DOI: 10.17803/1729-5920.2024.216.11.145-158

В. Д. Никишин
Московский государственный юридический
университет имени О.Е. Кутафина (МГЮА)
г. Москва, Российская Федерация

Правовое обеспечение медиабезопасности и когнитивного суверенитета: вызовы социальной инженерии, гибридных войн и механизмов Web 3.0 (часть 1)

Резюме. В статье рассмотрены основные технологии (в том числе социогуманитарные), выступающие вызовами для обеспечения безопасности коммуникации в интернет-среде и требующие выработки новых нормативных моделей. Рассмотрены соотношение и взаимосвязи концептов информационной, информационно-психологической, репутационной и медиабезопасности; информационного и когнитивного суверенитета; информационной, когнитивной и гибридной войны; феномена «мягкой силы», «социологической пропаганды», что имеет важное значение для унификации терминологического аппарата в указанной сфере. Впервые с точки зрения юриспруденции комплексно рассмотрен концепт когнитивного суверенитета и охарактеризованы его составляющие, в том числе медиабезопасность, культурный суверенитет, технологический суверенитет, управленческий суверенитет, правовая безопасность. Новизной обладает и раздел исследования, посвященный комплексному рассмотрению феномена социальной инженерии не только как совокупности методов психологического воздействия, направленного на получение неправомерного доступа к данным, но и как иных комплексов социогуманитарных технологий управления смыслами, методов и приемов информационно-психологического воздействия на поведение людей. Рассмотрено место юридической социальной инженерии в системе социальной инженерии и обоснована роль юриста-стратега (юриста-правотворца) как социального инженера, разрабатывающего модели нормирования не только текущих, но и зарождающихся, прогнозируемых общественных отношений. Анализ развития киберпространства с точки зрения концепции «Web 1.0 — Web 2.0 — Web 3.0 — Web 3» позволил, во-первых, выработать авторскую признаковую модель различных «типов» (этапов) развития интернет-среды и, во-вторых, обозначить вызовы праву, обусловленные необходимостью обеспечения медиабезопасности и когнитивного суверенитета, а также адаптации новых экономических моделей.

Ключевые слова: социогуманитарные технологии; информационная безопасность; репутационная безопасность; медиабезопасность; информационный суверенитет; когнитивный суверенитет; информационная война; гибридная война; цифровое право

Для цитирования: Никишин В. Д. Правовое обеспечение медиабезопасности и когнитивного суверенитета: вызовы социальной инженерии, гибридных войн и механизмов Web 3.0 (часть 1). *Lex russica.* 2024. Т. 77. № 11. С. 145–158. DOI: 10.17803/1729-5920.2024.216.11.145-158

Благодарности. Исследование выполнено в рамках реализации проекта «Когнитивный суверенитет и медиабезопасность: право, психология и IT» Университета имени О.Е. Кутафина (МГЮА) программы стратегического академического лидерства «Приоритет-2030» (Центр компетенций «Социоправо»).

Legal Support of Media Security and Cognitive Sovereignty: Challenges of Social Engineering, Hybrid Wars and Web 3.0 Mechanisms (Part 1)

Vladimir D. Nikishin
Kutafin Moscow State Law University (MSAL)
Moscow, Russian Federation

Abstract. The paper considers the main technologies (including socio-humanitarian ones) that pose challenges to ensure the security of communication in the Internet environment and require the development of new regulatory models. The correlation and interrelationships of the concepts of information, information-psychological, reputational and media security; information and cognitive sovereignty; information, cognitive and hybrid warfare; the phenomenon of «soft power», «sociological propaganda», which is important for the unification of the terminological apparatus in this area, are considered. For the first time, from the point of view of jurisprudence, the concept of cognitive sovereignty is comprehensively considered and its components are characterized, including media security, cultural sovereignty, technological sovereignty, managerial sovereignty, and legal security. The research section devoted to the comprehensive consideration of the phenomenon of social engineering is also new, not only as a set of methods of psychological influence aimed at obtaining unauthorized access to data, but also as other complexes of socio-humanitarian technologies for managing meanings, methods and techniques of information and psychological influence on human behavior. The place of legal social engineering in the system of social engineering is considered and the role of the lawyer-strategist (lawyer-lawmaker) is justified as a social engineer who develops models for rationing not only current, but also emerging, predictable social relations. An analysis of the development of cyberspace from the point of view of the concept «Web 1.0 — Web 2.0 — Web 3.0 — Web 3» made it possible, firstly, to develop an author's feature model of various «types» (stages) of the development of the Internet environment and, secondly, to identify challenges to the law caused by the need to ensure media security and cognitive sovereignty, and also the adaptation of new economic models.
Keywords: socio-humanistic technologies; information security; reputational security; media security; information sovereignty; cognitive sovereignty; information warfare; hybrid warfare; digital law
Cite as: Nikishin VD. Legal Support of Media Security and Cognitive Sovereignty: Challenges of Social Engineering, Hybrid Wars and Web 3.0 Mechanisms (Part 1). *Lex russica.* 2024;77(11):145-158. (In Russ.). DOI: 10.17803/1729-5920.2024.216.11.145-158

Acknowledgements. The research was carried out as part of the project «Cognitive Sovereignty and Media Security: Law, Psychology and IT», Kutafin Moscow State Law University (MSAL), strategic academic leadership program «Priority-2030» (Competence Center «Sociopravo»).

Введение

Подлежащие правовому регулированию отношения в настоящий момент представляют собой в значительной степени отношения внутри социотехнических систем и между ними. Это общественные отношения, «отягощенные» нечеловеческой квазисубъектностью (в терминологии Г. Хассельбальх — «нечеловеческой (nonhuman) агентностью»[1]) и развивающиеся в соответствии с логикой сетевых структур[2].
Имеет место искусственная социальность, подразумевающая «эмпирический факт участия агентов ИИ в социальных взаимодействиях в качестве активных посредников или участников этих взаимодействий»[3]; Интернет рассматрива-

[1] *Hasselbalch G.* Data Ethics of Power: A Human Approach in the Big data and AI Era. Cheltenham; Northampton. MA : Edward Elgar, 2021.

[2] *Кастельс М.* Галактика Интернет: Размышления об Интернете, бизнесе и обществе. Екатеринбург : У-Фактория, 2004.

[3] *Резаев А. В., Трегубова Н. Д.* «Искусственный интеллект», «онлайн-культура», «искусственная социальность»: определение понятий // Мониторинг общественного мнения: Экономические и социальные перемены. 2019. № 6. С. 43.

ется в парадигме «глобальной архитектуры по изменению поведения»[4], что позволяет исследователям говорить и о «цифровом тоталитаризме»[5].

Переход к «экономике внимания» (attention economy), переориентация мировой экономики с финансовых транзакций на «транзакции внимания»[6] подразумевает активное использование не только мультимедийных технологий, но и когнитивных и преаттентивных («предшествующих вниманию») технологий, которые «помогают организовать процессы восприятия на дорациональном, фактически бессознательном уровне»[7].

Интернет стал мощнейшим инструментом манипулятивного воздействия на всех без исключения пользователей, средой проведения широкомасштабных психологических операций, что диктует новые вызовы правовому обеспечению цифрового «иммунитета», информационной безопасности как отдельно взятых интернет-пользователей, так и общества и государства в целом.

1. Информационная, информационно-психологическая, репутационная и медиабезопасность, информационный и когнитивный суверенитет: соотношение концептов

В Доктрине информационной безопасности Российской Федерации[8] под информационной безопасностью Российской Федерации понимается «состояние защищенности *личности*, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются *реализация конституционных прав и свобод человека и гражданина*, достойные качество и уровень жизни граждан, *суверенитет,* территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства».

Информационная безопасность может рассматриваться, во-первых, в информационно-техническом аспекте как безопасность данных (персональных данных; государственной, коммерческой тайны и т.д.) и объектов информационной инфраструктуры (информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления и т.д.) и, во-вторых, в информационно-психологическом аспекте как защита от (деструктивной, токсичной) информации.

Информационно-психологическая (информационно-мировоззренческая) безопасность личности — состояние защищенности человека, при котором отсутствуют контентные и коммуникационные риски, связанные с причинением информацией вреда его здоровью и (или) физическому, психическому, духовному, нравственному развитию.

Информационно-психологическая безопасность предполагает защиту от манипулирования сознанием личности, насаждения симулякров и формирования, соответственно, псевдореальности, картины мира с искаженными или подмененными ценностями, установками и т.д., где во главу угла ставится культ агрессии к окружающим (собственно агрессивный дискурс) или к себе самому (депрессивно-аутодеструктивный дискурс).

Понятие ***«медиабезопасность»***, в своей семантике подчеркивая источник угроз — ме-

---

4 *Noor E.* Rethinking Decoupling: Interdependence, Dependence, Independence // Digital Debates: CyFy Journal. 2020. P. 36–46.

5 *Нечаев В. Д., Белоконев С. Ю.* Цифровая экономика и тенденции политического развития современных обществ // Контуры глобальных трансформаций: политика, экономика, право. 2020. Т. 13. № 2. С. 112–133. URL: https://doi.org/10.23932/2542-0240-2020-13-2-6 (дата обращения: 14.05.2024).

6 *Goldhaber M. H.* Principles of the new economy // URL: https://people.well.com/user/mgoldh/principles.html (дата обращения: 14.05.2024).

7 *Сарна А. Я.* Технологии воздействия на аудиторию в современном медиапространстве // Вестник Санкт-Петербургского университета. Социология. 2020. Т. 13. Вып. 2. С. 220.

8 Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ РФ. 2016. № 50. Ст. 7074.

9 Под медиасредой понимаются не столько журналы, телевидение и т.п. «традиционные» медиа, сколько «новые», «социальные» интернет-медиа, охватывающие и различные сайты независимо от их регистрации или нерегистрации в качестве СМИ, блоги, социальные сети, мессенджеры, видеоигры, новостные агрегаторы, видеохостинги и т.п.

диасреду[9], с одной стороны, входит в концепт информационной безопасности, но, с другой стороны, выступает по отношению к понятию «информационно-мировоззренческая безопасность» более широким, т.к., во-первых, охватывает в том числе информационные угрозы, не связанные с деструктивным информационно-психологическим воздействием, но нарушающие права человека посредством распространения в медиа иной противоправной информации, в том числе посягающей на его доброе имя, честь, достоинство, деловую репутацию ввиду диффамационного характера информации (***репутационная безопасность***)[10]; во-вторых, «медиабезопасность» — понятие, применимое по отношению не только к личности (физическим лицам), но и к юридическим лицам[11].

Таким образом, без учета детализации составляющих медиабезопасности, которые будут рассмотрены ниже, соотношение информационно-психологической и медиабезопасности с иными ключевыми концептами семантического поля «информационная безопасность» можно представить в кругах Эйлера следующим образом:

Рис. 1. Соотношение концептов информационной безопасности

В семантическое поле «информационная безопасность» также входит концепт «суверенитет». Так, в отечественной литературе можно встретить упоминания ценностного[12], эмоционального[13], духовного[14], культурного[15] ***суверенитета*** как феноменов, связанных с защитой

[10] Сто́ит отметить, что данные угрозы могут перерастать и в информационно-психологические: например, распространение дискредитирующей информации может ввести человека в депрессивное состояние, перерасти в кибersталкинг, кибербуллицид и т.д.

[11] Виды деструктивных онлайн-сообществ, деструктивной пропаганды и деструктивного сетевого контента см.: Карта информационных угроз медиабезопасности (автор — В. Д. Никишин) // URL: https://msal.ru/structure/dopolnitelnye-obrazovatelnye-programmy/institut-pravovogo-analiza-problem-informatsionnoy-i-mediabezopasnosti/laboratoriya-innovatsiy-laboratoriya-informatsionnoy-bezopasnosti-nesovershennoletnikh/ (дата обращения: 11.06.2024).

[12] *Дегтерев Д. А.* Ценностный суверенитет в эпоху глобальных конвергентных медиа // Вестник РУДН. Серия «Международные отношения». 2022. № 2. С. 352–371.

[13] *Сургуладзе В. Ш.* Эмоциональное измерение государственного суверенитета в контексте обеспечения национальной безопасности // Власть. 2023. № 4. С. 108–115 ; *Сургуладзе В. Ш.* Нейрополитика, принятие политических решений, эмоциональный суверенитет и обеспечение национальной безопасности Российской Федерации в контексте переосмысления политологического наследия Роберта Джервиса // Россия: тенденции и перспективы развития. 2023. № 18-1. С. 271–275.

[14] *Синютин А. А.* Проблемы формирования патриотизма как средства укрепления духовного суверенитета в современном российском обществе // Гуманитарий Юга России. 2024. Т. 13. № 3 (67). С. 88–99.

[15] Понятие «культурный суверенитет» также используется в разделе «Защита традиционных российских духовно-нравственных ценностей, культуры и исторической памяти» Стратегии национальной безопас-

населения от деструктивной пропаганды и навязывания ценностей, чуждых российскому цивилизационному коду. Кроме того, российские и зарубежные ученые оперируют понятиями информационного[16], цифрового[17], электронного[18] суверенитета, которые отражают зачастую сходные или идентичные сущности.

После того как 9 июня 2022 г. специальный представитель Президента РФ по вопросам цифрового и технологического развития Д. Песков, выступая на тему технологического суверенитета, заявил, что «нет смысла заниматься технологиями, не решив проблему когнитивного суверенитета»[19], в обиход вошел термин ***«когнитивный суверенитет»***, не получивший в настоящее время должного научного осмысления. Так, с 2022 г. вышли отдельные публикации филологов и философов[20], в которых когнитивный суверенитет упоминался или рассматривался преимущественно в рамках тезисов, озвученных Д. Песковым. В данной статье представлено ви́дение феномена когнитивного суверенитета с точки зрения права.

Прежде всего, представляется целесообразным установить взаимосвязь и соотношение понятий информационной и медиабезопасности и суверенитета.

В самом общем виде концепт суверенитета отражает верховенство, независимость от каких-либо сил, обстоятельств и лиц.

В подпункте «в» п. 2 Доктрины информационной безопасности Российской Федерации[21] *суверенитет отражен как часть информационной безопасности* Российской Федерации.

ности Российской Федерации (Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» // СЗ РФ. 2021. № 27 (ч. II). Ст. 5351), а также в Стратегии государственной культурной политики на период до 2030 года (распоряжение Правительства РФ от 11.09.2024 № 2501-р // Официальный интернет-портал правовой информации. URL: publication.pravo.gov.ru. 16.09.2024).

16 *Ефремов А. А.* Формирование концепции информационного суверенитета государства // Право. Журнал Высшей школы экономики. 2017. № 1. С. 201–215 ; *Нарутто С. В., Колмаков С. Ю., Япрынцев И. М.* Информационный суверенитет: конституционно-правовые основы в условиях развития цифрового государства // Образование и право. 2022. № 10. С. 14–22.

17 *Кочетков А. П., Маслов К. В.* Цифровой суверенитет как основа национальной безопасности России в глобальном цифровом обществе // Вестник Московского университета. Серия 12, Политические науки. 2022. № 2. С. 31–45 ; *Роблес-Каррильо М.* Суверенитет и цифровой суверенитет // Journal of Digital Technologies and Law. 2023. № 3. С. 673–690 ; *Володенков С. В., Воронов А. С., Леонтьева Л. С., Сухарева М.* Цифровой суверенитет современного государства в условиях технологических трансформаций: содержание и особенности // Полилог. 2021. Т. 5. URL: http://arxiv.gaugn.ru (дата обращения: 24.07.2024) ; *Кутюр С., Тоупин С.* Что означает понятие «суверенитет» в цифровом мире? // Вестник международных организаций. 2020. Т. 15. № 4. С. 48–69 ; *Зиновьева Е. С.* Формирование цифровых границ и информационная глобализация: анализ с позиций критической географии // Полис. Политические исследования. 2022. № 2. С. 8–21 ; *Pohle J., Thiel T.* Digital Sovereignty // Internet Policy Review. 2020. Vol. 9, No. 4. P. 1–19 ; *Cuihong Cai.* Building a New Digitalised World through Technology Centrism // Digital Debates: CyFy Journal. 2020. P. 48–53.

18 *Венидиктов С. В.* Платформы гражданской журналистики в контексте электронного суверенитета государств евразийского экономического союза // Среднерусский вестник общественных наук. 2017. № 4. С. 68–75.

19 URL: https://www.rbc.ru/opinions/economics/09/06/2022/62a0e95b9a79472d8b713207 (дата обращения: 24.07.2024).

20 *Яковлева И. В., Черных С. И.* Диалектика изменений аксиосистемы российского образования в переходный период // Вестник Том. гос. ун-та. 2023. № 497. С. 57–64 ; *Мирелли М. А.* Философия мягкой силы в международном взаимодействии: между «парасиловым» принуждением и скрытным управлением // Общество: философия, история, культура. 2023. № 12. С. 154–160 ; *Макулин А. В., Мирелли М. А.* Глобальные векторы «мягкой силы» в науке и образовании: социально-эпистемологические аспекты // Вестник Северного (Арктического) федерального университета. Серия «Гуманитарные и социальные науки». 2023. № 4. С. 92–103.

21 Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ РФ. 2016. № 50. Ст. 7074.

Пункт 56 Стратегии национальной безопасности Российской Федерации[22] гласит: «Целью обеспечения информационной безопасности является укрепление суверенитета Российской Федерации в информационном пространстве».

В актах Содружества Независимых Государств *информационный суверенитет* государств-участников понимается как «способность и возможность самостоятельно осуществлять функции государства в информационной сфере с целью соблюдения прав и свобод граждан, обеспечения национальной и коллективной безопасности»[23]. Учитывая широту спектра прав человека и комплексность понятия «национальная безопасность», охватывающего демографическую безопасность, государственную и общественную безопасность, оборону страны, информационную безопасность, экономическую безопасность, научно-технологическое развитие (технологический суверенитет), экологическую безопасность, защиту традиционных российских духовно-нравственных ценностей, культуры и исторической памяти (культурный (шире — когнитивный) суверенитет), стратегическую стабильность международного сотрудничества и т.д., — информационный суверенитет стран — участниц СНГ рассматривается в аспекте противодействия не только информационным, но и гибридным угрозам[24].

Таким образом, на наш взгляд, ***информационный суверенитет*** можно трактовать как *правовой статус безопасности* при осуществлении информационной политики государства, а также при информационном обеспечении иных политик государства.

В цифровом пространстве суверенитет, рассматриваемый Х. Ели с точки зрения интересов трех ключевых акторов: государства, гражданина и международного сообщества, — разделяется на три уровня:

1) базовый — «физический» уровень, отражающий инфраструктуру киберпространства;

2) срединный — уровень приложений (интернет-платформы и интернет-операторы), касающийся различных сфер жизнедеятельности;

3) верхний — основной (содержательный), включающий «режим, закон, политическую безопасность и идеологию, которая не подлежит сомнению и включает в себя руководящие основы и воплощает основные интересы страны»[25].

Примечательно, что автор указанной концепции, рассматривая верхний уровень суверенитета в киберпространстве, подчеркивает, что государства вполне естественно имеют различия в подходах к законодательному регулированию киберпространства ввиду национально-культурных, религиозных особенностей и т.д., что «разнообразие является нормой человеческого существования, которая не может быть отформатирована в соответствии с какой-либо одной культурой»[26]. Указанный тезис предлагаем развить в двух ипостасях: с одной стороны, киберпространство как пространство смыслов не должно быть организовано в духе однополярного мироустройства и культурной гегемонии отдельного государства или группы развитых стран; с другой стороны, информационная политика и выбор регуляторных моделей, ограничений и запретов на циркулирование в киберпространстве информации определенных типов и т.п. — прерогатива национальных правительств (законодателей), а не медиакорпораций, владельцев социальных сетей, новостных агрегаторов и других провайдеров интернет-сервисов, пытающихся в рамках своих коммуникационных режимов (локальных правил) установить цензуру, и, про-

---

[22] Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» // СЗ РФ. 2021. № 27 (ч. II). Ст. 5351.

[23] Постановление № 41-13 Межпарламентской Ассамблеи государств — участников СНГ «О проекте Стратегии обеспечения информационной безопасности государств — участников Содружества Независимых Государств». Принято в г. Санкт-Петербурге 28 ноября 2014 г. // Информационный бюллетень. Межпарламентская Ассамблея государств — участников Содружества Независимых Государств. 2014. № 62 (ч. 2) ; решение Совета глав правительств СНГ «О Стратегии обеспечения информационной безопасности государств — участников Содружества Независимых Государств». Принято в г. Москве 25 ноября 2019 г. // Единый реестр правовых актов и других документов СНГ. URL: http://cis.minsk.by/ (дата обращения: 11.05.2024).

[24] О понятии гибридной войны см. ниже.

[25] *Yeli H. A.* Three-Perspective Theory of Cyber Sovereignty // PRISM. 2017. Vol. 7. No. 2. P. 112–114.

[26] *Yeli H. A.* Op. cit. P. 114.

[27] Колумбайн (скулшутинг) — запрещенная в РФ террористическая организация.

двигая через алгоритмы «нужный» контент, зачастую преследуют политические цели (в том числе «большой киберпятерки» GAFAM: Google, Amazon, Facebook, Apple, Microsoft).

Перечисленные выше уровни суверенитета в киберпространстве предлагаем обозначить как *инфраструктурный, сервисный* и *когнитивный* соответственно, при этом обобщающим понятием для указанных уровней с точки зрения терминологического аппарата отечественных документов стратегического планирования и иных нормативных актов выступает понятие *информационного суверенитета*.

Соотношение безопасности как состояния защищенности или суверенитета как статуса безопасности и субъектов-обладателей такого состояния (статуса) можно систематизировать в виде следующей схемы:

Рис. 2. Виды безопасности и их обладатели

Когнитивный суверенитет (в узком понимании как часть информационной безопасности) предполагает прежде всего обеспечение защиты граждан от информационно-психологического воздействия со стороны зарубежных государств (финансируемых ими информационных «агентов»). Такое воздействие может проявляться в реализации широкого спектра психологических операций; распространении фейковой и диффамационной, дискредитирующей информации (в том числе с использованием аудио- и видеодипфейков, осуществления спуфинга); политической пропаганде сепаратистских настроений, экстремистской и террористической идеологии; инспирировании массовых беспорядков и иных противоправных акций; развитии в интернет-медиа сетей псевдосубкультурных течений радикальной направленности: гетероагрессивной (сообщества, оправдывающие и (или) пропагандирующие насилие по отношению к другим лицам: колумбайнеры (скулшутеры)[27], массшутеры, М.К.У.[28] и т.д.); аутодеструктивной (сообщества, оправдывающие и (или) пропагандирующие насилие по отношению к самому себе: суицидальные сообщества, «сообщества анорексичек», сообщества «опасных хобби», сообщества, пропагандирующие психоактивные вещества и т.д.); администрировании онлайн-сообществ, пропагандирующих антисемейные ценности, девальвацию традиционных ценностей, обесценивание самой человеческой жизни и т.д.[29]

Можно условно выделить две основные функции таких деструктивных онлайн-сообществ: 1) взращивание адептов, совершающих резонансные акты насилия (к другим или к самому себе), что ведет к устрашению населения и дестабилизации обстановки, *и (или)* моральное разложение, дегуманизация, разобще-

[28] М.К.У. — запрещенная в РФ террористическая организация.

[29] *Никишин В. Д., Осипов Д. П.* Понятие и сущность информационного суверенитета // Правовое обеспечение суверенитета России: проблемы и перспективы : сборник докладов XIII Московской юридической недели : в 4 ч. М. : Издательский центр Университета имени О.Е. Кутафина (МГЮА), 2024. Ч. 1. С. 170–171.

ние общества; 2) подготовка в целом из всего контингента подписчиков протестной массы молодых людей, готовых к противоправным действиям, в том числе к преступлениям против конституционного строя («цветным революциям» и пр.)[30].

В то же время *когнитивный суверенитет* можно представить в широком смысле как гораздо более сложное и многогранное понятие, составляющие которого будут рассмотрены далее в статье.

2. Понятия информационной, когнитивной и гибридной войны. Феномен «мягкой силы»

Рассмотренные выше концепты отражают безопасность как состояние защищенности от угроз или статус такой безопасности (суверенитет), при этом большинство информационных угроз обусловлено не действиями отдельных лиц, имеющими личную мотивацию (мести, опорочивания, нанесения ущерба и т.п.), а целенаправленной скоординированной деятельностью оппонентов в «войне смыслов» и «войне за умы». В этой связи целесообразно остановиться на содержании понятий информационной, психологической, когнитивной и гибридной войны.

Одной из распространенных дефиниций ***информационной войны*** выступает ее определение как комплекса «мероприятий по информационному воздействию на массовое сознание для изменения поведения людей и навязывания им целей, которые не входят в число их интересов, а также защита от подобных воздействий»[31].

А. В. Манойло определяет информационную войну как «вооруженный конфликт, в котором столкновение сторон происходит в форме информационных операций с применением информационного оружия»[32]. При этом А. В. Курилкин определяет психологические и кибернетические операции как подвиды информационных операций:

информационная операция — «спланированная деятельность, осуществляемая в мирное или военное время, рассчитанная на иностранные дружественные, враждебные или нейтральные аудитории с целью повлиять на информацию, информационные процессы и системы управления для достижения собственных внешнеполитических целей»[33];

психологическая операция — «спланированная деятельность по передаче информации широким народным массам и элитам иностранных государств с целью повлиять на их поведение, эмоции, мотивы, логические построения и ценности»[34];

кибернетическая операция — «деятельность по защите собственной киберинфраструктуры и выведению из строя и уничтожению киберинфраструктуры противника, а также похищение важной информации и использование специальных технических средств для воздействия на поведение людей в онлайн-пространстве в интересах проведения информационной операции»[35].

Гибридная война представляет собой стратегию и тактику сочетания конвенциональных (обычных, классических, симметричных) военных действий с методами экономического, политического и информационного давления на противника.

А. Н. Медушевский, рассматривая ***когнитивную войну*** как продолжение концепта гибридной войны, утверждает, что она направлена на такой обязательный признак суверенитета государства, как независимое правительство, свободное от внешнего вмешательства, и что «конечная цель когнитивной войны — преодолеть внутренние информационно-пропагандистские барьеры государства, изменить систему ценностей и понимание мира, вынудить население к принятию желательного решения, установить над ним “рефлексивный контроль”,

---

[30] *Никишин В. Д., Осипов Д. П.* Указ. соч. С. 170–171.

[31] *Василенко И.* Информационная война как фактор мировой политики // Государственная служба. 2009. № 3. С. 80–86.

[32] *Манойло А. В.* Информационные войны и психологические операции. Руководство к действию. М. : Горячая линия — Телеком, 2018. С. 75.

[33] *Курилкин А. В.* Информационные операции и кибервойна: от истории к современности. М. : Горячая линия — Телеком, 2022. С. 31.

[34] *Курилкин А. В.* Указ. соч. С. 31.

[35] *Курилкин А. В.* Указ. соч. С. 31.

подорвав его способности "наблюдать, ориентироваться, решать и действовать"»[36]. Отметим «зауженный» характер указанной дефиниции, сосредотачивающей акценты на изменение системы ценностей в целях формирования антиправительственных настроений и совершения соответствующих действий, в то время как когнитивная война — это «война за умы», это в том числе и культурная экспансия, размывание ценностей в целях разложения общества как такового, это также и распространение антисемейных ценностей как антидемографическая диверсия и депопуляционная политика и т.д. Когнитивная война охватывает не только ограниченные по времени информационные операции как таковые, но и поступательную социокультурную экспансию (в том числе «мягкую силу»), а также лоббирование определенных решений, влияющих на ту или иную политику государства.

Таким образом, понятия когнитивной войны и информационной войны выступают крайне пересекающимися, но не равнозначными по содержанию концептами. Гибридная же война может включать в себя элементы и информационной, и когнитивной войны (рис. 3).

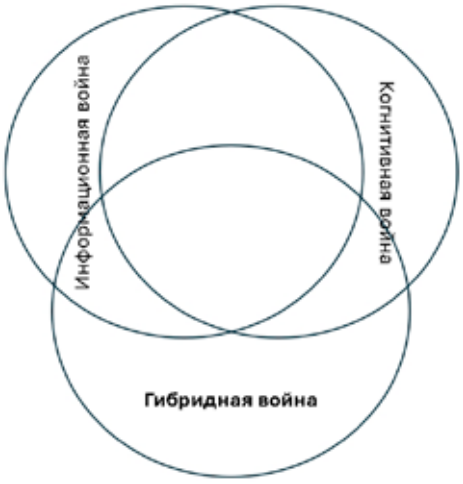

Рис. 3. Соотношение информационной, когнитивной и гибридной войны

Рассматривая феномен ***«мягкой силы»***, М. А. Мирелли утверждает, что «сегодня вопрос о возможности и условиях воздействия одной или нескольких стран на другие государства, культуры или цивилизации явно тяготеет к тому, чтобы предшествовать рассмотрению возможности соблюдения международного права или даже этики невмешательства в дела других стран»[37].

«Мягкую силу» можно понимать как разновидность рефлексивного управления объектом, под которым философ В. А. Лефевр понимал «воздействие на субъектов, склоняющее их принять решения, заранее подготовленные управляющей стороной»[38].

Близким по смыслу концептом выступает понятие ***«социологической» пропаганды***, введенное французским философом Ж. Эллюлем[39]. Данный концепт предполагает социокультурную экспансию, незаметное проникновение культурных, ценностных установок, моделей поведения, образа жизни через массовую культуру, рекламу, киноиндустрию и т.д. В качестве наглядных примеров «социологической» пропаганды, посягающей на медиабезопасность интернет-пользователей, можно привести популяризацию в русскоязычном сегменте интернет-медиа в последние 10–15 лет аниме-культуры, через которую транслируется широчайший пласт деструктивных идей (как депрессивно-суицидального, так и радикально насильственного характера, а также пропаганда сексуально-гендерных девиаций и т.п.). Другой пример — популяризация в России True Crime Community (поклонников «настоящих» преступлений) как очередной тренд вестернизации медиапотребления, при этом TCC-сообщества в основной своей массе содержат оправдание и героизацию маньяков и серийных убийц, служат основной воронкой вовлечения в радикальные М.К.У. и иные экстремистско-террористические сообщества.

Переход к Индустрии 4.0, всеобщая технологизация, цифровизация и глокализация

---

[36] *Медушевский А. Н.* Когнитивная война: социальный контроль, управление сознанием и инструмент глобального доминирования. Часть 2 // Вопросы теоретической экономики. 2023. № 3. С. 93.

[37] *Мирелли М. А.* Философия мягкой силы в международном взаимодействии: между «парасиловым» принуждением и скрытным управлением // Общество: философия, история, культура. 2023. № 12. С. 156.

[38] *Томас Т. Л.* Рефлексивное управление в России: теория и военные приложения // Рефлексивные процессы и управление. 2002. Т. 2. № 1. С. 72.

[39] *Ellul J.* Propaganda: The formation of men's attitudes / transl. K. Kellen, J. Lerner. New York : Random House / Vintage, 1973 ; *Ellul J.* Histoire de la propaganda. Paris : Presses Universitaires de France, 1967.

трансформируют «мягкую силу» из «искусства убеждения» в особую социальную технологию, под которой можно понимать вид социального контакта. Как утверждает А. А. Сазонова, этот вид социального контакта основан на «мягком» воздействии субъекта на ценностный пласт сознания объекта[40].

Информационные экстерналии «мягкой силы» имеют целью воздействия разрушение самого «цивилизационного кода» государства-мишени. А. В. Макулин и М. А. Мирелли, анализируя феномен «мягкой силы» в XX столетии, отмечают, что объектом воздействия выступала культура, экономика, политика, язык, социально-историческая память и образы самовосприятия, искусство, мода, наука, воспитание и образование будущих поколений, мировоззрение, оборона, безопасность, идеология, религия, «т.е. “генетические” основания деятельности, жизнедеятельности, роста и воспроизводства конкретной культуры-цивилизации»[41].

3. Социальная инженерия как вызов медиабезопасности и когнитивному суверенитету. Юридическая социальная инженерия

Феномен ***социальной инженерии*** фактически находился за орбитой интересов юристов, за исключением рассмотрения криминалистами социальной инженерии в крайне узком смысле с точки зрения расследования инцидентов неправомерного доступа к информации и т.п., а также работ, посвященных анализу трудов Р. Паунда, рассматривавшего социальную инженерию в рамках теории социальной юриспруденции[42].

На основе анализа трудов социологов, философов[43], филологов[44], правоведов[45], криминалистов и специалистов в области информационной безопасности[46] нами был сделан вывод, что социальную инженерию можно рассматривать в следующих ипостасях.

1) Как применение социогуманитарных технологий для создания новых социальных институтов, изменения существующих институтов

С точки зрения данного широкого подхода социальная инженерия — это «совокупность

---

[40] *Сазонова А. А.* Гуманитарные технологии как теоретический концепт: основные подходы // Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики. 2017. № 3-1 (77). С. 127.

[41] *Макулин А. В., Мирелли М. А.* Указ. соч. С. 94.

[42] *Pound R.* Mechanical Jurisprudence // Columbia Law Review. 1908. Vol. 8. P. 605–623; *Pound R.* The Spirit of the Common Law. Boston, 1921 ; *Pound R.* Interpretations of Legal History. N. Y., 1923 ; *Pound R.* An Introduction to the Philosophy of Law. New Haven, 1950 ; *Pound R.* New Paths of the Law. Lincoln, 1950 ; *Pound R.* Social Control through Law. Hamden, 1968.

[43] *Резник Ю. М.* Социальная инженерия: предметная область и границы применения // Социологические исследования. 1994. № 2. С. 87–96 ; *Федорова Ж. В.* О механизмах социокультурной инженерии в информационном обществе // Kant. 2022. № 2 (43). С. 196 ; *Фадеева В. Н.* Феномен социальной инженерии в концепции К. Поппера // Известия ТПУ. 2008. № 6. С. 107–110 ; *Моисеева А. П.* Генезис социальной инженерии в контексте междисциплинарности // Известия ТПУ. 2012. № 6. С. 64–69.

[44] *Макашова В. В.* Дезинформация как элемент технологий управления смыслами // МедиаВектор. 2023. № 9. С. 84–88 ; *Сарна А. Я.* Указ. соч. С. 218–235.

[45] *Груздев В. С.* Об истоках правовых взглядов Р. Паунда // Теория и практика общественного развития. 2020. № 8 (150). URL: https://cyberleninka.ru/article/n/ob-istokah-pravovyh-vzglyadov-r-paunda (дата обращения: 03.09.2024) ; *Pound R.* Social Control through Law. Hamden, 1968 ; *Мальцев Г. В.* Социальные основания права. М., 2007 ; История политических и правовых учений / под ред. В. С. Нерсесянца. М., 1998.

[46] *Кузнецов М., Симдянов И.* Социальная инженерия и социальные хакеры. СПб. : БХВ-Петербург, 2007 ; *Старостенко Н. И.* Криминалистический аспект техник социальной инженерии при совершении преступлений // Вестник КРУ МВД России. 2020. № 1 (47). С. 80–83 ; *Ревенков П. В., Бердюгин А. А.* Социальная инженерия как источник рисков в условиях дистанционного банковского обслуживания // Национальные интересы: приоритеты и безопасность. 2017. № 9 (354). С. 1747–1760 ; *Тумбинская М. В.* Процесс распространения нежелательной информации в социальных сетях // Бизнес-информатика. 2017. № 3 (41). С. 65–76.

подходов, ориентированных на целенаправленное изменение социальной реальности, ее структур и институтов, определяющих человеческое поведение и обеспечивающих контроль»[47].

Такое понимание социальной инженерии согласуется с концепцией открытости общества К. Поппера, который, сравнивая социальную инженерию с историцизмом[48], подчеркивает, что «инженер или технолог предпочитает рациональное рассмотрение институтов как средств, обслуживающих определенные цели, и оценивает их исключительно с точки зрения их целесообразности, эффективности, простоты, и т.п.»[49]. Таким образом, в указанной концепции предполагается возможность постоянных, но постепенных социальных изменений и преобразований в условиях неопределенности будущего и на основе рационально-демократического подхода, и социальная инженерия рассматривается как методология управления социальными институтами без революционных изменений и применения насилия как такового.

Таким образом, в целом нейтральное понятие, отражающее механизм социокультурного конструирования, трансформации социальных институтов, однако последствия использования социальной инженерии будут зависеть от акторов и их целеполагания.

Так, применение социальной инженерии может быть направлено и на социальную деструкцию — пропаганду девиантного и делинквентного поведения, пропаганду антисемейных ценностей для разрушения института семьи, попытки создания экстремистско-террористическими сетевыми структурами так называемых антисистем как «фантомных» социальных систем, т.к. разрушение элементов сложившихся социальных систем не влечет замену альтернативой, а образует вакуум.

Создание ***«фантомных» социальных образований*** можно проиллюстрировать на примере квазисубкультуры «ЧВК “Редан”», «раскрученной» в 2023 г. за счет фан-сообщества аниме «Hunter x Hunter». Распространение так называемых редановцев — наглядный пример psy-операции, применения технологий социального инжениринга, когда в течение пары дней в социальных сетях была создана сеть ресурсов «ЧВК Редан» и мессенджерах с многотысячными охватами аудитории — сеть, оказывающая реальное психологическое воздействие на подростков и выводящая их на «забивы». Причем истории переименований сообществ нередко показывают, что ранее ряд сообществ носил неонацистскую тематику («Слава Украине» и т.п. названия). Такие сообщества, ранее со сравнительно малочисленным количеством подписчиков, за несколько дней многократно увеличили свою аудиторию, т.к. стали появляться в результатах поисковых запросов по ключевому слову «Редан». Есть и примеры сообществ, созданных с нуля 19–20 февраля 2023 г. и моментально вовлекших тысячи подростков в свои подписчики. Инфоповод «Редан» является отличным примером создания универсального объекта ненависти у молодых людей различных субкультур, зачастую конфликтующих между собой, а также той части молодежи, которая избегает офлайн-проявлений своих настроений («дед-инсайды»). Так, объединялись в группировки совершенно идеологически недружественные друг к другу группы молодежи: представители кавказской молодежи, «АУЕшники»[50], националистические группировки, группы скинхедов и оффников — с целью насильственных акций по отношению к представителям «Редана». В свою очередь, множество подростков, причисляющих себя к «дед-инсайдам» или вовсе не состоящие ранее ни в каких субкультурах, выходили на улицы в погоне за «хайпом». Более того, общественный резонанс вокруг «ЧВК Редан» активно использовался представителями теневого сегмента: в крупных телеграм-сообществах «ЧВК Редан» активно рекламировались ресурсы, пропагандирующие и романтизирующие наркоторговлю, употребление наркотиков, сваттинг, продажу нелегального оружия, кардинг и т.д. Таким образом, в общественном сознании было сформировано представление о наличии некой доволь-

[47] *Резник Ю. М.* Социальная инженерия: предметная область и границы применения // Социологические исследования. 1994. № 2. С. 87–96.

[48] Историзм в понимании К. Поппера охватывает социально-философские теории, основанные на вере в исторически обусловленное развитие социальных институтов, существование тенденций и законов исторического развития, понимание которых позволяет прогнозировать будущее.

[49] *Поппер К.* Открытое общество и его враги : пер. с англ. М. : Международный фонд «Культурная инициатива». 1992. Т. 1. С. 54–55.

[50] АУЕ — экстремистская организация, запрещенная на территории РФ.

но массовой радикальной субкультуры, которой фактически не существовало за несколько дней до резонансных событий февраля 2023 г., что позволяет говорить о фантомном характере данной субкультуры (квазисубкультуры).

1.1) Юридическая социальная инженерия

Применительно к юриспруденции термин социальной инженерии был введен в научный оборот Р. Паундом — основоположником американской школы ***социологической юриспруденции***, «лейтмотивом которой стала разработка тезиса о цели права, положенного им в основу концепции социальной инженерии»[51].

По сути, Р. Паунд прагматично рассматривал само право как метод социальной инженерии, как арсенал средств регулирования общественных отношений через баланс интересов, как механизм координации поведения членов социума, как средство социального контроля согласования разнонаправленных интересов[52].

Как отмечает В. Г. Графский, социологическая юриспруденция оформилась «в самостоятельную дисциплину в связи с потребностью в целенаправленном изучении и использовании права в качестве инструмента регулирования и социального контроля»[53].

Идеи, заложенные Р. Паундом и его последователями, представляют живой интерес и сегодня, однако следует учитывать, что в своих работах американский правовед фактически сводит процесс нормотворчества к деятельности судей по созданию прецедентов, основанных на свободе судейского усмотрения («право в действии»). На наш взгляд, на ***юридическую социальную инженерию*** необходимо «смотреть» шире, в том числе не только с точки зрения англосаксонского прецедентного права. Юрист-стратег (юрист-правотворец), разрабатывающий модели нормирования не только текущих, но и зарождающихся, прогнозируемых общественных отношений, также выступает социальным инженером, конструируя модели должного социального взаимодействия в меняющемся обществе, учитывая риски нарушения интересов различных акторов, давая правовую «обвязку» новым социальным институтам и инструментарий разрешения потенциальных конфликтов.

При этом нельзя сводить право как институт исключительно к нормам, своду правил поведения. Право выступает средством моделирования («инжиниринга») социального поведения людей на определенной ценностной основе; правотворчество и правоприменение вкупе с восприятием правовых норм субъектами правоотношений (в том числе с ценностной оценкой, уровнем нигилизма, готовностью следовать предписаниям) образуют правовую парадигму мышления, «юридическую ментальность» общества.

2) Как манипулирование поведением человека в системе «человек — машина» с помощью психологических приемов, изменение его отношения к иным субъектам общественных отношений

С точки зрения данного подхода социальная инженерия рассматривается как методология компьютерно-опосредованного перекодирования сознания, изменения картины мира через дезинформацию, введение в заблуждение, манипулирование, искажение исторической памяти, использование информационных ресурсов лидеров общественного мнения (ЛОМов) для информационных вбросов и кампаний.

В цифровой коммуникации для этих целей могут применяться такие техники медиавоздействия, как импринтинг, прайминг, сторителлинг, фрейминг и дизайнинг и т.п.[54]

2.1) Как совокупность методов психологического воздействия, опосредованного цифровой коммуникацией и направленного на получение неправомерного доступа к данным информационных систем, и (или) совершение мошеннических действий без непосредственного доступа в ИС

Речь идет прежде всего о совершении мошеннических действий, получении конфиденциальной информации путем введения субъекта в заблуждение, в том числе через обман, отвлечение внимания, запугивание, шантаж, угрозы, нагнетание психологического напряжения, обещания вознаграждения, выдачу себя за другое лицо.

По определению Н. И. Старостенко, социальная инженерия — «это система способов воздействия и контроля людей, которая побуж-

---

[51] *Груздев В. С.* Указ. соч. URL: https://cyberleninka.ru/article/n/ob-istokah-pravovyh-vzglyadov-r-paunda (дата обращения: 03.09.2024).

[52] *Pound R.* Social Control through Law.

[53] История политических и правовых учений / под ред. В. С. Нерсесянца. М., 1998. С. 677.

[54] *Сарна А. Я.* Указ. соч. С. 218–235.

дает их совершать определенные действия, применяемая в целях получения персональных данных личности, а также иных конфиденциальных сведений для достижения преступного результата»[55]. К техникам социальной инженерии криминалисты и специалисты в области информационной безопасности относят в том числе фишинг, вишинг, претексинг, «троянский конь» и др.

С точки зрения данного узкого подхода социальную инженерию можно рассматривать как использование психологической уязвимости человека для несанкционированного доступа к информации.

Таким образом, ***социальная инженерия*** выступает в целом собирательным термином для обозначения прежде всего социогуманитарных технологий управления смыслами, методов и приемов информационно-психологического воздействия на поведение людей.

Выше была рассмотрена лишь часть примеров использования инструментария социальной инженерии для деструктивного информационно-психологического воздействия на интернет-пользователей, при этом было бы необъективно рассматривать социальную инженерию исключительно как атрибут внешней деструкции. Так, информационная политика государства и нормативные модели регулирования информационного пространства, включая установление ограничений и запретов на распространение информации определенных видов, также выступают элементами социальной инженерии, будучи направленными на защиту граждан от дезинформации; дискриминирующей и унижающей человеческое достоинство информации; контента, пропагандирующего антисемейные и иные нетрадиционные ценности; пропаганды экстремистской идеологии и т.д. (что в конечном счете необходимо не только для сохранения когнитивного иммунитета граждан, но и для обеспечения демографической политики, безопасности и суверенитета государства в целом). Как отмечает Ж. В. Федорова, «сама по себе данная парадигма *(парадигма социальной инженерии — прим. автора)* не несет негативную этимологию, так как, будучи механизмом социокультурного конструирования, в том числе способствует сохранению культурных кодов любого типа общества»[56]. Таким образом, использование социальной инженерии — неотъемлемый атрибут информационного общества, однако результат такого использования будет зависеть от акторов и их целеполагания.

Кроме того, следует учитывать трансформацию технологических особенностей киберпространства, которые позволяют повышать эффективность манипуляций индивидуальным и общественным сознанием, деструктивного информационно-психологического воздействия и в целом социальной инженерии.

В этой связи следует обратиться к концепции этапов развития Интернета «Web 1.0 — Web 2.0 — Web 3.0 — Web 3», которая до настоящего момента не находила должного правового анализа с точки зрения права и будет рассмотрена во второй части статьи.

СПИСОК ЛИТЕРАТУРЫ

Дегтерев Д. А. Ценностный суверенитет в эпоху глобальных конвергентных медиа // Вестник РУДН. Серия «Международные отношения». 2022. № 2. С. 352–371.

Ефремов А. А. Формирование концепции информационного суверенитета государства // Право. Журнал Высшей школы экономики. 2017. № 1. С. 201–215.

Сарна А. Я. Технологии воздействия на аудиторию в современном медиапространстве // Вестник Санкт-Петербургского университета. Социология. 2020. Т. 13. Вып. 2. С. 218–235.

Федорова Ж. В. О механизмах социокультурной инженерии в информационном обществе // Kant. 2022. № 2 (43). С. 195–199.

Яковлева И. В., *Черных С. И.* Диалектика изменений аксиосистемы российского образования в переходный период // Вестник Томского государственного университета. 2023. № 497. С. 57–64.

Ellul J. Propaganda: The formation of men's attitudes / transl. K. Kellen, J. Lerner. New York : Random House / Vintage, 1973. 352 p.

Ellul J. Histoire de la propaganda. Paris : Presses Universitaires de France, 1967. 128 p.

[55] *Старостенко Н. И.* Указ. соч. С. 81.

[56] *Федорова Ж. В.* Указ. соч. С. 196.

REFERENCES

Degterev DA. Value sovereignty in the era of global convergent media. *Vestnik RUDN. Seriya «Mezhdunarodnye otnosheniya» [RUDN Journal. International Relations Series].* 2022;2:352-371. (In Russ.).

Efremov AA. Formation of the concept of information sovereignty of the state. *Pravo. Zhurnal Vysshey shkoly ekonomiki [Law. Journal of the Higher School of Economics].* 2017;1:201-215. (In Russ.).

Ellul J. Histoire de la propaganda. Paris: Presses Universitaires de France, 19*67.*

Ellul J. Propaganda: The formation of men's attitudes. Transl. K. Kellen, J. Lerner. New York: Random House/ Vintage; 1973.

Fedorova ZhV. On the mechanisms of socio-cultural engineering in the information society. *Kant*. 2022;2(43):195-199. (In Russ.).

Sarna AYa. Technologies of influencing the audience in the modern media spac*e. Vestnik Sankt-Peterburgskogo universiteta. Sotsiologiya*. 2020;13(2):218-235. (In Russ.).

Yakovleva IV, Chernykh SI. Dialectics of changes in the axiosystem of Russian education in the transition period. *Vestnik Tomskogo gosudarstvennogo universiteta [Tomsk State University Journal]*. 2023;497:57-64. (In Russ.).

ИНФОРМАЦИЯ ОБ АВТОРЕ

Никишин Владимир Дмитриевич, кандидат юридических наук, доцент кафедры информационного права и цифровых технологий, директор Института информационной и медиабезопасности Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)
д. 9, Садовая-Кудринская ул., г. Москва 125993, Российская Федерация
vdnikishin@msal.ru

INFORMATION ABOUT THE AUTHOR

Vladimir D. Nikishin, Cand. Sci. (Law), Associate Professor, Department of Information Law and Digital Technologies, Director, Institute of Information and Media Security, Kutafin Moscow State Law University (MSAL), Moscow, Russian Federation
vdnikishin@msal.ru

Материал поступил в редакцию 20 марта 2024 г.
Статья получена после рецензирования 14 октября 2024 г.
Принята к печати 15 октября 2024 г.

Received 20.03.2024.
Revised 14.10.2024.
Accepted 15.10.2024.