

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 2)

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 важно 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 2). *Lex russica*. 2024. Т. 77. № 12. С. 140–155. DOI: 10.17803/1729-5920.2024.217.12.140-155

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»).

Начало см.: 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.

Legal Support of Media Security and Cognitive Sovereignty: Challenges of Social Engineering, Hybrid Wars and Web 3.0 Mechanisms (Part 2)

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. The 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» allowed, 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 2). *Lex russica*. 2024;77(12):140-155. (In Russ.). DOI: 10.17803/1729-5920.2024.217.12.140-155

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»).

See Part 1: 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.

4. Развитие киберпространства:

Web 1.0 — Web 2.0 — Web 3.0 — Web 3

Иерархия этапов развития Интернета «Web 1.0 — Web 2.0 — Web 3.0 — Web 3» выступает крайне условной (как по времени перехода, так и по признакам) и нелинейной концепцией, отражает в большей степени постфактумный ана-

лиз основных вех развития киберпространства, лишь концепция Web 3 выступает преимущественно прогностической.

К сожалению, в юридической литературе данный уровневый («этапный») подход к анализу эволюции киберпространства не нашел должного отражения. Нами был изучен ряд работ представителей технических специально-

стей¹, филологов², экономистов³, политологов⁴, маркетологов⁵. Следует отметить, что среди исследователей нет единства мнений по поводу и классификации этапов развития Интернета (в том числе к разграничению или отождествлению Web 3.0 и Web 3), и периодов данных этапов, и, что самое главное, отличительных особенностей данных этапов, т.к. одни и те же признаки у разных авторов порой характери-

зуют различные этапы в указанной иерархии или же различные признаки предлагаются как основные детерминанты одного и того же этапа. По результатам анализа литературы и социально-гуманитарного, и технического профиля нами была сформирована собственная концепция признаков модели иерархии «Web 1.0 — Web 2.0 — Web 3.0 — Web 3», представленная в таблице ниже.

Концепция эволюции развития Интернета «Web 1.0 — Web 2.0 — Web 3.0 — Web 3»

Критерий	Web 1.0	Web 2.0	Web 3.0	Web 3
Время	1989–2004	2004 — по наст. вр.	2006 — по наст.\вр.	2014 — по наст. вр.
Авторы / пользо- ватели терминов	Тим О'Рейли, Дейл Дугерти, Дарси Динуччи	Джейсон Калаканис ⁶ , Марчело Диас де Аморим, Тим Бер- нерс-Ли, Срамана Митра, Тед Хоу		
Условный благо- получатель	Интернет для читателей	Интернет для корпораций	Интернет для создателей	
Тип медиа	Массмедиа: один — многим	Новые (социаль- ные, интернет-) медиа: многие — многим	«Персональные» медиа: многие — одному	
Канал коммуника- ции	Линейный	Сетевой (ризомный)		
Формула действий	Read only (односто- ронний канал коммуникации)	Read and write (взаимодействие)	Read and write в «семантических капсулах»	Read-write-own, в том числе read and write в «кап- суле», управляемой самим пользовате- лем

¹ *Намиот Д. Е., Куприяновский В. П.* Архитектурные модели Web 3 // International Journal of Open Information Technologies. 2024. № 2. С. 84–95 ; *Lassila O., Hendler J.* Embracing «Web 3.0» // IEEE Internet computing. 2007. Т. 11. № 3. С. 90–93 ; *Mühle A. et al.* A survey on essential components of a selfsovereign identity // Computer Science Review. 30 (2018). Р. 80–86 ; *Hendler J.* Web 3.0 Emerging // Computer 42.1. 2009. Р. 111–113 ; *Getting B.* Basic Definitions: Web 1.0, Web 2.0, Web 3.0 // Practical Ecommerce. 18.04.2007. URL: <http://www.practicalecommerce.com/articles/464-Basic-DefinitionsWeb-1-0-Web-2-0-Web-3-0> (дата обращения: 05.05.2012) ; *Горячкин Б. С., Вдовкина Е. Д.* Тенденции развития Интернета: принципы и методы перехода к Web 3.0 // E-Scio. 2023. № 3 (78). URL: <https://cyberleninka.ru/article/n/tendentsii-razvitiya-interneta-printsipy-i-metody-perehoda-k-web-3-0> (дата обращения: 13.08.2024).

² *Кобенко Ю. В.* Аспекты медийной коммуникации в социальных сетях // Вестник Санкт-Петербургского университета. Язык и литература. 2023. № 20 (1). С. 183–190 ; *Итинсон К. С.* Web 1.0, Web 2.0, Web 3.0: этапы развития веб-технологий и их влияние на образование // КНЖ. 2020. № 1 (30). С. 19–21 ; *Итинсон К. С.* Web 3.0-технологии в образовании и научных исследованиях // КНЖ. 2020. № 1 (30). С. 22–24 ; Социальные сети: комплексный лингвистический анализ : монография : в 2 т. / под науч. ред. Н. Д. Голева ; отв. ред. Л. Г. Ким. Кемерово, 2021. Т. 1.

³ *Мальсагова Р. Г., Дугаев М. В., Ефремова С. А.* Блокчейн, криптовалюта, NFT, Web 3.0 и Smart-контракт как технологии развития и масштабирования метавселенных // Инновации и инвестиции. 2023. № 11. С. 199–207.

⁴ *Бронников И. А., Беденкова А. С.* Метавселенные и государства: вместе или порознь // Ars Administrandi. 2023. № 2. С. 224–250.

⁵ *Рвачев Н. А.* Революция в мире маркетинга: как Web 3.0 меняет лицо бизнеса // Инновации и инвестиции. 2022. № 8. С. 50–53.

⁶ *Calcanis J.* Web 3.0, the «official» definition // URL: <https://calcanis.com/2007/10/03/web-3-0-the-official-definition> (дата обращения: 03.04.2024).

Критерий	Web 1.0	Web 2.0	Web 3.0	Web 3
Основная идея	«Витринный» веб	— Социальный веб; — юзабилити, дизайн и интер-активность	Семантический веб (семантическая «паутина») — автоматизированный анализ UGC	Бессерверный децентрализованный веб — вернуть пользователям право владения данными посредством децентрализации с использованием суверенной идентификации на базе DAO (децентрализованных автономных организаций)
Основные характеристики	Статические страницы	— Динамические веб-страницы (CGI); — регистрация и авторизация на сайтах/в сервисах; — пользовательский контент (UGC — User Generated Content); — сетевая экстерналия; — сервисы, концепция которых построена на наполнении контентом исключительно самими пользователями (социальные сети, мессенджеры, блог-платформы, форумы, видеохостинги, «свободные» энциклопедии и т.п.); — возможность коллективного выполнения работ	— Мультимедийные технологии; — персонализация / кастомизация контента с использованием алгоритмов ИИ и big data (в том числе рекомендательные алгоритмы); — системы рейтинга; — мем-комплексы	— «Сеть сетей»; — веб как база данных; — децентрализованные приложения (DApp); — блокчейн; — ИИ; — big data; — НО! отсутствие рекомендательных алгоритмов; — прозрачность (ПО с открытым исходным кодом); — криптовалюта; — смарт-контракты; — NFT, токенизация интернет-активности; — иммерсивное пространство: метавселенные как новая версия интернет-интерфейса, включая AR, VR и т.д.; — SocialFi (социальные сети для социальных финансов); — «экспансия» NLP (технологий обработки естественного языка) и голосовых помощников; — расцвет использования IoT-устройств и смартгаджетов

Критерий	Web 1.0	Web 2.0	Web 3.0	Web 3
<i>Безопасность данных и контроль</i>	Централизованный контроль, гарантия компании	Централизованный контроль, уязвимость пользовательских данных, хранимых на сторонних серверах, гарантия компании	Защита информации, гарантия компании; авторизация преимущественно через аккаунты веб-гигантов, а также электронные почты (логины и пароли)	Самостоятельная авторизация — self-Sovereign Identity (SSI), контроль цифровой идентификации с использованием NFT (право собственности на «цифровую личность»), безопасность данных гарантируется блокчейн-технологией
<i>Право собственности на создаваемый контент</i>	Владельцы интернет-сайтов	Медиакорпорации, монетизирующие пользовательские данные, в том числе «продавая» рекламодателям. Коммерциализация контента — только через посреднические услуги медиа-корпораций	Пользователь (за счет NFT и т.д.)	
<i>Серверы</i>	Централизованный			Децентрализованный
<i>Интегративная / дезинтегративная функция языка</i>	Существенным образом не повлияло	Новый сетевой язык интернет-коммуникации: — принцип «нет среды без языка, нет языка» ⁷ ; — новые сетевые жанры ⁸ ; — «сетевой жаргон»; — ядро — интернациональные термины-англицизмы	Дополнительно к предшествующему: + машинный перевод сообщений, контента веб-страниц	?
<i>Медиатизация личности</i>	Homo sapiens	Homo digitalis	Homo confusus ⁹	
<i>Способ поиска информация</i>	Каталоги	Ключевые слова (теги), гипертекстовые связи	Гипертекстовые и семантические связи	

⁷ Кобенко Ю. В., Солодовникова О. В. Сегментация словарного состава немецкого литературного языка сквозь призму средового подхода // Вестник Томского государственного педагогического университета. 2019. № 4. С. 68.

⁸ Блог, влог, фанфик, паблик, рилз, секстинг, мемы, демотиваторы, подкасты и пр.

⁹ Черниговская Т. В. Человек растерянный: Homo Confusus и новая цифровая реальность // URL: <https://www.litres.ru/audiobook/t-v-chernigovskaya/lekciya-chelovek-rasteryannyi-homo-confusus-i-novaya-ci-42133413/> (дата обращения: 05.04.2024).

Критерий	Web 1.0	Web 2.0	Web 3.0	Web 3
Фейковизация	Существенным образом не повлияло	Рост в геометрической прогрессии «мусорного» контента (флуда), фейкового и иного деструктивного контента, распространяемого в том числе анонимно или под псевдонимами	+ Активное использование дипфейков для создания симулякров	
Цензура	Возведенная в абсолют свобода слова	Цензура возможна со стороны медиа-корпораций	Цензура отсутствует, только законодательно установленные ограничения распространения информации или потенциально возможно установление ограничений коллективным решением DAO	

Понятие «Web 1.0» вошло в обиход одновременно с понятием «Web 2.0», когда в 2005 г. Тим О’Рейли в статье *What Is Web 2.0? Design Patterns and Business Models for the Next Generation of Software*¹⁰ отразил эволюцию развития веб-пространства, перехода к новым программным сервисам.

Фактически переход к Web 2.0 означает смену принципа *read only* («только чтение» — односторонний канал коммуникации, характерный для традиционных СМИ) на принцип *read and write*, предполагающий взаимодействие пользователей и генерацию контента самими пользователями (UGC, *User Generated Content* — пользовательский контент), создание личных кабинетов и профилей в веб-сервисах, персонализацию (возможность самому выбирать дизайн своего профиля и наполнение его сторонним контентом) и т.д. Для Web 2.0 характерна сетевая экстерналия — феномен, означающий, что каждый пользователь влияет на развитие системы в целом.

К иным характеристикам Web 2.0 можно отнести:

— динамические веб-страницы (CGI);

— регистрация и авторизация на сайтах (в сервисах);

— сервисы, концепция которых построена на наполнении контентом исключительно самими пользователями (социальные сети, мессенджеры, блог-платформы, форумы, видеохостинги, «свободные» энциклопедии и т.п.);

— возможность коллективного выполнения работ.

Web 2.0 — это эра рассвета социальных сетей, блогов и других новых медиа; это переход от «витринного» Интернета (веба) к социальному вебу с акцентом на «юзабилити» (от англ. *usability* — «удобство и простота использования, степень удобства использования»), дизайн и интерактивность.

Использование в коммуникативной практике социальных сетей представляет собой неконтролируемое разветвление каналов передачи информации, генерация контента самими пользователями влечет преобразование линейной формы коммуникации в сетевую, хаотичную¹¹. Указанный процесс М. Б. Ворошилова предлагает именовать **ризоморфизацией**¹² — от термина «ризома», под которым

¹⁰ O’Reilly T. *What Is Web 2.0? Design Patterns and Business Models for the Next Generation of Software* // September 30, 2005. URL: <https://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html> (дата обращения: 05.04.2024).

¹¹ Строганов В. Б. Политическая ризоморфизация Интернета как форма «мягкой силы» // Мобильность как измерение мягкой силы: теория, практика, дискурс : сборник научных трудов по итогам Первой Всероссийской научно-практической молодежной конференции, Екатеринбург, 17 октября 2018 г. Екатеринбург : Дискурс-Пи, 2019. С. 277.

¹² Ворошилова М. Б. «Ризоморфизация» социальных сетей как этап перехода к системе Web 3.0 // Социальные сети: комплексный лингвистический анализ. С. 30–40.

понимается разветвленная корневая система с множеством «узлов», отменяющая жесткую иерархию отдельных элементов¹³. При этом стоит иметь в виду, что информационные кампании в социальных сетях представляют собой **«управление хаосом»**: при внешней неструктурированности, бессистемности, хаотичности информационные «вбросы» и кампании зачастую имеют признаки организованного характера. Так, при исследовании в 2021 г. в социальных сетях колумбайн-сообществ, внешне представляющих собой разрозненные фан-сообщества, нами было установлено, что один пользователь администрировал в среднем 7 колумбайн-сообществ, т.е. осуществлялась системная организованная деятельность по продвижению террористической идеологии скулшутинга в русскоязычном сегменте Интернета.

Начиная с Web 2.0, пользователи не только генерируют контент, но и активно оставляют информацию о себе, а аналитика данной информации и UGC позволяет формировать «цифровой портрет» пользователя, в том числе характеристику его предпочтений, интересов и т.д. Такой «цифровой портрет» — это товар, который медиаплатформа может продавать рекламодателям или самостоятельно использовать для продвижения собственных продуктов. Таким образом, бесплатные интернет-сервисы предоставляют свой функционал в обмен: 1) на возможность размещения встроенной рекламы, которую пользователь вынужден просматривать целиком, на время рекламы функционал сервиса недоступен¹⁴; 2) возможность сбора информации о пользователе, формирования его «цифрового портрета».

При этом механизмы Web 3.0 позволяют алгоритмизированно собирать и с использованием искусственного интеллекта обрабатывать массивы информации о пользователе на основе анализа не только указанных в профиле сведений, размещаемого пользователем контента,

проявленных реакций (лайков/дизлайков и т.п.), т.е. так называемых активных цифровых следов пользователя, но и на основе пассивных цифровых следов — сведений о его пользовательском поведении, которые он сам публично не размещал, например поисковые запросы; данные о переходах по гиперссылкам; сведения о том, просмотрел ли пользователь до конца конкретное видео, сколько раз он посмотрел видео конкретной тематики и т.п.

Как отмечают австрийские исследователи, одной из ярких характеристик современного веб-пространства выступает широкое распространение таргетированной информации, в том числе с целью получения конфиденциальной информации¹⁵.

Фактически Web 2.0 (собственно, как и Web 3.0) подразумевает мнимую человекоцентричность: под вуалью индивидуализации контента и сервисов для пользователей скрывается манипуляция пользователями, в Web 3.0 — в том числе через погружение их в «семантические капсулы» (информационные колодцы) посредством последовательного пропуска сквозь «пузыри фильтров». Иными словами, использование алгоритмов больших данных и искусственного интеллекта позволяет «подсовывать» пользователям «нужный» контент, преобразуя «тоннель виртуальной реальности» пользователей. Стоит отметить, что поисковые системы в киберпространстве типа Web 3.0 не только ищут указанные ключевые слова, но и интерпретируют контекст, в котором они представлены¹⁶. Указанные манипуляции осуществляются как в маркетинговых целях, так и в целях навязывания определенных ценностей и установок, изменения мировоззрения пользователей. Таким образом, киберпространство типа Web 2.0 (и особенно Web 3.0) — это пространство мнимой свободы выбора, выбор без выбора в условиях цензуры контента владельцами медиаплатформ, навязывания нарративов и

¹³ Современная западная философия : словарь. 2-е изд., перераб. и доп. М. : Остожье, 1998. С. 357.

¹⁴ Один из очевидных примеров с точки зрения угроз медиабезопасности — факты размещения «рекламных» заставок просуицидального характера в приложении, ориентированном на детскую аудиторию.

¹⁵ Krombholz K., Hobel H., Huber M., Weippl E. Advanced social engineering attacks // Journal of Information Security and Applications. 2015. № 22. P. 113–122 ; Richard G. B., William B. B., Lewis C. Flying under the radar: Social engineering // International Journal of Accounting and Information Management. 2012. Vol. 20. No. 4. P. 335–347 ; Тумбинская М. В. Процесс распространения нежелательной информации в социальных сетях // Бизнес-информатика. 2017. № 3 (41). С. 65–76.

¹⁶ Fuchs C., Hofkirchner W., Schafranek M., Raffl C., Sandoval M., Bichler R. Theoretical Foundations of the Web: Cognition, Communication, and CoOperation. Towards an Understanding of Web 1.0, 2.0, 3.0 // Future Internet. 2010. № 2. P. 41–59.

формирования у пользователей симулякров — псевдообразов несуществующих явлений.

Развитие киберпространства типов (этапов) Web 2.0 — Web 3.0 можно обозначить как развитие «Интернета для корпораций», т.к. в интернет-среде суверенитет преломляется через призму «сетевой власти», обладателями которой выступают крупнейшие медиахолдинги. Например, медиагиганты Google, Amazon, Facebook (Meta¹⁷), Apple, Microsoft («большая киберпятерка» GAFAM) используют искусственный интеллект и аналитику больших данных для продвижения идеологически «правильного» контента и цензуры «неудобного» контента и пользователей¹⁸.

К основным характеристикам Web 3.0 можно отнести:

- мультимедийные технологии;
- персонализацию/кастомизацию контента с использованием алгоритмов ИИ и big data (в том числе рекомендательные алгоритмы);
- системы рейтинга;
- мем-комплексы¹⁹.

Вышесказанное позволяет обозначить в качестве основной идеи киберпространства типа

Web 3.0 построение семантической паутины (семантического веба), т.е. глобальной семантической сети, формируемой посредством стандартизации представления информации в виде, пригодном для машинной обработки UGC с использованием различных семантических моделей²⁰. Существуют несколько языков для записи семантических моделей, основными из которых являются RDF/RDFS (Resource Description Framework)²¹ и OWL (Ontology Web Language)²².

Г. Хассельбалх, исследователь этики и политики использования данных и искусственного интеллекта, рассматривает ИИ как социотехническую эволюцию систем больших данных²³ и вводит понятия социотехнических инфраструктур больших данных (Big data Sociotechnical Infrastructures — BDSTIs), которые отвечают за пространство, и социотехнических инфраструктур ИИ (Artificial Intelligence Sociotechnical Infrastructures — AISTIs), которые отвечают за время. «Иными словами, собранные большие данные — это прошлое, на основе которого ИИ обучается в настоящем и влияет на будущее»²⁴.

Г. Хассельбалх затрагивает и проблемы «ценностного» наполнения BDSTIs и AISTIs,

¹⁷ Решением Тверского районного суда города Москвы от 21.03.2022 компания «Мета Платформс, Инк.» (Meta Platforms, Inc.) признана экстремистской организацией и ее деятельность запрещена на территории Российской Федерации.

¹⁸ Дегтерев Д. А. Ценностный суверенитет в эпоху глобальных конвергентных медиа // Вестник РУДН. Серия «Международные отношения». 2022. № 2. С. 354.

¹⁹ См. также об американском проекте DARPA «Социальные медиа в стратегических коммуникациях», посвященном методам информационно-психологического воздействия, в том числе с использованием метаметической инженерии: Waltzman R. The Story Behind the DARPA Social Media in Strategic Communication (SMISC) Program // Information Professionals Association. 2015. April. URL: <https://information-professionals.org/the-darpa-social-media-in-strategic-communication-smisc-program> (дата обращения: 05.04.2024).

²⁰ См. также: Plesniewicz G., Karabekov B. Specifying temporal knowledge for workflows ontologies // Open Computer Science. 2016. Vol. 6. No. 1. P. 226–231; Hendler J. Op. cit.

²¹ Chernenkiy V. et al. Using the metagraph approach for addressing RDF knowledge representation limitations // Internet Technologies and Applications (ITA). 2017. P. 47–52; Plesniewicz G. S. Masherov D. E., Nguen Thi Min Vu, Karabekov A. B. «Binary Knowledge Model»: Specifying, instantiating, and interpreting advanced ontologies // 9th International Conference on Application of Information and Communication Technologies (AICT). 2015. P. 314–318; Kurbatov S., Fominykh I., Vorobyev A. Cognitive Patterns for Semantic Presentation of Natural-Language Descriptions of Well-Formalizable Problems // Artificial Intelligence. RCAI 2021. Lecture Notes in Computer Science. Vol. 12948 / S. M. Kovalev, S. O. Kuznetsov, A. I. Panov (eds). Springer, Cham.

²² Mishra D. S. et al. Natural language query formalization to SPARQL for querying knowledge bases using Rasa // Progress in Artificial Intelligence. 2022. Vol. 11. No. 3. P. 193–206; Lassila O., Hendler J. Op. cit.; Bobe A., Konyshov D., Vorotnikov S. Emotion Recognition System for Human-Robot Interface: Comparison of Two Approaches // Interactive Collaborative Robotics. ICR 2017. Lecture Notes in Computer Science. 2017. Vol. 10459. A. Ronzhin, G. Rigoll, R. Meshcheryakov (eds). Springer, Cham.

²³ Hasselbalch G. Data Ethics of Power: A Human Approach in the Big data and AI Era. Cheltenham; Northampton, MA: Edward Elgar, 2021.

²⁴ Коваль Е. А. Новые алгоритмы власти в мире алгоритмов. Рец. на кн.: Hasselbalch G. Data Ethics of Power: A Human Approach in the Big data and AI Era. Cheltenham; Northampton, MA: Edward Elgar, 2021. 208 p. // Мониторинг общественного мнения: экономические и социальные перемены. 2023. № 5. С. 271.

ведь внедрение ИИ и использование больших данных предполагает не просто «оцифровку» социальных норм, а трансформацию этих норм и ценностных установок в условиях «распределенной агентности» с участием «нечеловеческой (nonhuman) агентности»²⁵, когда ИИ выступает активным посредником или участником в социальных взаимодействиях. Таким образом, на первый план выходит проблема законодательного регулирования степени свободы разработчиков систем ИИ в выборе ценностей, закладываемых при обучении нейросетей. Как подчеркивает Г. Хассельбалх, эти ценности и будут потом влиять на «моральные факторы социальной среды»²⁶.

Большинство исследователей упоминают исключительно классификацию «Web 1.0 — Web 2.0 — Web 3.0», однако некоторые выделяют отдельно Web 3, определяя его собственные архитектурные модели. На наш взгляд, в данном типе киберпространства функционируют, как и в Web 3.0, персонализированные медиа (принцип «многие — одному»), однако ключевым распорядителем данных становится не владелец интернет-ресурса, а сам пользователь, т.е. речь идет о смене «Интернета для корпораций» на «Интернет для создателей».

В основе концепции Web 3 лежит идея децентрализации информации, функционирования бессерверного децентрализованного веба, призванного **вернуть пользователям право владения данными**. Данная цель может быть достигнута посредством децентрализации с использованием суверенной идентификации на базе DAO (децентрализованных автономных организаций)²⁷.

К основным характеристикам Web 3 можно отнести:

- «сеть сетей»;
- веб как база данных;
- децентрализованные приложения (DApp);
- блокчейн;
- искусственный интеллект, big data, но отсутствие рекомендательных алгоритмов;

- прозрачность (программное обеспечение с открытым исходным кодом);
- криптовалюта;
- смарт-контракты;
- NFT, токенизация интернет-активности;
- иммерсивное пространство: метавселенные как новая версия интернет-интерфейса, включая AR, VR и т.д.;
- SocialFi (социальные сети для социальных финансов);
- экспансия NLP (технологий обработки естественного языка) и голосовых помощников;
- расцвет использования IoT-устройств и смартгаджетов.

Децентрализация обеспечивает более персонализированный, эффективный и контролируемый самим пользователем опыт поиска, а также в целом более высокую степень контроля пользователя над личными данными и конфиденциальностью. Для описания этой концепции аналитики нередко используют формулу «read — write — own», т.е. «читай — пиши — владей»²⁸. Полагаем целесообразным дополнить эту формулу: «read — write — own», в том числе «read and write» в «семантической капсуле», управляемой самим пользователем.

Если для Web 1.0 — Web 2.0 характерна зависимость качества работы сервисов от конкретных компаний-владельцев, то Web 3.0 подразумевает сетевую экосистемность и «медиахолдинговую олигополию», т.к. пользовательские портреты принадлежат ограниченной группе корпораций (веб-гигантов). За счет использования технологии блокчейн и невзаимозаменяемых токенов NFT²⁹ пользователь Web 3 может самостоятельно управлять личными данными, в том числе определять круг субъектов доступа к ним и действий в отношении них (право собственности на «цифровую личность»).

Таким образом, если в Web 1.0 безопасность данных обеспечивалась централизованным контролем с гарантией компании (владельца интернет-сервиса); в Web 2.0 — аналогично,

²⁵ Hasselbalch G. Op. cit. P. 80.

²⁶ Hasselbalch G. Op. cit. P. 80.

²⁷ Намиот Д. Е., Куприяновский В. П. Архитектурные модели Web3 // International Journal of Open Information Technologies. 2024. № 2. С. 84–95.

²⁸ Рвачев Н. А. Революция в мире маркетинга: как Web 3.0 меняет лицо бизнеса // Инновации и инвестиции. 2022. № 8. С. 51.

²⁹ Алгоритм, позволяющий присвоить любому цифровому контенту отметку уникальности и затем передавать право на его владение другим игрокам рынка.

при этом появились массивы пользовательских данных, хранимых на сторонних серверах и уязвимых; для Web 3.0 характерно развитие средств защиты информации, при этом 1) их использование зависит от владельца интернет-сервиса, 2) тренд на авторизацию преимущественно через аккаунты веб-гигантов сосредотачивает пользовательские данные в олигополии веб-гигантов; то в Web 3 подразумевается альтернативный подход к управлению цифровой идентификацией, самостоятельная авторизация (Self-Sovereign Identity — SSI).

SSI подразумевает, что каждый интернет-пользователь контролирует все аспекты своей цифровой личности, что гарантирует конфиденциальность и безопасность³⁰.

Последний критерий, на котором хотелось бы остановиться в рамках настоящей статьи, — это цензура. На заре своего существования интернет позиционировался как пространство анонимности и возведенной в абсолют свободы слова, в Web 2.0 — Web 3.0, как было указано выше, осуществляется цензура со стороны медиакорпораций, а в Web 3 предполагается отсутствие цензуры, что не отменяет возможности установления ограничений распространения информации на уровне законодательства или посредством коллективного решения DAO.

В настоящее время лишь отдельные сервисы соответствуют основным характеристикам Web 3, однако основываются всё еще на принципах централизации. С одной стороны, децентрализация и полноценное функционирование инфраструктуры киберпространства типа Web 3 будут иметь очевидные преимущества (в аспекте и защиты от манипуляций, и электронной коммерции, и т.п.), с другой стороны, возникает необходимость принципиального пересмотра правовых подходов к регулированию интернет-отношений, выработки новых нормативных моделей в этой сфере, в том числе ввиду риска роста киберпреступности.

Концепция «Web 1.0 — Web 2.0 — Web 3.0 — Web 3» отражает не признаковое разграничение неких изолированных типов веб-пространства, а ключевые вехи эволюции веба как такового, при этом данные этапы (вехи) не изолированы, границы размыты, признаки различных типов веб-пространства могут проявляться в один и тот же период, когда отдельные медиахолдинги внедряют инновации, связанные уже с другим типом веб-пространства.

Эволюция веб-пространства, в особенности переход к моделям Web 3.0 и Web 3, в высшей степени воздействует на изменение социальных связей, сущностную трансформацию и отчасти революцию экономических моделей, трансформацию общественных отношений в целом, поэтому указанная проблематика нуждается в дальнейшем глубоком междисциплинарном анализе для выстраивания надлежащих правовых рамок, реализации нормативных моделей, обеспечивающих защиту от манипулирования с использованием средств социальной инженерии и цифровую безопасность интернет-пользователей в целом.

5. Синтезируя концепты: современная система медиабезопасности и когнитивного суверенитета

С точки зрения широкого толкования концепт **когнитивного суверенитета государства** можно рассматривать как совокупность двух важных аспектов: 1) независимость от каких-либо внешних сил в реализации политики государства, связанных с познавательной деятельностью, в том числе информационной политики, политики в области образования и науки, культурной политики, правовой политики (нормотворческой и правоприменительной); 2) независимость в целеполагании, стратегическом планировании и принятии управленческих решений в условиях защищенности от навязывания социально-экономических практик, чуждых цивилизационному коду государства (суверенные управленческие практики) (см. рис. 4).

Таким образом, когнитивный суверенитет включает в себя следующие взаимопересекающиеся и взаимодополняющие составляющие, обеспечивающие указанные два аспекта:

1. **Медиабезопасность** как состояние защищенности ментально-когнитивного иммунитета населения от внешнего деструктивного информационно-психологического воздействия, в том числе вовлечения в сообщества аутодеструктивной и гетероагрессивной направленности; пропаганды противоправного поведения; пропаганды установок, противоречащих традиционным российским духовно-нравственным ценностям; фальсификации истории и политической пропаганды через распространение фейковой информации; распространения дискредитирующего и диффамационного контента

³⁰ Mühle A. et al. Op. cit. P. 80–86.

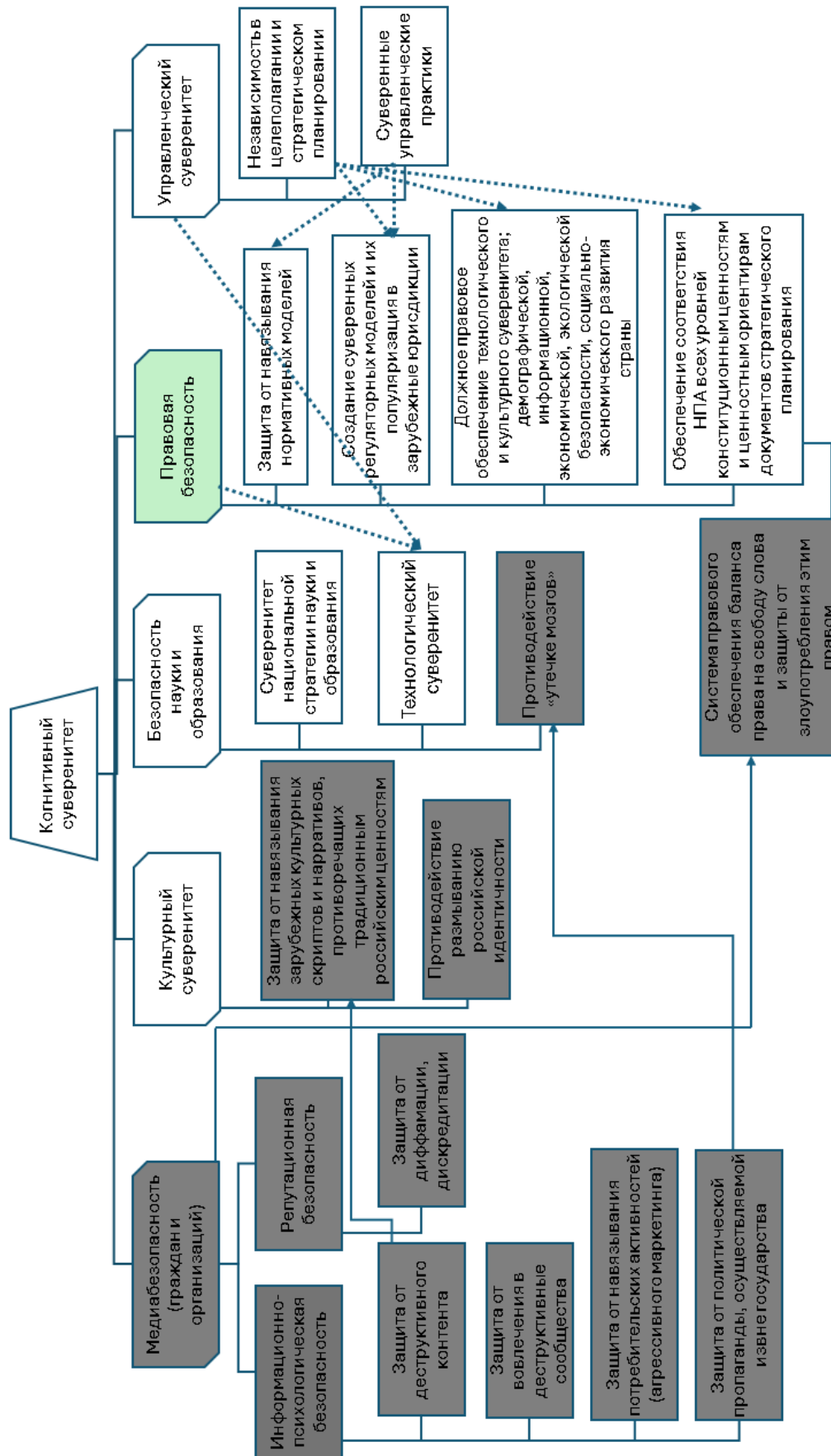


Рис. 4. Системные элементы когнитивного суверенитета государства

(репутационная безопасность); манипулирование потребительской активностью (в том числе через агрессивный маркетинг) и т.д.

Обеспечение медиабезопасности тесно связано с *правовой политикой* государства, выстраиванием такой регуляторной модели, которая обеспечивает баланс права на свободу слова и защиту от злоупотребления этим правом, т.е. защиту прав иных лиц от манипулятивного воздействия.

2. Культурный суверенитет как независимость от каких-либо сил, обстоятельств и лиц в реализации культурной политики государства, что предполагает не только обеспечение медиабезопасности, но и защиту от «мягкой силы» иностранных государств, предпринимающих попытки размывания российской идентичности, навязывания культурных образцов (скриптов), обычаев, трендов моды и брендов, моделей поведения, причем в случае пропаганды деструктивной идеологии данные нарративы идут в разрез с традиционными российскими духовно-нравственными ценностями.

3. Безопасность науки и образования — независимость от каких-либо сил, обстоятельств и лиц в реализации политики государства в области образования и науки, что требует реализации суверенной стратегии развития научно-образовательной отрасли, обеспечения технологического суверенитета и противодействия «утечке мозгов» вследствие политической пропаганды, осуществляемой извне государства, и воздействия «мягкой силы».

Обеспечение **технологического суверенитета** является приоритетной задачей социально-экономического развития России и связано практически со всеми составляющими когнитивного суверенитета, в том числе с независимостью в рамках стратегического планирования, суверенными управленческими практиками, а также разработкой нормативно-правовых моделей опережающего развития, использованием права как драйвера, а не барьера научно-технологического развития.

4. Управленческий суверенитет предполагает независимость от каких-либо сил, обстоятельств и лиц в целеполагании, стратегическом планировании, развитие суверенных управленческих практик, критический подход при внедрении заимствуемых управленческих практик, защиту от внедрения социально-экономических практик, чуждых цивилизационному коду го-

сударства. Как отмечает Д. А. Дегтерев, «ценностная повестка в конечном счете определяет и расстановку приоритетов для целеполагания при стратегическом планировании»³¹.

5. Правовая безопасность выступает синтезирующей материей в вышеприведенной концепции двух аспектов когнитивного суверенитета государства. С одной стороны, правовая безопасность призвана обеспечить: 1) соответствие нормативных правовых актов всех уровней конституционным ценностям и ценностным ориентирам документов стратегического планирования; 2) должное правовое обеспечение технологического и культурного суверенитета, демографической, информационной, экономической, экологической безопасности, социально-экономического развития страны; 3) суверенные регуляторные модели и их популяризацию в зарубежных юрисдикциях, что тесно связано с защитой от навязывания нормативных моделей. С другой стороны, право как социальный регулятор призвано нормативно обеспечить управленческий суверенитет государства.

Правовая безопасность России предполагает, что правотворческая и правоприменительная деятельность должна проходить сквозь призму российской ментальности и ценностных ориентиров, заложенных в документах стратегического планирования.

Заключение

В рамках данного исследования были рассмотрены основные технологии (в том числе социогуманитарные), выступающие вызовами прежде всего для обеспечения медиабезопасности интернет-пользователей, организаций и когнитивного суверенитета государства и требующие, соответственно, выработки новых нормативных моделей.

Рассмотрены содержание и взаимосвязь ключевых концептов семантического поля «медиабезопасность и когнитивный суверенитет», что имеет теоретико-практическую значимость для разработки единого терминологического аппарата в указанной сфере.

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

³¹ Дегтерев Д. А. Указ. соч. С. 359.

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.

Исследование носит в определенной степени футуристический характер и затрагивает не только текущие вызовы праву, но и про-

гнозируемые с позиции трендов развития киберпространства (прежде всего в рамках концепций Web 3.0, Web 3). В этой связи с точки зрения юридической инноватики важна роль юристов-стратегов (юристов-правотворцев), выступающих социальными инженерами и разрабатывающих модели регулирования не только текущих, но и зарождающихся, а также прогнозируемых общественных отношений.

СПИСОК ЛИТЕРАТУРЫ

- Бронников И. А., Беденкова А. С. Метавселенные и государства: вместе или порознь // *Ars Administrandi*. 2023. № 2. С. 224–250.
- 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.
- Кастельс М. Галактика Интернет : Размышления об Интернете, бизнесе и обществе. Екатеринбург : У-Фактория, 2004. 328 с.
- Кобенко Ю. В. Аспекты медийной коммуникации в социальных сетях // *Вестник Санкт-Петербургского университета. Язык и литература*. 2023. № 20 (1). С. 183–190.
- 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.
- Курилкин А. В. Информационные операции и кибервойна: от истории к современности. М. : Горячая линия — Телеком, 2022. 164 с.
- Макашова В. В. Дезинформация как элемент технологий управления смыслами // *МедиаВектор*. 2023. № 9. С. 84–88.
- Моисеева А. П. Генезис социальной инженерии в контексте междисциплинарности // *Известия ТПУ*. 2012. № 6. С. 64–69.
- Намиот Д. Е., Куприяновский В. П. Архитектурные модели Web 3 // *International Journal of Open Information Technologies*. 2024. № 2. С. 84–95.
- Поппер К. Открытое общество и его враги : пер. с англ. Т. 1. М. : Международный фонд «Культурная инициатива», 1992. 448 с.
- Резник Ю. М. Социальная инженерия: предметная область и границы применения // *Социологические исследования*. 1994. № 2. С. 87–96.
- Роблес-Каррильо М. Суверенитет и цифровой суверенитет // *Journal of Digital Technologies and Law*. 2023. № 3. С. 673–690.
- Сарна А. Я. Технологии воздействия на аудиторию в современном медиа-пространстве // *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.
- Bobé A., Konyshov D., Vorotnikov S. Emotion Recognition System for Human-Robot Interface: Comparison of Two Approaches // *Interactive Collaborative Robotics. ICR 2017. Lecture Notes in Computer Science*. 2017. Vol. 10459. A. Ronzhin, G. Rigoll, R. Meshcheryakov (eds). Springer, Cham.
- Cuihong Cai. Building a New Digitalised World through Technology Centrism // *Digital Debates: CyFy Journal*. 2020. P. 48–53.
- Ellul J. Histoire de la propaganda. Paris : Presses Universitaires de France, 1967. 128 p.
- Ellul J. Propaganda: The formation of men's attitudes / transl. K. Kellen, J. Lerner. New York : Random House / Vintage, 1973. 352 p.

Fuchs C., Hofkirchner W., Schafranek M., Raffl C., Sandoval M., Bichler R. Theoretical Foundations of the Web: Cognition, Communication, and CoOperation. Towards an Understanding of Web 1.0, 2.0, 3.0 // *Future Internet*. 2010. № 2. P. 41–59.

Plesniewicz G. S. Masharov D. E., Nguyen Thi Min Vu, Karabekov A. B. «Binary Knowledge Model»: Specifying, instantiating, and interpreting advanced ontologies // 9th International Conference on Application of Information and Communication Technologies (AICT). 2015. P. 314–318.

Hasselbalch G. Data Ethics of Power: A Human Approach in the Big data and AI Era. Cheltenham ; Northampton, MA: Edward Elgar, 2021. 208 p.

Hendler J. Web 3.0 Emerging // *Computer* 42.1. 2009. P. 111–113.

Krombholz K., Hobel H., Huber M., Weippl E. Advanced social engineering attacks // *Journal of Information Security and Applications*. 2015. № 22. P. 113–122.

Kurbatov S., Fominykh I., Vorobyev A. Cognitive Patterns for Semantic Presentation of Natural-Language Descriptions of Well-Formalizable Problems // *Artificial Intelligence. RCAI 2021. Lecture Notes in Computer Science*. Vol. 12948 / S. M. Kovalev, S. O. Kuznetsov, A. I. Panov (eds). Springer, Cham.

Lassila O., Hendler J. Embracing «Web 3.0» // *IEEE Internet computing*. 2007. Vol. 11. No. 3. P. 90–93.

Mishra D. S. et al. Natural language query formalization to SPARQL for querying knowledge bases using Rasa // *Progress in Artificial Intelligence*. 2022. Vol. 11. No. 3. P. 193–206.

Mühle A. et al. A survey on essential components of a selfsovereign identity // *Computer Science Review*. 2018. No. 30. P. 80–86.

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

Plesniewicz G., Karabekov B. Specifying temporal knowledge for workflows ontologies // *Open Computer Science*. 2016. Vol. 6. No. 1. P. 226–231.

Pohle J., Thiel T. Digital Sovereignty // *Internet Policy Review*. 2020. Vol. 9. No. 4. P. 1–19.

Pound R. Mechanical Jurisprudence // *Columbia Law Review*. 1908. Vol. 8. P. 605–623.

Richard G. B., William B. B., Lewis C. Flying under the radar: Social engineering // *International Journal of Accounting and Information Management*. 2012. Vol. 20. No. 4. P. 335–347.

Chernenkiy V. et al. Using the metagraph approach for addressing RDF knowledge representation limitations // *Internet Technologies and Applications (ITA)*. 2017. P. 47–52.

Yeli H. A. Three-Perspective Theory of Cyber Sovereignty // *PRISM*. 2017. Vol. 7. No. 2. P. 109–115.

REFERENCES

Bobе A, Konyshеv D, Vorotnikov S. Emotion Recognition System for Human-Robot Interface: Comparison of Two Approaches. *Interactive Collaborative Robotics. ICR 2017. Lecture Notes in Computer Science*. Vol. 10459. Ronzhin A, Rigoll G, Meshcheryakov R, editors. Springer, Cham.

Bronnikov IA, Bedenkova AS. Metaverses and states: Together or separately. *Ars Administrandi*. 2023;2:224-250. (In Russ.).

Castells M. Galaxy Internet: Reflections on the Internet, business and society. Ekaterinburg: U-Factoriya Publ.; 2004. (In Russ.).

Chernenkiy V et al. Using the metagraph approach for addressing RDF knowledge representation limitations. *Internet Technologies and Applications (ITA)*. 2017:47-52.

Cuihong Cai. Building a New Digitalised World through Technology Centrism. *Digital Debates: CyFy Journal*. 2020:48-53.

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 propagande. Paris: Presses Universitaires de France; 1967.

Ellul J. Propaganda: The formation of men's attitudes. Transl. by 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.).

- Fuchs C, Hofkirchner W, Schafranek M, Raffl C, Sandoval M, Bichler R. Theoretical Foundations of the Web: Cognition, Communication, and CoOperation. Towards an Understanding of Web 1.0, 2.0, 3.0. *Future Internet*. 2010;2:41-59.
- Hasselbalch G. Data Ethics of Power: A Human Approach in the Big data and AI Era. Cheltenham; Northampton, MA: Edward Elgar; 2021.
- Hendler J. Web 3.0 Emerging. *Computer*. 2009;42.1;111-113.
- Kobenko YuV. Aspects of media communication in social networks. *Vestnik Sankt-Peterburgskogo universiteta. Yazyk i literatura [Vestnik of Saint Petersburg University. Language and literature]*. 2023;20(1):183-190. (In Russ.).
- Kochetkov AP, Maslov KV. Digital Sovereignty as the basis of Russia's National Security in a global digital society. *Vestnik Moskovskogo Universiteta. Seriya 12, Politicheskie nauki*. 2022;2:31-45. (In Russ.).
- Krombholz K, Hobel H, Huber M, Weippl E. Advanced social engineering attacks. *Journal of Information Security and Applications*. 2015;22:113-122.
- Kurbatov S, Fominykh I, Vorobyev A. Cognitive Patterns for Semantic Presentation of Natural-Language Descriptions of Well-Formalizable Problems. Artificial Intelligence. RCAI 2021. Lecture Notes in Computer Science. Vol. 12948. Edited by S.M. Kovalev, S.O. Kuznetsov, A.I. Panov. Springer, Cham.
- Kurilkin AV. Information operations and cyberwarfare: From history to the present. Moscow: Goryachaya liniya — Telekom; 2022. (In Russ.).
- Lassila O, Hendler J. Embracing «Web 3.0». *IEEE Internet computing*. 2007;11(3):90-93.
- Makashova VV. Disinformation as an element of meaning management technologies. *MediaVektor*. 2023;9:84-88. (In Russ.).
- Mishra DS et al. Natural language query formalization to SPARQL for querying knowledge bases using Rasa. *Progress in Artificial Intelligence*. 2022;11(3):193-206.
- Moiseeva AP. The genesis of social engineering in the context of interdisciplinarity. *Izvestiya TPU*. 2012;6:64-69. (In Russ.).
- Mühle A et al. A survey on essential components of a selfsovereign identity. *Computer Science Review*. 2018;(30):80-86.
- Namiot DE, Kuprianovsky VP. Architectural models of Web3. *International Journal of Open Information Technologies*. 2024;2:84-95. (In Russ.).
- Noor E. Rethinking Decoupling: Interdependence, Dependence, Independence. *Digital Debates: CyFy Journal*. 2020:36-46.
- Plesniewicz G, Karabekov B. Specifying temporal knowledge for workflows ontologies. *Open Computer Science*. 2016;6(1):226-231.
- Plesniewicz GS, Masherov DE, Nguen Thi Min Vu, Karabekov AB. «Binary Knowledge Model»: Specifying, instantiating, and interpreting advanced ontologies. 9th International Conference on Application of Information and Communication Technologies (AICT). 2015. Pp. 314–318.
- Pohle J, Thiel T. Digital Sovereignty. *Internet Policy Review*. 2020;9(4):1-19.
- Popper K. The open society and its enemies. Transl. from English. Vol. 1. Moscow: International Foundation «Cultural Initiative»; 1992. (In Russ.).
- Pound R. Mechanical Jurisprudence. *Columbia Law Review*. 1908;8:605-623.
- Reznik YuM. Social engineering: Domain area and application boundaries. *Sotsiologicheskie issledovaniya*. 1994;2:87-96. (In Russ.).
- Richard GB, William BB, Lewis C. Flying under the radar: Social engineering. *International Journal of Accounting and Information Management*. 2012;2(4):335-347.
- Robles-Carrillo M. Sovereignty and Digital Sovereignty. *Journal of Digital Technologies and Law*. 2023;3:673-690. (In Russ.).
- Sarna AY. Technologies of influencing the audience in the modern media space. *Vestnik Sankt-Peterburgskogo universiteta. Sotsiologiya [Vestnik of Saint Petersburg University. Sociology]*. 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.).
- Yeli HA. Three-Perspective Theory of Cyber Sovereignty. *PRISM*. 2017;7(2):109-115.

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 22 ноября 2024 г.*

*Received 20.03.2024.
Revised 14.10.2024.
Accepted 22.11.2024.*