подключались к внутренней военной сети, чтобы сделать технологии доступными для нескольких человек в распределённой среде.

То, что тогда было военным мейнфреймом, быстро развивалось, и к 1996 году компания Compaq придумала термин для описания концепции распределённых вычислений — облачные вычисления.

Продвижение XaaS

XaaS (anything as a service, «всё как услуга») — это термин, обозначающий предоставление решений, приложений, продуктов, инструментов и технологий в виде услуг.

Большинство приложений XaaS имеют ИТ-компонент, разработанный в соответствии с моделью обслуживания, необходимой предприятию. В отличие от своих физических аналогов или аналогов, размещённых на месте, приложения XaaS обычно предоставляются в цифровом виде с помощью облачных вычислений по сети, подключённой к интернету.

XaaS — это общий термин, который охватывает множество различных типов ИТ-услуг, таких как SaaS (программное обеспечение как услуга),

PaaS (платформа как услуга) и IaaS (инфраструктура как услуга). Сегодня большинство крупных технологических компаний, таких как Microsoft™ Azure, Amazon Web Services (AWS), Google Cloud и IBM®, предлагают услуги XaaS. Предложения XaaS обладают высокой масштабируемостью, что позволяет поставщикам услуг предоставлять их на гибкой основе по мере необходимости, а не по более традиционной модели ценообразования.

Модели XaaS

По мере того, как технологии становились более доступными, всё больше персональных компьютеров подключалось к сети. В 1999 году компания Salesforce предложила свои приложения в онлайн-режиме, ознаменовав появление модели SaaS («программное обеспечение как услуга»). Идея прижилась, и почти всё, что только можно было представить, — продукты, инструменты,

технологии и т. д. — стало размещаться в облаке, что привело к появлению множества решений «aaS».

ХааS относится к модели предоставления услуг, которая использует облачную платформу, а не физический формат, и направлена на упрощение развёртывания и обеспечение быстрого доступа к услугам.

Существует множество примеров ХааS. Вот некоторые из них:

- Программное обеспечение как услуга (SaaS) — Salesforce
- Платформа как услуга (PaaS) — Azure, AWS Beanstalk
- Инфраструктура как услуга (IaaS) — AWS, облачные сервисы IBM
- База данных как услуга (DBaaS) — Oracle Database, Amazon Relational Database Services (RDS)
- Данные как услуга (DaaS) — Fairhair.ai
- АaaS (Аналитика как услуга) — Sisense, ScienceSoft

Различие между ХааS и SaaS

Хотя эти термины иногда используются как взаимозаменяемые из-за популярности многих SaaS-решений, ХааS и SaaS имеют разные значения. SaaS относится к продуктам ХааS в сфере программного обеспечения, в то время как ХааS включает в себя не только программное обеспечение. Некоторые примеры ХааS, которые не являются SaaS, включают PaaS и IaaS, не говоря уже о восстановлении после сбоев как услуге (DRaaS), базе данных как услуге (DBaaS) и многих других.

Значимость ХааS

Развитие облачных вычислений и распространение высокоскоростного доступа в интернет по всему миру превращают ХааS в основу многих успешных предприятий.

От 5G и периферийных вычислений до искусственного интеллекта (ИИ) и интернета вещей (IoT).

Требования к обработке корпоративных данных растут с каждым днём. Многие успешные компании теперь обращаются к облачным платформам и сервисам ХааS, которые помогают им достигать целей цифровой трансформации.

Эффективный подход к ХааS повышает производительность в критически важных областях искусственного интеллекта, больших данных и гибридного облака. Платформы ХааS объединяют эти возможности, позволяя предприятиям объединять данные в рамках гибридного облака и предоставлять передовые сервисы искусственного интеллекта, которые выделяют их на фоне конкурентов.

Ещё одним преимуществом надёжного подхода ХааS является то, что он даёт предприятиям возможность стратегически размещать наиболее важные сервисы. Например, SaaS, IaaS и PaaS, три распространённые категории продуктов ХааS, обычно размещаются в среде публичного облака. Однако некоторые предприятия предпочитают локальную облачную среду для большего кон-

троля. Надежная бизнес-модель ХааS даёт им возможность выбирать, какие сервисы размещать в локальном облаке, а какие — в публичном.

Пять корпоративных преимуществ ХааS

Основное преимущество ХааS для организаций — финансовое. До появления ХааS компаниям приходилось приобретать программное обеспечение, решения, услуги и продукты, необходимые для работы, за полную стоимость. Такой подход означал большие капиталовложения, зачастую без каких-либо гарантий, что услуга или решение будут работать так, как нужно.

Масштабируемая, гибкая модель ХааS с оплатой по факту использования позволяет предприятиям разных размеров и из разных отраслей экспериментировать с подходящими для них сервисами ХааS без больших первоначальных затрат. Помимо экономии средств, предприятия обычно получают и другие преимущества:

1. Рост инноваций: Подход ХааS к мультитенантному обслуживанию, при котором одно приложение обслуживает несколько пользователей, упрощает процесс внедрения новых сервисов и вывода из эксплуатации старых. Такая гибкость позволяет предприятиям с возможностями ХааS быстрее внедрять новые технологии и обеспечивает автоматизацию инфраструктуры по мере необходимости.

2. Удаленное развертывание: во время пандемии COVID-19 спрос на удаленные сервисы и решения резко возрос. ХааS, который предоставляется удаленно через интернет-сети и общедоступные и частные облачные среды, идеально подходил для помощи организациям. ХааS обеспечивал быструю удаленную реализацию приложений и сервисов, что помогало ИТ-отделам поддерживать непрерывность бизнес-процессов в трудное время. Когда пандемия пошла на спад, большинство организаций, использующих платформы ХааS, обнаружили, что они более эффективны, чем их старые бизнес-процессы, и сохранили их.

3. Сокращение ресурсов: Enterprise ХааS позволяет многим организациям сократить ресурсы, необходимые для работы их устаревшей ИТ-инфраструктуры. С увеличением количества рабочих нагрузок в облаке устаревшее оборудование, такое как локальные центры обработки данных, жесткие диски (HDD) и серверы, становится избыточным.

4. Повышение эффективности: перенос рабочих нагрузок в облако помогает организациям оптимизировать бизнес-процессы и сделать их более рентабельными. В облачной модели ИТ-специалисты могут быть переквалифицированы с обслуживания на более стратегически важные проекты и техническую поддержку. К распространенным ИТ-услугам, которые можно передать на аутсорсинг в рамках ХааS, относятся настройка, обновление и устранение неполадок.

5. Более быстрая цифровая трансформация: модели ХааS позволяют предприятиям быстро внедрять новые технологии и оставаться на передовой своих отраслей. Такое быстрое внедрение облачных сервисов в первую очередь ощущается в сфере ИТ, где повышенная масштабируемость ХааS позволяет пользо-

вателям быстрее получать доступ к новым технологиям через облако, упрощая путь к инновациям.

Проблемы, связанные с ХааS

Хотя преимущества для бизнеса от внедрения подхода ХааS неоспоримы, он также сопряжён с трудностями, о которых предприятиям необходимо знать.

1. Отказоустойчивость: поскольку все приложения, сервисы и решения в рамках ХааS зависят от облака и стабильного подключения к интернету, любые сбои в подключении могут вызвать проблемы.

2. Прозрачность: Предприятия, которые переносят свои основные возможности и сервисы в облако, не имеют полного представления о методах работы поставщиков и их инфраструктуре.

3. Зависимость: CSP и поставщики управляемых услуг (MSP), которые составляют основу моделей ХааS, могут быть приобретены, выйти из бизнеса или пострадать от ряда других сбоев, как и в любом другом бизнесе. Предприятия, выбирающие CSP или MSP, должны тщательно изучить их историю и надёжность, прежде чем соглашаться на какие-либо долгосрочные обязательства с ними.

4. Безопасность: Часто безопасность данных клиентов и пользовательских данных является главной заботой предприятий, переходящих на модель ХааS. Каждый день в новых заголовках подробно описываются проблемы кибербезопасности и утечки данных в ведущих компаниях. Если сторонний поставщик, такой как MSP или CSP, столкнется с нарушением безопасности, это может поставить под угрозу данные и репутацию своих клиентов.

Принцип работы ХааS

Чтобы эффективно внедрять возможности ХааS в своей организации, руководителям необходимо применять осознанный и вдумчивый подход. Сотрудники, которые годами выполняли свои задачи одним и тем же способом, часто сопротивляются изменениям, даже если понимают, что это выгодно для бизнеса. Предприятиям следует помнить, что ХааS лучше всего работает при поддержке пользователей, а это может потребовать времени и терпения.

Пошаговый подход, который могут использовать предприятия для эффективной реализации ХааS:

Определение цели

Прежде чем планировать внедрение ХааS, руководителям компаний следует обсудить это с заинтересованными сторонами и сформулировать, чего они надеются достичь. Цифровая трансформация, снижение затрат и повышение инновационности — вот некоторые распространённые примеры преимуществ, которые можно получить при внедрении ХааS.

Построение стратегии

Распространённая ошибка, которую допускают предприятия, стремящиеся

перейти на модель ХааS, — это попытка перенести всё в облако сразу. Некоторые инфраструктуры переносятся проще и быстрее, чем другие, и наличие продуманной стратегии для каждого сервиса, приложения или решения имеет решающее значение.

Подготовка заинтересованных сторон

Когда меняются критически важные сервисы и бизнес-процессы, это может повлиять на всех сотрудников компании. От клиентов и пользователей ваших продуктов и услуг до сотрудников, менеджеров и руководителей высшего звена — убедитесь, что все знают, как переход на ХааS повлияет на них. Если сотрудникам или клиентам требуется специальное обучение, убедитесь, что у них есть к нему доступ, а также к любым дополнительным ресурсам, которые могут понадобиться для работы в среде ХааS.

Правильный выбор -MSP (Managed Service Provider) или CSP (Cloud Service Provider)

Выбор подходящих поставщиков для внедрения ХааS, пожалуй, является самым важным шагом в этом процессе. При выборе поставщика убедитесь, что у него большой опыт внедрения и поддержки, особенно при развёртывании новой инфраструктуры, которая должна взаимодействовать с существующей инфраструктурой. Снижение рисков — ещё одна важная функция, на которую следует обратить внимание. Надежные поставщики ХааS должны быть хорошо знакомы с методами DRaaS и иметь протоколы резервного копирования данных.

Определение ключевых показателей эффективности

Как только наша платформа ХааS начнёт работать, нам понадобится чёткий способ измерения её производительности. Ключевые показатели эффективности (KPI) помогают оценить успешность внедрения ХааS. KPI могут включать в себя несколько ключевых преимуществ, которых вы ожидаете от ХааS, таких как снижение затрат, повышение эффективности и внедрение инноваций.

Примеры ХааS

ХааS — это широкий термин, который охватывает различные сервисы и решения, необходимые предприятиям для работы. Многие популярные сервисы и решения, от широко распространённого SaaS до менее известных контейнеров как сервиса (CaaS), поддерживают платформу ХааS.

Программное обеспечение как услуга (SaaS)

Программное обеспечение как услуга (SaaS) — это прикладное программное обеспечение, размещённое в облаке и используемое через интернет-соединение с помощью веб-браузера или мобильного приложения. Поставщики SaaS отвечают за эксплуатацию, управление и обслуживание приложений SaaS, а заказчик или клиент обычно подписывается на них на ежемесячной основе.

SaaS — это самый популярный и широко используемый сервис XaaS, примерами которого являются приложения, ежедневно используемые миллионами людей, такие как Zoom, Slack, Adobe Creative Cloud (ACM) и другие.

Инфраструктура как услуга (IaaS)

Инфраструктура как услуга (IaaS) — это форма облачных вычислений, которая предоставляет потребителям ресурсы ИТ-инфраструктуры, такие как вычислительные ресурсы, серверы, виртуальные машины, сети и хранилища, на основе подписки. IaaS невероятно популярна среди предприятий, которым нужна помощь в достижении целей цифровой трансформации, поскольку она позволяет легко увеличивать и уменьшать количество ресурсов. Некоторые из наиболее популярных вариантов использования IaaS включают резервное копирование и восстановление данных, веб-хостинг и внедрение гибридного мультиоблачного решения.

Платформа как услуга (PaaS)

PaaS — это модель облачных вычислений, которая предоставляет клиентам аппаратное обеспечение, программное обеспечение и инфраструктуру, необходимые для разработки, запуска и управления приложениями в облаке. Поставщики PaaS размещают необходимые серверы, сети, хранилища, базы данных, программное обеспечение и операционные системы (ОС) и позволяют клиентам использовать их за плату. Популярность PaaS среди современных предприятий во многом обусловлена тем, что PaaS позволяет клиентам создавать, тестировать, развёртывать, запускать, обновлять и масштабировать приложения быстрее и дешевле, чем если бы им приходилось создавать собственную локальную платформу и управлять ею.

База данных как услуга (DBaaS)

DBaaS, также известная как служба управляемой базы данных, представляет собой разновидность XaaS, которая позволяет пользователям получать доступ к облачной системе баз данных и использовать ее без покупки и настройки собственного оборудования или установки собственного программного обеспечения для баз данных. В модели DBaaS CSP заботится обо всем - от периодических обновлений до резервного копирования и обеспечения круглосуточной доступности и безопасности системы баз данных.

Контейнеры как услуга (CaaS)

CaaS — это тип XaaS, который позволяет разработчикам управлять контейнерными приложениями и разворачивать их, предоставляя компаниям любого размера доступ к переносимым и легко масштабируемым облачным решениям. Контейнерные приложения состоят из программного кода, упакованного только с библиотеками ОС и зависимостями, необходимыми для его запуска. Это гибкие исполняемые модули, которые могут работать практически в любой

ИТ-инфраструктуре.

Настольный компьютер как услуга (DaaS)

«Рабочий стол как услуга» (DaaS) — это способ предоставления пользователям полных виртуальных рабочих сред, включая операционную систему, приложения, файлы и пользовательские настройки из облака. В этой модели XaaS рабочие столы работают на виртуальных машинах, которые размещаются в вычислительной, сетевой и инфраструктуре хранения данных, управляемых поставщиком облачных услуг.

Функция как услуга (FaaS)

Функция как услуга (FaaS) — это сервис облачных вычислений, который позволяет клиентам запускать код в ответ на события, не управляя сложной инфраструктурой, которая обычно требуется для создания и запуска микросервисных приложений. Для размещения программного приложения в интернете обычно требуется подготовка и управление виртуальным или физическим сервером. При использовании FaaS физическое оборудование, операционная система виртуальной машины и управление программным обеспечением веб-сервера автоматически обрабатываются поставщиком облачных услуг.

Хранилище как услуга (STaaS)

Хранилище как услуга (STaaS) — это управляемый сервис, в рамках которого клиенты приобретают доступ к платформе хранения данных, такой как Dropbox, Google Диск или iCloud. STaaS часто предоставляется в публичном облаке по модели подписки с оплатой по факту использования, но может быть приобретён одним клиентом и настроен как локальная среда.

5 отраслей, максимально использующих XaaS

1. Программное обеспечение как услуга (SaaS)

На ИТ-отрасль приходится основная часть примеров XaaS. Из них SaaS занимает лидирующие позиции. Когда мы говорим, что SaaS стала первопроходцем в этой модели, мы имеем в виду именно это. По прогнозам, в 2025 году глобальные расходы на SaaS вырастут на 18% и составят 385 миллиардов долларов.

Пример SaaS: специалист по CRM и программному обеспечению для продаж Salesforce получает основную часть своих доходов за счет облачной модели подписки. Предприятия могут выбирать из множества интегрированных сервисов, которые входят в их облака продаж, сервиса или маркетинга. По прогнозам, в 2025 году мировые расходы на общедоступные облачные сервисы вырастут на 20% и составят больше 900 миллиардов долларов.

2. Хранение как услуга (STaaS)

Поскольку объём корпоративных данных продолжает расти, компании ча-

сто предпочитают хранить свои данные у третьей стороны, что называется «хранилище как услуга». Это позволяет им экономить на оборудовании, программном обеспечении и ИТ-персонале и гибко платить только за то, что они используют. Аналитики прогнозируют, что к 2027 году рынок STaaS будет оцениваться в 49,5 миллиардов долларов.

Пример STaaS: миллионы клиентов используют Amazon Web Services (AWS) для хранения своих бизнес-данных. Например, с помощью продукта Amazon S3 клиенты платят в зависимости от того, сколько данных они хранят и как часто им нужен к ним доступ.

3. Устройства как услуга (DVaaS)

В модели «устройства как услуга» компании предлагают смартфоны, ПК и другие вычислительные устройства, а также другие виды оборудования в качестве услуги. Это снижает затраты и повышает гибкость для клиентов, а поставщики DaaS получают доход от новых услуг и более предсказуемый поток доходов. В 2015 году ни один производитель ПК не предлагал DaaS в качестве опции, но к 2019 году, по данным Accenture, этот показатель вырос до 65% среди производителей ПК.

Пример DaaS: Hewlett Packard — один из многих поставщиков DaaS, предлагающих программу жизненного цикла для различных аппаратных устройств. Компании платят ежемесячную плату за получение необходимого оборудования (например, ноутбуков), а также за услуги по ремонту и аналитику на основе ИИ.

4. Склад как услуга (WaaS)

Компании, предоставляющие складские услуги, предлагают хранение и доставку по требованию для предприятий электронной коммерции. В рамках модели «склад как услуга» компании предлагают услуги по хранению, упаковке и доставке товаров по требованию для предприятий электронной коммерции и логистики. WaaS используется компаниями, которые хотят повысить свою гибкость, быстрее расширяться и повышать производительность. Стоимость зависит от нескольких факторов, таких как количество хранимых и обрабатываемых товаров, количество отработанных часов и размер хранилища.

Пример WaaS: ShipBob хранит товары для небольших и средних компаний, занимающихся электронной коммерцией, и предоставляет им все необходимые услуги. Платформа ShipBob также использует искусственный интеллект для автоматического выбора наиболее оптимального центра выполнения заказов.

5. Транспортные средства как услуга (также известные как car as a service)

В последние годы автомобильные компании внедрили модели по подписке. При таком типе обслуживания пользователи могут переключаться на разные автомобили в рамках одной подписки, и нет долгосрочных обязательств, как при традиционной аренде. По данным Technavio, с 2020 по 2025 год доля рынка

«автомобиль как услуга» вырастет на 187 миллиардов долларов.

Пример «автомобиль как услуга»: с пакетом «Care by Volvo» от Volvo водители платят ежемесячную плату за свой автомобиль, а также за техническое обслуживание, страховку и услуги консьержа. Клиенты получают 30-дневный возобновляемый контракт без обязательств по продлению.

Реализация ХааS

Внедрение платформ ХааS требует планирования и разработки стратегии, чтобы руководители компаний могли убедиться, что их организации и сотрудники готовы к внедрению ХааS. Для этого необходимо выполнить следующие действия:

- Определите цели. Четко сформулируйте бизнес-требования, которые могут удовлетворить платформы ХааS, и степень их влияния на работу.
- Разработайте стратегию миграции. Вполне вероятно, что некоторые внутренние процессы будут перенесены к поставщику ХааS. Комплексная стратегия миграции, учитывающая потенциальные препятствия, обеспечит плавный переход.
- Обучите сотрудников. Сотрудники должны быть в курсе событий и обладать навыками, необходимыми для участия в миграции и последующем использовании инструментов ХааS.
- Общайтесь с заинтересованными сторонами. Необходимо информировать заинтересованные стороны, чтобы они были готовы к переходу на ХааS. Этот переход может оказать значительное влияние на организацию.
- Определите подходящих поставщиков услуг. При выборе поставщиков ХааS важно учитывать такие факторы, как простота интеграции их платформ с существующей инфраструктурой, а также соглашения об уровне обслуживания и возможности аварийного восстановления.
- Измерение производительности. Первым шагом в процессе непрерывного мониторинга производительности является определение критериев и показателей, которые будут использоваться для оценки успешности ХааS.
- Снижайте риски. После полной реализации систем ХааS разработайте планы по упреждающему снижению рисков и устранению простоев, вызванных такими проблемами, как перебои в подаче электроэнергии.

Будущий рынок ХааS

Сочетание облачных вычислений и повсеместного доступа в интернет с высокой пропускной способностью по всему миру способствует росту ХааS. По мнению поставщиков и исследователей, ХааS продолжит расти по мере того, как клиенты будут переносить все больше рабочих нагрузок в облако. Согласно отчету Fortune Business Insight, в 2030 году рынок ХааS вырастет до 3,2 триллиона долларов с 700 миллиардов долларов в 2023 году.

Некоторые организации не решаются внедрять ХааS из-за проблем с ки-

бербезопасностью, соблюдением нормативных требований и управлением. Однако поставщики услуг всё чаще решают эти проблемы.

Конвергенция 5G, периферийных вычислений, больших данных, искусственного интеллекта, автоматизации, машинного обучения и Интернета вещей способствовала развитию модели ХааS и облачных технологий в целом. По мере того как компаниям требуется обрабатывать всё больше информации, становится менее экономически целесообразным размещать вычислительные сервисы локально. Это привело к тому, что многие стали использовать облачные платформы в рамках цифровой трансформации.

Одним из видов ХааS, популярность которого возросла в последние годы, является резервное копирование как услуга.

Будущее за гибкими моделями потребления

Модели «как услуга» продолжают набирать популярность. Но чтобы получить от них максимальную отдачу, необходимо учитывать важный момент: возможность отслеживать, как клиенты используют ваши услуги. Эта информация имеет решающее значение для управления доходами и качеством обслуживания клиентов.

Новые тенденции в ХааS

Специализированные и профильные (нишевые) ХааS

По мере насыщения рынка поставщики, скорее всего, будут выделяться на фоне конкурентов, ориентируясь на конкретные отрасли или сценарии использования и предлагая индивидуальные услуги для удовлетворения конкретных потребностей клиентов.

Интеграция искусственного интеллекта, ML и интернета вещей

Интеграция новых технологий, таких как искусственный интеллект (ИИ), машинное обучение (МО) и Интернет вещей (IoT), формирует будущее ХааS. Эти технологии расширяют возможности и функциональность решений ХааS, обеспечивая более персонализированные и интеллектуальные сервисы.

Гибридный ХааS

Ожидается, что ХааS приведёт к распространению гибридных моделей, сочетающих локальные и облачные сервисы. Такой подход позволяет компаниям сохранять гибкость и контроль, используя преимущества ХааS.

Заключение.

ХааS - это новая парадигма цифровой трансформации, и ее будущее выглядит многообещающим благодаря глобальной доступности интернета с высокой пропускной способностью и платформ облачных вычислений. Исследование Persistence прогнозирует рост компании с 5 млрд долларов США в 2020 году до колоссальных 97 млрд долларов США в 2031 году при ожидаемом CAGR (совокупном годовом темпе роста) в 12,5%. ХааS является движущей силой се-

годняшних цифровых преобразований и привлекает клиентов, которые пожидают их плоды. Вы готовы присоединиться к ним?

Для организаций, находящихся на пути цифровой трансформации, гибкость является ключевым фактором в реагировании на быстро меняющиеся технологии и бизнес-среду. Сейчас, как никогда ранее, важно оправдывать и превосходить ожидания организаций с помощью надёжного цифрового мышления, подкреплённого инновациями. Возможность для компаний чувствовать, учиться, реагировать и развиваться как живой организм станет залогом успеха в будущем. Комплексный, но при этом модульный набор услуг делает именно это. Новые платформы позволяют организациям автоматически принимать интуитивно понятные решения в больших масштабах, получать полезную информацию на основе решений в реальном времени, работать в любое время и в любом месте, а также получать подробные данные по всем функциям, что приводит к сверхпроизводительности. Новые решения позволяют создавать взаимосвязанные организации, которые совместно внедряют инновации для будущего.

Список источников

1. McHaney, Roger (2021). *Cloud technologies: an overview of cloud computing technologies for managers*. Hoboken, NJ. ISBN 978-1-119-76951-4. OCLC 1196822611.
2. Linkin, Peter (2022). *Data Management as a Service for Dummies* (PDF). John Wiley & Sons, Inc. ISBN 978-1-119-87093-7.
3. Basta, Alfred; Basta, Nadine; Anwar, Waqar (2024). *Pen Testing from Contract to Report*. John Wiley & Sons. p. 334. ISBN 978-1-394-17680-9.
4. "Exploit-as-a-service: Cybercriminals exploring potential of leasing out zero-day vulnerabilities". 16 November 2021. Archived from the original on 2021-11-23.
5. Brunette, B. (7 March 2017). "Lighting as a Service: A New Model for Energy Efficiency" (PDF). *ecoengineering.com*. Eco Engineering. Retrieved 8 July 2020.
6. Guidehouse Insights. "Market Data: Lighting as a Service". *guidehouseinsights.com*. Guidehouse Insights. Retrieved 8 July 2020.
7. Smith, Göran. "Making Mobility-as-a-Service: Towards Governance Principles and Pathways". Retrieved 2020-09-25.
8. Mladenović, Miloš N. (2021). "Mobility as a Service". *International Encyclopedia of Transportation*. pp. 12–18. doi:10.1016/B978-0-08-102671-7.10607-4. ISBN 978-0-08-102672-4. S2CID 242133419.
9. Hudson, Caroline (January 26, 2022). "CEO at local fintech firm talks 'generosity trend,' what's next for 2022". *www.bizjournals.com*. Retrieved 15 March 2022.

Авторский коллектив

*Азарян Е.М., Аменицкая Л.А., Аменицкий А.В., Аменицкий Д.А., Блиничкина Н.Ю., Бузни А.Н.,
Воликов В.В., Гаврилов В.А., Грабков Ю.П., Дерябин Н.И., Зайналов Ж.Р., Кудрявцева Н.А.,
Матевосова Е.К., Маторина О.С., Рухович И.В., Тарасов А.В., Удавцова Е.Ю.,
Халаимова В.И., Хачатурян Э.В., Четкин А.В.*



НАУЧНОЕ ИЗДАНИЕ
НОВЫЕ НАУЧНЫЕ ИССЛЕДОВАНИЯ И
ТЕХНОЛОГИИ: АКТУАЛЬНЫЕ ВОПРОСЫ,
ДОСТИЖЕНИЯ И ИННОВАЦИИ

Монография

Под общей редакцией

кандидата экономических наук Г. Ю. Гуляева

Подписано в печать 12.12.2024.

Формат 60×84 1/16. Усл. печ. л. 12,4

Тираж 500 экз.

МЦНС «Наука и Просвещение»

440062, г. Пенза, Проспект Строителей д. 88, оф. 10

www.naukaip.ru

ISBN 978-5-00236-641-5



9 785002 366415 >

Уважаемые коллеги!

Приглашаем Вас принять участие в Международных научно-практических конференциях!

| Дата | Название конференции | Услуга | Шифр |
|-----------|--|-----------------------|---------|
| 8 января | XV Международная научно-практическая конференция АКТУАЛЬНЫЕ ВОПРОСЫ СОВРЕМЕННЫХ НАУЧНЫХ ИССЛЕДОВАНИЙ | 120 руб. за 1 стр. | МК-2224 |
| 8 января | II Международная научно-практическая конференция СОВРЕМЕННОЕ ОБЩЕСТВО, НАУКА И ОБРАЗОВАНИЕ: АКТУАЛЬНЫЕ ВОПРОСЫ, ДОСТИЖЕНИЯ И ИННОВАЦИИ | 120 руб. за 1 стр. | МК-2225 |
| 8 января | Международная научно-практическая конференция НАУКА И МОЛОДЫЕ УЧЁНЫЕ | 120 руб. за 1 стр. | МК-2226 |
| 10 января | II Международная научно-практическая конференция АКТУАЛЬНЫЕ ВОПРОСЫ НАУКИ, ОБЩЕСТВА И ОБРАЗОВАНИЯ | 120 руб. за 1 стр. | МК-2227 |
| 10 января | XV Международная научно-практическая конференция НАУЧНОЕ ОБОЗРЕНИЕ: АКТУАЛЬНЫЕ ВОПРОСЫ ТЕОРИИ И ПРАКТИКИ | 120 руб. за 1 стр. | МК-2228 |
| 10 января | XXIII Международная научно-практическая конференция СТУДЕНЧЕСКИЕ НАУЧНЫЕ ИССЛЕДОВАНИЯ | 120 руб. за 1 стр. | МК-2229 |
| 15 января | VI Международная научно-практическая конференция АКТУАЛЬНЫЕ ВОПРОСЫ НАУКИ 2025 | 120 руб. за 1 стр. | МК-2230 |
| 15 января | XII Международная научно-практическая конференция НАУКА, ИННОВАЦИИ, ОБРАЗОВАНИЕ: АКТУАЛЬНЫЕ ВОПРОСЫ XXI ВЕКА | 120 руб. за 1 стр. | МК-2231 |
| 15 января | XI Международная научно-практическая конференция МОЛОДОЙ УЧЁНЫЙ | 120 руб. за 1 стр. | МК-2232 |
| 15 января | X Международная научно-практическая конференция ЭКОНОМИКА, ФИНАНСЫ И УПРАВЛЕНИЕ: АКТУАЛЬНЫЕ ВОПРОСЫ ТЕОРИИ И ПРАКТИКИ | 120 руб. за 1 стр. | МК-2233 |
| 15 января | VII Международная научно-практическая конференция ОБРАЗОВАНИЕ, ОБУЧЕНИЕ И ВОСПИТАНИЕ: АКТУАЛЬНЫЕ ВОПРОСЫ ТЕОРИИ И ПРАКТИКИ | 120 руб. за 1 стр. | МК-2234 |
| 15 января | VII Международная научно-практическая конференция ЮРИСПРУДЕНЦИЯ, ЗАКОН И ПОРЯДОК: АКТУАЛЬНЫЕ ВОПРОСЫ ТЕОРИИ И ПРАКТИКИ | 120 руб. за 1 стр. | МК-2235 |
| 17 января | XV Международная научно-практическая конференция СТУДЕНЧЕСКИЙ НАУЧНЫЙ ФОРУМ 2025 | 120 руб. за 1 стр. | МК-2236 |
| 17 января | VI Международная научно-практическая конференция НАУКА, ОБЩЕСТВО, ИННОВАЦИИ: АКТУАЛЬНЫЕ ВОПРОСЫ СОВРЕМЕННЫХ ИССЛЕДОВАНИЙ | 120 руб. за 1 стр. | МК-2237 |
| 17 января | II Международная научно-практическая конференция EURASIAN RESEARCH | 120 руб. за 1 стр. | МК-2238 |
| 20 января | XIX Международная научно-практическая конференция АКТУАЛЬНЫЕ ВОПРОСЫ СОВРЕМЕННОЙ НАУКИ | 120 руб. за 1 стр. | МК-2239 |
| 20 января | IV Международная научно-практическая конференция НАУКА, ТЕХНОЛОГИИ, ОБРАЗОВАНИЕ: АКТУАЛЬНЫЕ ВОПРОСЫ, ДОСТИЖЕНИЯ И ИННОВАЦИИ | 120 руб. за 1 стр. | МК-2240 |
| 20 января | XXIX Международная научно-практическая конференция НАУЧНЫЕ ИССЛЕДОВАНИЯ МОЛОДЫХ УЧЁНЫХ | 120 руб. за 1 стр. | МК-2241 |
| 23 января | XI Международная научно-практическая конференция НАУЧНЫЙ ФОРУМ | 120 руб. за 1 стр. | МК-2242 |

www.naukaip.ru