ИНТЕРНЕТ СЕГОДНЯ И ЗАВТРА

Сборник авторских статей
к Четырнадцатому российскому форуму по управлению интернетом
(RIGF 2024)
9–10 апреля 2024 г.

АНО «Центр глобальной ИТ-кооперации»
ANO Center for Global IT-Cooperation (CGITC)

Москва, 2024

Для цитирования / for citation:
«Интернет сегодня и завтра», Сборник авторских статей к Четырнадцатому российскому форуму по управлению интернетом - RIGF 2024, Центр глобальной ИТ-кооперации, Москва, 2024, С. 67

«Internet Today and Tomorrow», Collection of author's articles for the XIV Russian Internet Governance Forum - RIGF 2024, Center for Global IT Cooperation, Moscow, 2024, P. 67

АНО «Центр глобальной ИТ-кооперации»
ANO «Center for Global IT-Cooperation» (CGITC)
https://cgitc.ru/

Редакторы-составители: **Игнатьев А.Г., Шамраев Р.А.,** АНО «Центр глобальной ИТ-кооперации»
Дизайн и иллюстрации: CGITC (DALL·E 3.0 OpenAI)

Аннотация

К Четырнадцатому российскому Форуму по управлению интернетом (RIGF 2024, 9–10 апреля 2024 г.) Центр глобальной ИТ-кооперации (CGITC) традиционно, уже третий год подряд, представляет сборник экспертных статей по широкому спектру вопросов в рамках тематики развития цифровых технологий и управления Интернетом.

Вниманию профессионального сообщества предлагаются авторские статьи по разнообразным проблемам, связанным с вопросами развития цифровых технологий на российском и международном пространстве. Авторами материалов являются специалисты различных российских и зарубежных площадок и институтов развития, которые в данном случае выступают от своего имени, как профильные эксперты.

Статьи охватывают актуальные вызовы в сфере информационного пространства и цифровой экономики, проблематику внедрения и использования сквозных технологий, задачи укрепления глобального Интернета и российской ИТ-отрасли. Материалы содержат обзорную аналитику, прогнозы, отдельные предложения, рекомендации и выводы.
Сборник выпущен с целью активизировать межинституциональный диалог среди специалистов и придать новый импульс экспертной дискуссии по актуальным проблемам цифровизации и развития Интернет-технологий, включая вопросы выработки сбалансированных позиций и приоритетов для эффективного участия России в международном сотрудничестве в современных условиях.

Мнения, содержательные тезисы и выводы авторов могут не совпадать с позицией и подходами АНО «Центр глобальной ИТ-кооперации». Центр не принимает на себя обязательств или ответственности за использование информации, содержащейся в Сборнике, равно как и не несет ответственности за точность приведенных данных. Используемые авторами материалы и ссылки на сторонние веб-сайты находятся вне контроля CGITC.

Возможные отзывы, мнения, а также различные предложения по развитию кооперации или совместным исследовательским проектам в рамках затронутых в Сборнике вопросов можно направить в адрес CGITC info@cgitc.ru.

АНО «Центр компетенций по глобальной ИТ-кооперации» создан в 2020 году для экспертного изучения вопросов международного сотрудничества в сфере информационных технологий (ИТ), укрепления позиций России в глобальной ИТ-кооперации, а также продвижения новых подходов к многостороннему управлению Интернетом.

CGITC является членом Сектора развития электросвязи (ITU-D) Международного союза электросвязи, участником международного Форума по управлению интернетом (IGF), организатором ежегодного Молодежного цифрового форума (Youth RIGF) и соорганизатором Российского форума по управлению интернетом (RIGF). Российские форумы Youth RIGF и RIGF — это часть инициативы Форумов по управлению Интернетом, которые проводятся по всему миру под эгидой ООН с 2005 года.

Центр проводит исследования и реализует проекты в области цифровой грамотности, управления Интернетом, научно-технического сотрудничества в сфере цифровой экономики, оказывает практическое содействие новым командам и начинающим экспертам по продвижению инноваций и стартапов. Во взаимодействии с международным сообществом и при поддержке заинтересованных специалистов в России CGITC на регулярной основе проводит ряд научных и экспертных круглых столов, конференций и вебинаров. Также в 2024 году CGITC выступает организатором Молодежного цифрового форума.

Правила использования Сборника

Аналитические статьи, включенные в Сборник, подпадают под действие Закона об авторских правах Российской Федерации. Исключительные права на Сборник принадлежат АНО «Центр глобальной ИТ-кооперации» (далее – «правообладатель»).

Сборник может использоваться в целях ознакомления. Допускается размещение активных ссылок на него в информационных источниках без непосредственного копирования его содержания. При любом использовании Сборника активная ссылка на источник обязательна.

Частичное или полное воспроизведение и распространение, а также любое коммерческое использование обзора запрещено без письменного разрешения правообладателя, а также без ссылки на авторов исследования.

Приступая к ознакомлению с материалом, вы подтверждаете свое согласие с изложенными ниже условиями:

- Центр глобальной ИТ-кооперации не несет ответственность за позиции и подходы авторов статей и может не разделять представленные в Сборнике взгляды и рекомендации.
- Правообладатель не принимает на себя обязательства или ответственность за использование информации, содержащейся в Сборнике.
- Информация статей носит исключительно информационный характер и подготовлена на основе открытых источников, признанных надежными, однако правообладатель не несет ответственность за точность приведенных данных.
- Выводы, представленные в статьях, также носят исключительно информационный характер и основаны на данных, полученных из открытых источников, указанных в сносках и библиографии.
- Сборник не является юридическим заключением по вопросам, рассмотренным в нем. Правообладатель не несет ответственность за решения, принятые на основании представленных в Сборнике данных.
- Сборник включает в себя ссылки на сторонние веб-сайты, находящиеся вне контроля правообладателя.

  Правообладатель не несет ответственность за содержание этих ссылок. Такая ответственность во всех случаях возлагается на соответствующего провайдера либо оператора этих сторонних веб-сайтов.

Оглавление

В КОНКУРЕНЦИИ С РАЗУМОМ

(вступительная статья редактора)

Автор: **Игнатьев Андрей**
Центр глобальной ИТ-кооперации
Руководитель аналитического направления
Аспирант Школы философии и культурологии НИУ ВШЭ

Человеческая цивилизация, построенная Homo sapiens или человеком современного анатомического типа, который сформировался не менее чем 200–150 тыс. лет назад[1], достигла такого рубежного этапа трансформации, когда трудно прогнозировать будущее и определять его очертания, ни в социотехническом, ни в экономическом, ни в культурном измерении. Даже в умозрительных контурах и философских терминах с доказательной определенностью нельзя точно охарактеризовать завтрашний виток развития техники на крошечной (в масштабах космоса) планете людей, которая продолжает двигаться вокруг светила, отсчитывая очередной звездный год.

От способности первой речевой коммуникации и передачи информации в форме знаков или сигналов современное человечество, после изобретения письменности, пороха и электричества, овладело техникой передачи электрических сигналов. Сегодня информация в двоичной системе счисления (единица и ноль) с огромными скоростями передается сквозь пространство и время, приобретает совершенно новую природу и функции, становится больше, чем просто набор сигналов, а появление Интернета можно сравнить с обретением новой формы коммуникации или новой речи - Речи 2.0. К 2024 году по разным оценкам примерно около 100 Зеттабайт[2] данных (как значимых, так и совершенно бесполезных и неструктурированных) образуют бесконечный поток контролируемых и стихийных операций, транзакций и цифровых «мутаций», которые во многом определяют жизнь современного общества. Генеративный ИИ способен уже в среднесрочной перспективе значительно увеличить объемы этих данных и цифровой вес глобального Интернета. Вероятно, можно говорить о том, что в мире формируется новая семиотическая среда, на основе которой неизбежно возникнет и новая культура (и новые общественные отношения? новый социальный договор? и новая мораль?). Если так - какова модальность и траектория таких изменений? Способны ли сегодняшние аналитики предвосхитить сценарий будущего и предложить безопасный, социогуманитарный путь развития?

Назначения и режимы использования систем ИИ и приложений на их основе настолько многослойны и многомерны, что их эффективное правовое регулирование должно быть также сложно и также инновационно, как и сами передовые технологии. Тем не менее, продвижение от общих принципов к нормативному регулированию и отраслевой стандартизации сегодня необходимо и оправдано.

[1] А.П. Деревянко, Новые археологические открытия на Алтае и проблема формирования Homo sapiens: лекция памяти проф. Х. Мовиуса, прочитанная в Гарвардском ун-те / А.П. Деревянко; Рос. акад. наук, Сиб. отд-ние, Ин-т археологии и этнографии. – Новосибирск: Изд-во ИАЭТ СО РАН, 2012. – 132 с.
[2] В 2025 г. общий данных на планете увеличится до 175 зеттабайтов (1 зеттабайт — это 10 в 21 степени байтов). IDC, The Digitization of the World. From Edge to Core, 2018, https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf (дата обращения 03.04.2024). По прогнозам ICANN к концу XXI века этот объем может составить более 4 йоттабайт (1 йоттабайт - 1024 зеттабайта).

Чрезвычайность сегодняшней фазы технического развития состоит в том, что обозначенные потоки данных и цифровые «мега-пульсации», повсеместно опоясывающие планету, могут обрабатываться мощнейшими высокопродуктивными вычислительными машинами нового поколения. Преобразуя огромные массивы данных предустановленными, но не всегда прозрачными и контролируемыми алгоритмами, такие машины имитируют человеческий разум, стремятся демонстрировать человекоподобное поведение, когнитивные и даже эмоциональные способности. Масштабное внедрение таких интеллектуальных машин в совокупности с облачными хранилищами образует целые экосистемы, способные влиять на технологический уклад и траекторию дальнейшего мироустройства. В этих условиях научно-обоснованная, общепланетарная политика, принципы и методология управления NBICS-конвергенцией, дальнейшей коэволюцией человека и техники формируются и развиваются неоправданно медленно. А за этапом философского и исследовательского осмысления еще предстоит формализовать результирующие подходы и императивы в практическую нормативную базу.

Решения и действия таких систем, условно названных «искусственным интеллектом» (ИИ), все более встраиваются во все процессы жизнедеятельности человека, легко и трансгранично масштабируются, проникая, по сути, в ткань бытия отдельного человека и всего планетарного социума. Вне зависимости от любых ограничений, амбициозные задачи моделирования человеческого мозга (или цифровой сущности, превосходящей его) уже «зажгли» идеями одержимые головы ученых и разработчиков, порождая самые дерзкие проекты. Машинное обучение дает таким системам ИИ все новые и новые «потоки опыта» из глобальной паутины и огромных мировых библиотек данных (насколько ответственно формируются эти библиотеки и датасеты, всегда ли они отвечают требованиям функциональной корректности и нормативно-техническим стандартам, насколько соблюдаются меры предосторожности при проектировании моделей ИИ - вопросы, на которые не всегда можно дать однозначный ответ). В вычислительную обработку таких машин, помимо текста и видеоданных, поступают цифровые профили и биометрия, оцифрованные жесты и мимика, эмоциональные состояния, нервные импульсы, запахи и вкусовые ощущения, генетические параметры, данные о хромосомах, отвечающих за наследство, характеристики ДНК, результаты астрономических наблюдений, химических экспертиз и многое другое.

Таким образом, отсутствие у машин творческих озарений, эвристических способностей и телесности (биологическое тело и нервная система играют значительную роль для формирования сознания) инженеры пытаются компенсировать в системах ИИ огромной размерностью вычислений, поиском нелинейных корреляций и гиперобъемом самых различных данных. Уже всерьез обсуждается вопрос о возможности создания в цифровой среде субстанции, подобной живой материи со способностью воспроизводства «цифровой жизни» и другими свойствами, подобными или не уступающими биологической жизни. Новым источником «опыта и воспитания» машин в перспективе может стать виртуальная вселенная - искусственный цифровой мир, как прототип

физического, в котором системы будут «взрослеть» и обучаться, выступая цифровыми субъектами внутри такой искусственной среды. Риски последующей «прописки» и легализации таких систем в реальном, физическом мире, в человеческом социуме, в том числе в различных системах управления, пока глубоко не изучены и нам еще предстоит вскрыть сложные взаимосвязи и парадоксальные эмерджентности в новой возникающей парадигме субъекта и объекта, человека и техники.

Такой социотехнический фазовый переход и трансформация происходит в условиях, когда человечество еще не преодолело цивилизационных противоречий и конфликтов, не достигло гармонии в области морали, социальной ответственности и еще находится в поиске справедливых или, по крайней мере, прогрессивных социальных моделей. Далеко не исчерпывающими являются и наши сегодняшние представления о природе собственного сознания - в этом смысле описанные выше воздействия гиперцифровизации, или, по Буданову В.Г., «синергийно переплетенные социотехнические практики»[3], и, как результат, перспектива появления все более «человекоподобных» машин могут восприниматься и как неизбежное напутствие человечеству разобраться с дальнейшим экзистенциальным выбором, прийти к осознанному пониманию своей роли и предотвратить саморазрушение себя и планеты.

Большая советская энциклопедия[4] определяет человека как «общественное существо, представляющее собой высшую ступень развития живых организмов на Земле, способное производить орудия труда, использовать их в своём воздействии на окружающий мир и обладающее сложно организованным мозгом, сознанием и членораздельной речью». Изначально зародившиеся как «современные орудия труда» цифровые технологии и ИИ, как наиболее продвинутое сочетание и кульминация таких технологий, в сегодняшних реалиях приобретают более сложную внутреннюю «механику» и функции, могут оказаться вне контроля, быть использованы не в интересах общества и представить угрозу для субъектности человека или субъектности отдельных стран. На критическом этапе возгонки цифровизации и в условиях «экспансии» алгоритмов, конкурирующих с человеческим интеллектом и получающих все большие полномочия и в Интернете, человеку важно воспользоваться «сложно организованным мозгом» и сознанием («как в высшей степени самореферентной системой»[5]) для комплексного анализа происходящих процессов, выработки и реализации рациональных путей развития техники во благо общества.

Не отказываясь от прогрессивных инноваций и воспринимая такой вызов, как неизбежный этап развития техники, было бы разумно, преодолевая разногласия и различные конъюнктурные мотивы акторов, сформировать «ответственный и беспристрастный совет мудрецов», способный выработать ясный план действий по преодолению рисков и угроз, сопряженных с цифровыми технологическими прорывами.

[3] Антропомерность как вызов и ответ современности: Коллективная монография/Отв. редактор В.Г.Буданов. Курск: Изд-во ЗАО «Университетская книга», 2022, - 309 с.
[4] Большая советская энциклопедия / гл. ред. Б. А. Введенский. 2-е изд. М., 1957.
[5] Е.Н. Князева, Когнитивная сложность. Исследование «Инновационная сложность: методологические, когнитивные и социальные аспекты». Философия науки. 2013. № 18. С. 81-94.

СПУТНИКИ КАК НОВЫЙ ФАКТОР МЕЖДУНАРОДНОГО ПОРЯДКА

Автор: **Хапов Алим**,
менеджер проектов Центра глобальной ИТ-кооперации;

Автор: **Черников Андрей**
студент 2-го курса магистратуры программы "Космос и мировая политика", факультет мировой политики, МГУ им. М.В. Ломоносова

Спутниками принято считать небесные объекты, обращающиеся по определённой траектории (орбите) вокруг другого объекта. В данной же статье речь пойдет об искусственных спутниках Земли, которыми считаются космические аппараты, выведенные на орбиту вокруг Земли и совершившие не менее одного оборота[6]. Запуск Советским Союзом первого в мире спутника в 1957 году ознаменовал начало космической эры человечества и совершенно изменил представление о космосе в умах обычных людей и политиков. Если на начальных этапах освоения космоса спутники являлись частью научно-технической гонки между Советским Союзом и Соединенными Штатами, то позднее стал очевиден потенциал применения этой технологии не только в гражданских целях, но и в вопросах обеспечения национальной безопасности. Уже в середине 1980-х годов Советский Союз начинает рассматривать целый ряд технологических достижений в качестве технологий двойного назначения, что подразумевает их потенциальное использование как в гражданских, так и военных целях[7]. Одновременно с появлением нового взгляда на ракетно-космические технологии наблюдается резкое увеличение количества космических аппаратов на околоземных орбитах. Со временем вопросы, связанные со спутниковыми группировками и развитием спутниковой связи, начинают рассматриваться на самом высоком уровне, приобретая всё более стратегический характер. Данная статья предлагает краткий обзор нынешнего положения спутников в системе международной безопасности и состояние российской космической группировки.

Важно начать с того, что космическая связь является хоть и не единственной, но одной из наиболее важных функций, которую сегодня выполняют спутники. Орбитальная инфраструктура, служащая ретрансляторами, действует совместно с наземными передатчиками и приёмниками, а главным преимуществом такой связи является её повсеместное проникновение. Другие же спутники позволяют не только передавать данные, но и собирать новые сведения, например, путем использования различных методов дистанционного зондирование земли (ДЗЗ) и сбора соответствующей информации.

На момент написания данной статьи безоговорочным гегемоном в отрасли космической связи является американская система «Starlink», разворачиваемая компанией Илона Маска «SpaceX». «Starlink» – это крупнейшая глобальная низкоорбитальная система спутниковой связи, обеспечивающая широкополосный доступ к Интернету в любой точке земного шара (где есть терминал для приёма сигнала). В ближайшие годы «Starlink» планирует пройти сертификацию во множестве государств, соседствующих с Россией: в 2024 система появится в Азербайджане, Казахстане, Монголии, Кыргызстане, Таджикистане, Туркменистане, а с 2025 в Узбекистане и Армении[8]. «Starlink» отличается простотой обслуживания и довольно быстрой скоростью загрузки. Главный конкурент «Starlink» на данный момент – это другая западная система, британская низкоорбитальная группировка «OneWeb». Стоит отметить, что некоторые крупные страны, включая Россию и Китай, запрещают

[6] Графодатский / Искусственный спутник земли // Большая российская энциклопедия [Электронный ресурс] https://old.bigenc.ru/technology_and_technique/text/2022575.
[7] С. Б. Иванов / Технологии двойного назначения // Военная энциклопедия / – Москва: Военное издательство, 2004. – Т. 8. – С. 73.
[8] В.А. Мосеев. Starlink нависает над Китаем и Россией. // [Электронный ресурс] https://ko.ru/articles/starlink-navisaet-nad-kitaem-i-rossiey/ https://ko.ru/contact/.

использование терминалов «Starlink» и «OneWeb» на своей территории по соображениям безопасности. Хотя формальным поводом для отсутствия компаний на российском рынке служит аргумент, что обе системы претендуют на уже занятые частоты[9].

Говоря о состоянии российской спутниковой группировки, стоит отметить, что существует очевидный диспаритет в области обеспечения широкополосного доступа в Интернет посредством спутниковой связи в сравнении с западными системами, который признается и Правительством России. В Стратегии развития отрасли связи Российской Федерации на период до 2035 года отмечается отсутствие полноценной технологической кооперации, которое не позволяет России сформировать современную конкурентоспособную национальную космическую группировку, и, как следствие, усложняет выход российских компаний – операторов спутниковой связи на иностранные рынки[10]. Более того, подчеркивается влияние западных санкций на поставки ключевого иностранного оборудования и комплектующих для создания космических аппаратов, которые ранее составляли в российских космических аппаратах связи более 80 процентов.

Тем не менее на российском рынке постоянно появляются новые игроки и проекты. Так, проект ГК Роскосмос «Сфера», анонсированный ещё в 2018 году, призван укрепить потенциал спутниковой группировки России. В рамках проекта планируется запустить на орбиту к 2025–2026 годам спутники связи «Скиф», которые увеличат охват российской спутниковой связи до 90% земной поверхности[11]. В свою очередь, компания «ИКС холдинг» также намерена обеспечить россиян и жителей 75 стран мира доступом в высокоскоростной интернет к 2035 г. Ожидается, что коммерческий сервис спутникового Интернета, разрабатываемый «Бюро 1440» (входит в «Икс холдинг») начнет функционировать уже в 2027 г. А к 2035 году будет сформирована полноценная группировка низкоорбитальных спутников связи численностью более 900 космических аппаратов[12]. Но, несмотря на амбициозность подобных отечественных проектов, по состоянию на сегодняшний день ни одна российская система не может сравниться со «Starlink» по количеству спутников на околоземной орбите и масштабности охвата[13].

Почему спутники, в общем, и спутники связи, в частности, так важны? Наличие независимой и конкурентоспособной спутниковой группировки не только имеет важность ввиду обеспечения стабильной и надежной связи “материковой” части России с такими труднодоступными территориями, как Арктическая зона РФ (АЗРФ), но и является критическим элементом архитектуры технологического суверенитета и национальной безопасности. Вполне очевидно, что функционал спутников позволяет пользоваться ими не только в гражданских целях. Яркой иллюстрацией двойного назначения подобных технологий является использование украинскими военными «Starlink» в ходе вооруженного конфликта на Украине[14]. А такие державы, как Соединенные Штаты и Китай в своих военных доктринах и вовсе отводят защите собственных спутников и уничтожению чужих отдельную роль[15]. В частности, спутники ДЗЗ и навигации являются ключевым компонентом сбора разведданных, а спутники связи и Интернета способствуют вертикальной и горизонтальной коммуникации между командованием и войсками. По сути, любой спутник поддержки изначально уже является военным объектом и может в любой момент реализовать свое “двойное назначение”. Сложно переоценить ту роль, которую в последнее десятилетие играют спутники как инструмент поддержки наземных операций в военных конфликтах. Можно ли в таком случае считать спутники новым фактором международного порядка и рассматривать их в качестве стратегического компонента международной безопасности?

[9] Разработчик «Гонца» объяснил, почему в России нет Starlink и OneWeb. // [Электронный ресурс] https://www.rbc.ru/rbcfreenews/639ab3439a794726e1cbbec4.
[10] Распоряжение Правительства Российский Федерации от 24 ноября 2023 г. № 3339-р
[11] Шесть спутников “Скиф” запустят на орбиту к середине 2026 года. // [Электронный ресурс] https://tass.ru/kosmos/16252523.
[12] Россия начала строить международного конкурента Starlink и OneWeb. Первые спутники уже запущены. // [Электронный ресурс] https://www.cnews.ru/news/top/2023-07-07_v_rossii_sozdaetsya_mezhdunarodnyj
[13] Starlink: как сверхскоростной интернет покоряет космос / РБК [Электронный ресурс] // https://trends.rbc.ru/trends/industry/5f72f4e39a7947caaf0f5bf1.
[14] Starlink and the Russia-Ukraine War: A Case of Commercial Technology and Public Purpose? // [Электронный ресурс] https://www.belfercenter.org/publication/starlink-and-russia-ukraine-war-case-commercial-technology-and-public-purpose.
[15] Военные доктрины США и КНР: геополитические аспекты. [Электронный ресурс] //https://nvo.ng.ru/concepts/2023-08-17/1_1249_aspect.html

Ответ не столь очевиден, так как использование подобных технологий двойного назначения практически не регулируется, ведь согласно Договору о космосе, подписанному в 1967 году, в космосе запрещено применять оружие массового поражения, а спутники таковым не являются. Стоит упомянуть, что многие попытки определить границы использования ракетно-космических технологий в военных целях не раз оборачивались провалом[16]. В условиях растущей зависимости от спутников защита своих спутников и противодействие чужим космическим аппаратам становится вопросом обеспечения национальной безопасности. Соответственно, защита подобной инфраструктуры является приоритетной задачей для любого государства. Таким образом, вновь по классической дилемме безопасности мир оказывается в состоянии гонки вооружений, но и эта гонка имеет новые черты. Среди угроз для спутников существуют не только угрозы физического (кинетического) воздействия, но и риски иного характера, такие как кибератаки, электронное воздействие, подавление, подмена сигналов и т.д. Этот вид угроз является относительно новым. Первый случай кибератаки на спутник датируется 1998 годом[17]. Если на начальных этапах основная угроза состояла в том, что хакеры взламывали наземные системы управления спутником, то со временем увеличивалась степень уязвимости и самих космических аппаратов. Как отмечают эксперты «Лаборатории Касперского», производители спутников зачастую пытаются использовать дешёвые и широкодоступные компоненты, особенно когда дело касается сборки и обслуживания больших спутниковых группировок. Это в свою очередь создает риски уязвимости в самих спутниках через наличие недоброкачественных элементов в составе аппаратов[18]. Разумеется, в области обеспечения безопасности спутников уже проведена большая работа – защищённые частоты передачи данных, инновационные способы шифрования, новые программы подготовки специалистов по информационной безопасности и т.д. Эксперты также отмечают, что искусственный интеллект способен помочь в создании динамической системы защиты, которая будет подстраиваться под конкретную атаку[19]. Зависимость от космических технологий растет, так что необходимо продолжать заниматься всеми аспектами безопасности как физической, так и информационной, а также диверсифицировать используемые опорные системы.

С ускорением технологического развития возрастает зависимость человечества от услуг и функций, предоставляемых спутниками, которые теперь приобретают характер критической инфраструктуры, наряду с нефте- и газопроводами, электростанциями, а также подводными кабелями связи. Всё более очевидным становится двойное назначение спутников как элемента гражданской инфраструктуры и как технологии, обеспечивающей безопасность. Как видно из выше представленного материала, многие игроки уже осознали новую роль, отведенную спутниковой инфраструктуре в системе безопасности. Российские власти, не являясь исключением, делают ставку на развитие собственной национальной космической группировки спутников, что отражает стремление России к самодостаточности в вопросах технологического суверенитета и национальной безопасности. А защита спутников становится ключевой для их успешного и эффективного функционирования.

[16] Договор о предотвращении размещения оружия в космическом пространстве, применения силы или угрозы силой в отношении космических объектов. // [Электронный ресурс] https://www.mid.ru/ru/foreign_policy/international_safety/1686193/.
[17] Космические кибератаки: кто и зачем ворует данные со спутников. // РБК [Электронный ресурс] // https://trends.rbc.ru/trends/industry/614da42d9a7947b3101372b3.
[18] Космические хакеры: мифы и реальность. / Лаборатория Касперского [Электронный ресурс] //https://www.kaspersky.ru/blog/cybersecurity-in-outer-space/32303/.
[19] В условиях космической гонки кибербезопасность по-прежнему вызывает беспокойство. // SecurityLab.ru [Электронный ресурс] // https://www.securitylab.ru/news/523447.php

Библиографический список:

1. О.С. Графодатский / Искусственный спутник земли // Большая российская энциклопедия [Электронный ресурс] https://old.bigenc.ru/technology_and_technique/text/2022575 (дата обращения: 17.03.2024).
2. С. Б. Иванов / Технологии двойного назначения // Военная энциклопедия / – Москва: Военное издательство, 2004. – Т. 8. – С. 73.
3. В.А. Мосеев. / Starlink нависает над Китаем и Россией. // [Электронный ресурс] https://ko.ru/articles/starlink-navisaet-nad-kitaem-i-rossiey/ https://ko.ru/contact/ (дата обращения: 17.03.2024).
4. Разработчик «Гонца» объяснил, почему в России нет Starlink и OneWeb. // [Электронный ресурс] https://www.rbc.ru/rbcfreenews/639ab3439a794726e1cbbec4 (дата обращения: 17.03.2024).
5. Распоряжение Правительства Российский Федерации от 24 ноября 2023 г. № 3339-р
6. Шесть спутников «Скиф» запустят на орбиту к середине 2026 года. // [Электронный ресурс] https://tass.ru/kosmos/16252523 (дата обращения: 17.03.2024).
7. Россия начала строить международного конкурента Starlink и OneWeb. Первые спутники уже запущены. // [Электронный ресурс] https://www.cnews.ru/news/top/2023-07-07_v_rossii_sozdaetsya_mezhdunarodnyj (дата обращения: 17.03.2024).
8. Starlink: как сверхскоростной интернет покоряет космос / РБК [Электронный ресурс] // https://trends.rbc.ru/trends/industry/5f72f4e39a7947caaf0f5bf1 (дата обращения: 17.03.2024).
9. Starlink and the Russia-Ukraine War: A Case of Commercial Technology and Public Purpose? // [Электронный ресурс] https://www.belfercenter.org/publication/starlink-and-russia-ukraine-war-case-commercial-technology-and-public-purpose (дата обращения: 17.03.2024).
10. Военные доктрины США и КНР: геополитические аспекты. [Электронный ресурс] // https://nvo.ng.ru/concepts/2023-08-17/1_1249_aspect.html. (дата обращения: 17.03.2024).
11. Договор о предотвращении размещения оружия в космическом пространстве, применения силы или угрозы силой в отношении космических объектов. // [Электронный ресурс] https://www.mid.ru/ru/foreign_policy/international_safety/1686193/ (дата обращения: 17.03.2024).
12. Космические кибератаки: кто и зачем ворует данные со спутников. // РБК [Электронный ресурс] // https://trends.rbc.ru/trends/industry/614da42d9a7947b3101372b3 (дата обращения: 17.03.2024).
13. Космические хакеры: мифы и реальность. / Лаборатория Касперского [Электронный ресурс] // https://www.kaspersky.ru/blog/cybersecurity-in-outer-space/32303/ (дата обращения: 17.03.2024).
14. В условиях космической гонки кибербезопасность по-прежнему вызывает беспокойство. // SecurityLab.ru [Электронный ресурс] // https://www.securitylab.ru/news/523447.php (дата обращения: 17.03.2024).

АЛЬТЕРНАТИВНЫЕ ВЗГЛЯДЫ НА ПРОБЛЕМУ СЕТЕВОЙ СЕГМЕНТАЦИИ В ПОЛЬЗОВАТЕЛЬСКИХ СООБЩЕСТВАХ: ВОПРОСЫ ПУЗЫРЕЙ ФИЛЬТРОВ И ЭХО-КАМЕР

Автор: **Колотаев Юрий Юрьевич**,
ассистент кафедры европейских исследований, факультет международных отношений,
Санкт-Петербургский государственный университет

Развитие цифровой среды, происходящее на сегодняшний день в условиях активной конфронтации различных социально-политических единиц на множественных уровнях международной системы, констатирует тенденцию к появлению разделительных линий, проходящих насквозь через сетевое пространство. Последнее десятилетие учеными и аналитиками активно продвигается мысль о сосуществовании процесса глобального распространения сетевых технологий и платформ с повсеместным образованием национальных и локальных сообществ, разделяющих информационную среду[20]. Степень разделения, при этом, зависит от типа этих сообществ, ведь к ним можно отнести как малочисленные группы со схожими интересами и позициями, так и более крупные скопления институтов и групп людей[21], формирующих целые государства.

Последние, в меру дивергенции политических позиций и экономических интересов, используют разделение сетевого пространства как способ защиты того сетевого сегмента, который ассоциирован с национальным пространством или его гражданами[22]. Такого рода разделение формирует предпосылки для формирования реальных или вербальных границ, или, скорее, барьеров в интернете.

Вместе с тем не менее важными барьерами, разбивающими сеть на сегменты, являются не национальные политические инициативы, а пользовательские сообщества. Они также проводят границы внутри сети, сопряженные с границами их информационного поля и получаемого контента. В начале 2010-х гг. это явление получило множественные облачения научного и аналитического характера, будучи выраженными в категориях сетевых «эхо-камер»[23] и поддерживающих их «пузырей-фильтров»[24]. Оба термина используются для описания ситуации, когда пользователь получает информацию только от источников, которые подтверждают его собственные убеждения и мнения. В частности, эффект эхо-камеры возникает на социальных сетях, новостных сайтах и других онлайн-платформах. В классическом представлении в эхо-камере пользователи становятся все более изолированными от других точек зрения и теряют способность критически оценивать информацию.

Инструментальным воплощением создаваемых эхо-камерой границ становятся пузыри фильтров, отражающие ситуации, когда алгоритмы поиска и рекомендации в интернете формируют индивидуальный пользовательский «пузырь», в котором информация соответствует интересам и предпочтениям человека. В результате это потенциально может привести к тому, что пользователь становится изолирован от альтернативных точек зрения, закрепляя собственную эхо-камеру. Подобные явления иллюстрируют, что сетевое дробление способно формироваться не только намеренным вмешательством классических политических акторов и социальных институтов, но и культивироваться изнутри сообщества.

[20] Drake W. J., Vinton C. G., Kleinwachter W. Internet fragmentation: An overview. – World Economic Forum, 2016.
[21] Кириллина Н. В. О роли пользователя и фрагментации сети //Коммуникология. – 2021. – Т. 9. – №. 2. – С. 41-49.
[22] Зиновьева Е. С. Кибер-дипломатия в условиях обострения конкуренции между великими державами //Вестник МГИМО-Университета. – 2022. – С. 1-21.
[23] Sunstein C. R. Echo chambers: Bush v. Gore, impeachment, and beyond. – Princeton, NJ: Princeton University Press, 2001; Sunstein C. R. Republic. com. – Princeton, NJ: Princeton university press, 2001.
[24] Pariser E. The filter bubble: How the new personalized web is changing what we read and how we think. – Penguin, 2011; Pariser E. The filter bubble: What the Internet is hiding from you. – Penguin, 2011.

В совокупности, разделение сообществ по собственным информационным средам может происходить на различных уровнях среды, будь то поляризация внутри национального государства, либо фрагментация по неполитическим интересам в трансграничном формате[25]. Эффект эхо-камеры при этом принято на сегодняшний день считать для цифровой среды опасным, т.к. он способствует распространению ложной информации или приводит к замкнутости процесса выработки мировоззрения[26], что в свою очередь формирует предпосылки для принятия неправильных решений или даже к опасным действиям. Немалая доля в этой проблеме отводится именно алгоритмам, ведь они формируют информационное поле, ограничивающее поступающие сведения[27]. На основе этого в последние годы цифровые платформы становятся предметом активных общественных и политических инициатив по сдерживанию их влияния и повышению подотчетности.

Однако вышеуказанная конвенциональная позиция имеет ряд недостатков. Наиболее существенные из них отражены в ряде работ, подвергающих сомнению масштаб проблемы, стоящей за эхо-камерами и пузырями фильтров в сети[28]. В частности, А. Брунс отмечает, что помимо терминологической неопределенности у данных явлений имеется явный техноцентризм при установлении проблемного поля[29]. Иначе говоря, когда речь идёт о формировании обособленных информационных пространств в сети, главенствующая роль в этом вопросе отводится цифровым платформам, т.к. их статус посредника обеспечивает исключительную позицию при ретрансляции информации.

Вместе с тем дивергенция позиций и информационных потоков не может быть обеспечена на наивысшем уровне только через сами платформы. Человеческое информационное потребление не находится в исключительной зависимости от онлайн-медиа[30], которые формируют лишь фрагмент общего потребления информации. Превозношение же эхо-камер и пузырей фильтров в исключительное положение центральной угрозы сетевого пространства является редукционистским. В частности, оно толкает к моральной панике техноскептиков[31] или к техносолюционизму[32] сторонников цифровой трансформации.

Однако проблемным явлением в этой связи является не сам факт наличия или отсутствия эхо-камер и методов их усиления, сколько социальных предпосылок, формирующих условия для эксплуатации изъянов цифровой среды. Формирование границ и барьеров в распределении информации в обществе складывается не из-за самой технической возможности, а из-за социального спроса, на подтверждение собственной позиции и обособления от враждебных точек зрения. Опора на техноцентричную перспективу исходит из того, что наличие непримиримых позиций, нуждающихся в обособлении – это естественное состояние сообществ. Вместе с тем этот аспект требует более критического рассмотрения.

Степень разобщенности общества имеет градацию, которая может упускаться при изучении пользовательских пространств. В частности, существует три взаимопересекающихся категории: сегментация, фрагментация и поляризация. Последующий переход от одной стадии к другой характеризуется сокращением интенсивности связей между сообществами и даже их отношением друг к другу[33]. Если сегментация подразумевает распад сообщества на обособленные части при сохранении взаимных контактов, то фрагментация отражает процесс сокращения или даже исчезновения подобных связей. Поляризация закрепляет распад и ведёт к формированию непересекающихся или даже конфликтных позиций по какому-либо вопросу[34]. Важно отметить, что все три стадии в рамках групповой динамики возможны лишь при наличии общего явления, от которого эти процессы отталкиваются. Отсутствие общего проблемного поля не создает никаких связей, ни положительных, ни негативных.

[25] Malcomson S. Splinternet: How geopolitics and commerce are fragmenting the World Wide Web. – OR books, 2016.
[26] Krafft P. M., Donovan J. Disinformation by design: The use of evidence collages and platform filtering in a media manipulation campaign //Political Communication. – 2020. – Vol. 37. – №. 2. – P. 194-214.
[27] Cohen J. N. Exploring echo-systems: how algorithms shape immersive media environments //Journal of Media Literacy Education. – 2018. – Vol. 10. – №. 2. – P. 139-151.
[28] Garrett R. K. The "echo chamber" distraction: Disinformation campaigns are the problem, not audience fragmentation // Journal of Applied Research in Memory and Cognition. - 2017. - Vol. 6(4), P. 370–376; Bruns A. It's not the technology, stupid: How the 'Echo Chamber' and 'Filter Bubble' metaphors have failed us //International Association for Media and Communication Research. – 2019.
[29] Bruns A. Are filter bubbles real? – John Wiley & Sons, 2019
[30] Bruns A. Are filter bubbles real? – John Wiley & Sons, 2019
[31] Walsh J. P. Social media and moral panics: Assessing the effects of technological change on societal reaction //International Journal of Cultural Studies. – 2020. – Vol. 23. – №. 6. – P. 840-859.
[32] Kalpokas I., Salaseviciute V., Lipske M. Technology as a Threat or a Solution? The Challenges of Responding to Synthetic Media //Baltic Journal of Law & Politics. – 2023. – Vol. 16. – №. 2. – P. 1-22.
[33] Белоброва О. Д. Социальная фрагментация как сущностный феномен дифференциации //PolitBook. – 2016. – №. 4. – С. 56-64.
[34] Spohr D. Fake news and ideological polarization: Filter bubbles and selective exposure on social media //Business information review. – 2017. – Vol. 34. – №. 3. – P. 150-160.

Альтернативная репрезентация проблемы указывает на то, что сегментация – обобщающее явление, которое может проходить по двум направлениям: фрагментации и поляризации. Однако вне зависимости от этого сегментация означает разделение пользователей на группы по определенным характеристикам, что является предпосылкой, но необязательно неотъемлемым поводом для создания информационных пузырей.

Фрагментация проявляется в изменении приверженности диалогу в пользу обособлению, аналогично процессу отхода от многостороннего управления техническим уровнем Интернета в пользу закрепления национальных стандартов[35]. Акцент на локальном опыте в пользовательском сообществе может привести к фрагментации с обрывом взаимных связей между фрагментированными частями информационного пространства. При этом на саму фрагментацию технические инструменты, провоцирующие пузыри фильтров, оказывают опосредованное воздействие, т.к. они не способны стать триггером для социальной или пользовательской фрагментации с идейно-тематической точки зрения.

Итоговая же фаза деградации связей пользовательских сообществ – поляризация – связана не просто с разделением на группы с разными взглядами, убеждениями и интересами, а с последующей фиксацией различий в конфликтующих нарративах[36]. Этот этап в наибольшей степени и ассоциируется с эхо-камерами или пузырями фильтров, т.к. эксплуатация различий становится более функциональной и облегчённой в силу кристаллизации границ. Социальные сети и алгоритмы рекомендаций могут усиливать поляризацию, показывая пользователям контент, который соответствует их предпочтениям, что дополнительно может привести к усилению конфликтов и недопонимания между разными группами.

Проведя указанную градацию важно подчеркнуть, что она не отрицает угрозу, исходящую от эффектов информационных пузырей. Альтернативная позиция, озвученная выше, лишь акцентирует внимание на том, что рассматриваемые феномены установления социальных границ и их трансформация в реальную опасность для сообщества непропорционально распределены между уровнями дивергенции сообществ. Не всякое установление базовых границ культивирует самостоятельные эхо-камеры в сети, ровно, как и не всякое погружение в близкий пользователю информационный поток культивирует пузыри фильтров. В отдельных случаях генерация собственного «фильтра» оказывает скорее обратный эффект противодействия информационным пузырям, если он соответствует принципам цифровой и информационной гигиены.

Таким образом, сегментация, фрагментация и поляризация пользователей в сети Интернет – это важные явления, которые оказывают влияние на структуру и функционирование пользовательских сообществ. Они формируют границы между пользователями, но, вместе с тем, подобные границы имеют разную степень проницаемости, что указывает на важность теоретической и фактической дифференциации не только уровней системы информационных и социальных интеракций, но и степени интенсивности обмена информации между сообществами.

Важно осознавать эти явления и искать способы балансировать между локальными потребностями и общими интересами, чтобы обеспечить устойчивое и разнообразное функционирование Интернета. Сами же эхо-камеры и пузыри фильтров являются проблемами, которые необходимо рассматривать на дифференцированной основе, чтобы обеспечить более объективное и сбалансированное представление информации в интернете. Но для этого требуется более сбалансированный подход, избегающий полярных опасностей техносолюционизма и моральной паники от новых технологий.

[35] Гленн Д. Фрагментация и национализация //Россия в глобальной политике. – 2022. – Т. 20. – №. 2 (114). – С. 224-229.
[36] Bliuc A. M., Bouguettaya A., Felise K. D. Online intergroup polarization across political fault lines: An integrative review //Frontiers in Psychology. – 2021. – Vol. 12. – P. 641215.

Библиографический список:

1. Белоброва О. Д. Социальная фрагментация как сущностный феномен дифференциации //PolitBook. – 2016. – №. 4. – С. 56-64.
2. Гленн Д. Фрагментация и национализация //Россия в глобальной политике. – 2022. – Т. 20. – №. 2 (114). – С. 224-229.
3. Зиновьева Е. С. Кибер-дипломатия в условиях обострения конкуренции между великими державами //Вестник МГИМО-Университета. – 2022. – С. 1-21.
4. Кириллина Н. В. О роли пользователя и фрагментации сети //Коммуникология. – 2021. – Т. 9. – №. 2. – С. 41-49.
5. Bliuc A. M., Bouguettaya A., Felise K. D. Online intergroup polarization across political fault lines: An integrative review //Frontiers in Psychology. – 2021. – Vol. 12. – P. 641215.
6. Bruns A. Are filter bubbles real? – John Wiley & Sons, 2019
7. Bruns A. It's not the technology, stupid: How the 'Echo Chamber' and 'Filter Bubble' metaphors have failed us // International Association for Media and Communication Research. – 2019.
8. Cohen J. N. Exploring echo-systems: how algorithms shape immersive media environments //Journal of Media Literacy Education. – 2018. – Vol. 10. – №. 2. – P. 139-151.
9. Drake W. J., Vinton C. G., Kleinwächter W. Internet fragmentation: An overview. – World Economic Forum, 2016.
10. Garrett R. K. The "echo chamber" distraction: Disinformation campaigns are the problem, not audience fragmentation // Journal of Applied Research in Memory and Cognition. - 2017. - Vol. 6(4), P. 370–376
11. Kalpokas I., Šalaševičiūtė V., Lipskė M. Technology as a Threat or a Solution? The Challenges of Responding to Synthetic Media //Baltic Journal of Law & Politics. – 2023. – Vol. 16. – №. 2. – P. 1-22.
12. Krafft P. M., Donovan J. Disinformation by design: The use of evidence collages and platform filtering in a media manipulation campaign //Political Communication. – 2020. – Vol. 37. – №. 2. – P. 194-214.
13. Malcomson S. Splinternet: How geopolitics and commerce are fragmenting the World Wide Web. – OR books, 2016.
14. Pariser E. The filter bubble: How the new personalized web is changing what we read and how we think. – Penguin, 2011
15. Pariser E. The filter bubble: What the Internet is hiding from you. – Penguin, 2011.
16. Spohr D. Fake news and ideological polarization: Filter bubbles and selective exposure on social media //Business information review. – 2017. – Vol. 34. – №. 3. – P. 150-160.
17. Sunstein C. R. Echo chambers: Bush v. Gore, impeachment, and beyond. – Princeton, NJ: Princeton University Press, 2001
18. Sunstein C. R. Republic. com. – Princeton, NJ: Princeton university press, 2001.
19. Walsh J. P. Social media and moral panics: Assessing the effects of technological change on societal reaction // International Journal of Cultural Studies. – 2020. – Vol. 23. – №. 6. – P. 840-859.

ПРОБЛЕМЫ ПРАВОВОЙ ОХРАНЫ РЕЗУЛЬТАТОВ ИНТЕЛЛЕКТУАЛЬНОЙ ДЕЯТЕЛЬНОСТИ, СОЗДАННЫХ ПРИ ПОМОЩИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Автор: **Нигмазятова Дана**
студентка 1-го курса магистратуры, юридический факультет, МГУ им. М.В. Ломоносова;
юрист, ООО «Саграда Лигал»

Современные технологии подвержены экспоненциальному росту: с каждым днем развитие ускоряется и прогресс предлагает человечеству новые решения. Но у данного развития есть обратная сторона – появление новых технологий приводит к возникновению новых, ранее не существовавших отношений. Урегулирование последних является важной задачей законодателей.

Так, актуальным предстает вопрос искусственного интеллекта (далее – «ИИ»). Само понятие появилось относительно давно: 1956 году группа молодых ученых, математиков и теоретиков предложили программу, которая способна имитировать человека в области решения проблем и задач[37]. С этого момента началось осмысление феномена ИИ, в результате чего было сформулированы две основные концепции – «сильного ИИ» и «слабого ИИ».

В рамках настоящей работы сконцентрируемся на системе слабого ИИ как уже существующей и применяемой технологии. Это программа, построенная на нейросетях, позволяющая систематизировать, анализировать, синтезировать информацию, выделять наиболее важные аспекты, делать выводы. Но ключевая особенность этой технологии – способность к самообучению без вмешательства человека. Основываясь на заранее загруженном объеме данных, ИИ воссоздает новые варианты решений, которые не входят в изначальный алгоритм[38].

Поэтому ИИ применяется во многих сферах, начиная с промышленности и науки, заканчивая сферой развлечений и оказания услуг. Вполне обоснованно возникает вопрос, как же регулировать все те результаты, которые создаются автоматизированной самообучающейся программой, ввиду отсутствия участия человека в их создании. Данная проблема содержит в себе массу правовых, этических, философских аспектов, в работе будут рассмотренные лишь некоторые, самые важные.

Проблема ответственности является центральной для раскрытия предложенной темы. На данный момент ведутся активные дискуссии по поводу признания или отказа в признании правоспособности, дееспособности и деликтоспособности ИИ. Известным прецедентом признания правосубъектности ИИ стало приобретения

[37] Бегишев И.Р., Хисамова З.И. Криминологические риски применения искусственного интеллекта // Всероссийский криминологический журнал. 2018. №6. URL: https://cyberleninka.ru/article/n/kriminologicheskie-riski-primeneniya-iskusstvennogo-intellekta (дата обращения: 03.03.2024).
[38] Ролинсон П., Ариевич Е.А., Ермолина Д.Е. Объекты интеллектуальной собственности, создаваемые с помощью искусственного интеллекта: особенности правового режима в России и за рубежом. Закон. 2018. N 5. С. 63 – 71 (дата обращения: 19.02.2024).

гражданства роботом София в Саудовской Аравии. Однако широко распространения данная практика не получила. Тем не менее, правовой статус ИИ является камнем преткновения для многих правопорядков, в том числе, и для России. Так, современная научная доктрина предлагает следующие возможные варианты: создание особого правового статуса, основанного на теории фикции – «электронного лица» или «технического лица»[39]; придание режима объекта гражданских прав, представление в качестве источника повышенной опасности; предлагается также инструментальный подход, то есть восприятие ИИ как средство решения определенных задач.

Основываясь на действующем российском законодательстве, корректнее воспринимать ИИ как объект гражданских прав, источник повышенной опасности, не обладающий правосубъектностью, ответственность за которого несет его владелец[40]. Можно допустить аналогию с правовым статусом раба в римском праве, результаты деятельности которого переходили к его владельцу. Однако этот подход вызывает ряд вопросов. В первую очередь, не всегда есть возможность контролировать деятельность системы ИИ ввиду скорости операций и способности к самообучению[41]. Также остается открытым вопрос, когда рассматриваемому объекту можно придать статус ИИ. В процессе создания и функционирования системы участвуют и разработчик самой программы, и обучающее лицо, и непосредственный владелец девайса, куда ИИ помещается. Все три представленные функции нередко исполняют несколько субъектов. Так, если обучающее лицо включило в базу данных объекты, охраняемые авторским правом, можно ли признать охраноспособность полученного результата? В то же время, кто будет нести ответственность за полученный продукт – носитель девайса или обучающее лицо? Вопросы остаются открытыми, но данное суждение может привести к выводу, что подобные результаты охране подлежать не должны.

С другой стороны, не всегда возможно установить, какие данные закладываются в программу. Проблема публичности алгоритмов также нашла свое отражение в представленной дискуссии. Во Франции Комиссия по информатике и гражданским свободам представила доклад по «Этическим аспектам машинных алгоритмов и искусственного интеллекта», согласно которому провозглашается политика противодействия эффекту «черного ящика» и нарушениям прав и интересов граждан и общества[42]. Прозрачность деятельности ИИ позитивно для всеобщего развития, так как существующие результаты могут стать «фундаментом», на котором могут основываться дальнейшие технологические открытия. Однако эта политика не так однозначна. Существует несколько соображений в пользу отказа в раскрытии алгоритмов ИИ. Во-первых, программа использует иной язык, не понятный непосвященному человеку, что вызывает потребность в постоянной интерпретации операций системы. Более того, алгоритмы не всегда прозрачны даже для создателей[43]. Во-вторых, необходимо понимать, что цели создания определенных продуктов неодинаковы, так как программа может использоваться в совершенно разных сферах деятельности человека.

В промышленности использование ИИ порой просто необходимо для ускорения и оптимизации процессов, чтобы получить конкурентное преимущество. Для бизнеса результаты деятельности ИИ – коммерческий продукт, поэтому инвесторы и предприниматели заинтересованы не только в конфиденциальности своих технологий,

[39] Морхат П. М. Правосубъектность юнитов искусственного интеллекта и ответственность за их действия //Право и государство: теория и практика. – 2017. – №. 11. – С. 30-36. (дата обращения: 10.02.2024).
[40] Антонов А.А. Искусственный интеллект как источник повышенной опасности // Юрист. 2020. N 7. С. 69 - 74. (дата обращения: 30.01.2024).
[41] Хисамова З.И., Бегишев И.Р. Сущность искусственного интеллекта и проблема определения правосубъектности // Вестник МГОУ. Серия: Юриспруденция. 2020. №2. (дата обращения: 09.02.2024).
[42] Дюфло А. Искусственный интеллект во французском праве // Вестник Университета имени О. Е. Кутафина. 2021. №1 (77). URL: https://cyberleninka.ru/article/n/iskusstvennyy-intellekt-vo-frantsuzskom-prave (дата обращения: 19.02.2024).
[43] Кузнецов А.Г. Туманности нейросетей: «Черные ящики» технологий и наглядные уроки непрозрачности алгоритмов // Социология власти. 2020. №2. (дата обращения: 09.02.2024).

но и в охране полученных результатов. Хорошим примером может послужить прецедент в Китае, где была предоставлена охрана продукции, созданной ИИ. Спор о плагиате текста, созданного ИИ, между компаниями Shanghai Yingxun Technology Company и Tencent был разрешен в пользу последнего. Китайский суд пришел к выводу, что текст должен охраняться авторским правом и что ИИ – «электронное лицо»[44].

В Российской Федерации правовой режим охраны объектов, полученных в результате деятельности ИИ, законодательно не установлен. Возможно, это вызвано тем, что вопрос еще не был актуализирован судебной практикой. Несмотря на существующую законодательную неопределенность, в доктрине представлено несколько подходов к правовой охране рассматриваемых результатов: в качестве объектов, охраняемые авторским правом; объектов смежного права; объектов патентного права; как часть базы данных и т.п. Все рассматриваемые режимы относятся к праву интеллектуальной собственности, которое регулирует вопросы, касающиеся художественно-символичных образов, научных новшеств, технических идей и открытий и других нематериальных объектов[45].

Самым обсуждаемым и критикуемым из возможных режимов является охрана авторским правом. Рассмотрим практику других стран. В международном праве, согласно Бернской конвенции об охране литературных и художественных произведений, определяющими категориями являются гражданство и место жительства, чего ИИ, по общему правилу, иметь не может. В Великобритании данный вопрос регулируется Законом «Об авторском праве, промышленных образцах и патентах». Согласно ст. 9 Закона автором произведений, созданных с помощью ИИ (так называемые «computer-generated works») признается физическое лицо, контролирующее программу[46]. Также имеется практика защиты результатов деятельности ИИ на подобии охраны части инвестиционных баз данных. В США в соответствии с позицией Бюро авторского права и Патентным кодексом, автором произведения или изобретения может быть только человек. В Германии создание произведения возможно только в результате созидательной деятельности человека, что ведет к отрицанию охраны всех объектов, созданных без участия человека[47].

Данный подход объясняется тем, что сущность авторского права основана на творческой составляющей человека. При использовании ИИ в создании объекта авторского права вклад человека очень сомнителен, так как выбор, на котором базируется процесс создания нового, делается программой[48]. Также стоит сказать о рисках, но уже не правового, а морально-этического толка. В существующем мире многообразия очень трудно найти по-настоящему новую, оригинальную идею. Человек с каждым годом становится все ближе к исчерпанию идей и своего творческого потенциала. Е.Г. Авакян приводит очень хорошую аналогию: один человек,

[44] Гомзякова Е. М. Искусственный интеллект: инструмент или автор? //Научное обозрение. – 2021. – С. 183-186. (дата обращения: 02.03.2024).
[45] Суханов Е. А. Гражданское право. В 4 томах. Том 2. Вещное право. Наследственное право. Интеллектуальные права. Личные неимущественные права //М.: Статут. – 2019. С. 239-241. (дата обращения: 19.02.2024).
[46] Ролинсон П., Ариевич Е.А., Ермолина Д.Е. Указ. Соч.
[47] Харитонова Ю. С. Правовой режим результатов деятельности искусственного интеллекта //Современные информационные технологии и право: монография/МГУ им. МВ Ломоносова. Юридический факультет. – 2019. – С. 68-83. (дата обращения: 17.02.2024).
[48] Харитонова Ю. С. Правовой режим результатов деятельности искусственного интеллекта //Современные информационные технологии и право: монография/МГУ им. МВ Ломоносова. Юридический факультет. – 2019. – С. 68-83. (дата обращения: 17.02.2024).

прочитавший около 50 любовных романов, со временем начнет не только прогнозировать сюжетные повороты, но и понимать, когда идеи были заимствованы у других писателей[49]. Готово ли человечество создать себе реального конкурента в сфере, которая, возможно, со временем станет единственным прибежищем разума в мире превосходства машин?

Другой важный этический и правовой вопрос, который был частично затронут ранее, это возможность наложение запрета на обучение на примере своих работ. Любой автор, будь то художник или инженер, заинтересован в своем детище, в признании его личного авторства в создании. ИИ же безразличен к этим категориям, программа использует все данные, которым она обучилась. На данный момент существует нейросеть, обученная на картинах Рембрандта, которая восстановила некогда обрезанную картину «Ночной дозор»[50]. Соответственно, она способна скомпилировать и новую картину, используя авторский стиль и техники великого художника. Но можно ли обучить ИИ не так линейно, то есть включить в базу данных картины не только одного художника? Технологии на данный момент достигли уровня, дающего эту возможность. Выборочность в избрании объектов для дальнейшей компиляции – задача для ИИ трудновыполнимая ввиду возможности отсутствия охранных маркировок, использования ранее скопированной работы без обозначения первоначального автора, а также вопроса добросовестности обучающего лица. Рассмотренный аспект подкрепляет позицию прозрачности и открытости алгоритмов ИИ.

Законодательным препятствием такого режима в российском праве является п. 1 ст. 1228 ГК РФ[51], в соответствии с которым «не признаются авторами результата интеллектуальной деятельности граждане, не внесшие личного творческого вклада в создание такого результата, в том числе оказавшие его автору только техническое, консультационное, организационное или материальное содействие или помощь либо только способствовавшие оформлению прав на такой результат или его использованию, а также граждане, осуществлявшие контроль за выполнением соответствующих работ».

Несмотря на это, ряд ученых продолжают поддерживать внедрение правового режима охраны авторским правом результатов, созданных ИИ. Одним из аргументов предстает тенденция создания многих объектов авторского права группой физических лиц, каждое из которых внесло свой вклад в создание. Определение наличия творческой составляющих каждого участника вызывает проблему[52]. Именно поэтому предлагается расширение или изменение категории авторских прав, которая бы позволяла регулировать новые формы творческой деятельности, в число которых, со временем, добавится и деятельность ИИ.

[49] О ПЕРСПЕКТИВАХ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА И О НОВАЦИЯХ В ОБЛАСТИ ЦИФРОВОГО ПРАВА. ИНТЕРВЬЮ ЕЛЕНЫ АВАКЯН ДЛЯ РАСПИ. URL: https://epam.ru/ru/media/view/o-perspektivah-elektronnogo-dokumentooborota-i-o-novaciyah-v-oblasti-cifrovogo-prava-or-lessemgreater-intervyu-eleny-avakyan-dlya-rapsi-lessemgreater (дата обращения: 17.02.2024).
[50] Нейросеть смогла дорисовать картину Рембрандта “Ночной дозор” URL: https://www.m24.ru/news/tehnologii/25062021/171113 (дата обращения: 19.02.2024).
[51] «Гражданский кодекс Российской Федерации (часть первая)» от 30.11.1994 N 51-ФЗ (ред. от 25.02.2022). [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_5142.(дата обращения: 19.02.2024).
[52] Синельникова В.Н. Правовой Режим результатов интеллектуальной деятельности, созданных саморазвивающимися программами // Пермский юридический альманах. 2019. №2. (дата обращения: 19.02.2024).

Другим распространенным подходом является придание результатам статуса объекта смежных прав. Можно, пожалуй, провести аналогию с охраной фонограмм, так как это техническая фиксация звуков, творческая деятельность человека в данном процессе не требуется. Защита направлена не на конечный, а условный промежуточный результат. Соответственно, можно защитить созданную ИИ картину, однако не запрещается использовать полученный результат, например, для обучения другими программами или для переработки иными субъектами права.

Существуют и другие концепции. В частности, Е.Г.Авакян предположила появление новых режимов охраны, таких, как долевое исключительное право для ключевых участников процесса создания продукта (разработчик, обучающее лицо и владелец носителя)[53].

Таким образом, законодательное регулирование вопроса режима правовой охраны результатов деятельности, созданных при помощи ИИ, является важнейшей задачей, которая необходима для создания благоприятных условий для дальнейшего экономического и технологического развития сферы IT и науки, и защиты прав и интересов граждан и всего общества в целом. На данный момент Российская Федерация не отразила критерии и принципы регулирования ИИ в своем законодательстве, однако политический курс направлен на достижение лидерства в сфере развития и использования технологий ИИ и разрешение ряда сложных этических и правовых вопросов, в том числе, и определение режима правовой охраны.

[52] Гомзякова Е. М. Указ. Соч.

Библиографический список:

1. Антонов А.А. Искусственный интеллект как источник повышенной опасности // Юрист. 2020. N 7. С. 69 - 74.
2. Бегишев И.Р., Хисамова З.И. Криминологические риски применения искусственного интеллекта // Всероссийский криминологический журнал. 2018. №6. URL: https://cyberleninka.ru/article/n/kriminologicheskie-riski-primeneniya-iskusstvennogo-intellekta
3. Гомзякова Е. М. Искусственный интеллект: инструмент или автор? //Научное обозрение. – 2021. – С. 183-186.
4. Дюфло А. Искусственный интеллект во французском праве // Вестник Университета имени О. Е. Кутафина. 2021. №1 (77). URL: https://cyberleninka.ru/article/n/iskusstvennyy-intellekt-vo-frantsuzskom-prave
5. Кузнецов А.Г. Туманности нейросетей: «Черные ящики» технологий и наглядные уроки непрозрачности алгоритмов // Социология власти. 2020. №2. URL: https://cyberleninka.ru/article/n/tumannosti-neyrosetey-chernye-yaschiki-tehnologiy-i-naglyadnye-uroki-neprozrachnosti-algoritmov
6. Мохат П. М. Правосубъектность юнитов искусственного интеллекта и ответственность за их действия // Право и государство: теория и практика. – 2017. – №. 11. – С. 30-36.
7. Ролинсон П., Ариевич Е.А., Ермолина Д.Е. Объекты интеллектуальной собственности, создаваемые с помощью искусственного интеллекта: особенности правового режима в России и за рубежом // Закон. 2018. N 5. С. 63 - 71.
8. Синельникова В.Н. Правовой Режим результатов интеллектуальной деятельности, созданных саморазвивающимися программами // Пермский юридический альманах. 2019. №2. URL: https://cyberleninka.ru/article/n/pravovoy-rezhim-rezultatov-intellektualnoy-deyatelnosti-sozdannyh-samorazvivayuschimisya-programmami
9. Суханов Е. А. Гражданское право. В 4 томах. Том 2. Вещное право. Наследственное право. Интеллектуальные права. Личные неимущественные права //М.: Статут. – 2019. С. 239-241.
10. Харитонова Ю. С. Правовой режим результатов деятельности искусственного интеллекта //Современные информационные технологии и право: монография/МГУ им. МВ Ломоносова. Юридический факультет. – 2019. – С. 68-83.
11. Хисамова З.И., Бегишев И.Р. Сущность искусственного интеллекта и проблема определения правосубъектности // Вестник МГОУ. Серия: Юриспруденция. 2020. №2. URL: https://cyberleninka.ru/article/n/suschnost-iskusstvennogo-intellekta-i-problema-opredeleniya-pravosubektnosti

КАК ТЕХНОЛОГИИ WEB 3.0 СПАСУТ МИР ОТ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Автор: **Шрайбман Михаил**
CEO, «Осьминожка» - integrator web 3.0

В современном мире происходят глобальные изменения разных сфер жизни, связанные с появлением и развитием искусственного интеллекта (далее– ИИ). Кажется, что технологии только-только начали завоёвывать разные отрасли, но исследователи уже долгое время пытаются найти как удачные модели применения ИИ, так и решение проблем, вызванных его появлением и последующим развитием. К таким проблемам относят качество результата работы, выполненной с помощью ИИ, ошибки в выдаче и обработке информации, субъективизм, отсутствие необходимой инфраструктуры, мощностей и технологий[54]. Также остро стоит вопрос правового статуса, которым можно наградить ИИ, вопрос ответственности и последствий, вопрос разрешения конфликтных и спорных ситуаций с участием лиц, использовавших ИИ[55]. Таким образом, актуальным вопросом, поднятым в рамках данной работы, становится поиск технологий, которые могут спасти интернет-среду и другие отрасли от угроз, созданных ИИ, и создать более благоприятные условия для его использования и развития. Но, прежде чем перейти к рассмотрению этого вопроса, поговорим о том, какие отрасли в мире и в России выигрывают от применения технологий ИИ.

Применение искусственного интеллекта зачастую связывают с решением маркетинговых задач, например, созданием контента, или находят следы его применения в сфере e-commerce. Однако его возможности гораздо шире. Из-за возможности работы с большим объёмом данных, применение ИИ актуально для ряда промышленных сфер, например, нефтегазовой. ИИ здесь выступает как инструмент обработки и сортировки данных, связанных с показателями качества нефти[56]. При этом нейросеть пока не выдаёт абсолютно точный результат, а также может использоваться для обработки закрытых данных, что в случае атак приведёт к утечке конфиденциальной информации и нарушению безопасности[57]. Технологии ИИ повлияли на сферу туризма и гостиничного сервиса. Доставка, уборка и даже заселение гостей – всё это теперь можно выполнять без участия человека[58]. Такая ситуация позитивно влияет на экономические показатели туристического бизнеса. Но при этом вновь создаются угрозы – потеря рабочих мест,

[54] Седых Н.В., Фоканов И.П. Проблемы и перспективы развития технологии искусственного интеллекта // ЕГИ. 2022. №44 (6).
[55] Лазарева М.М. Правовой статус искусственного интеллекта // Вестник науки. 2022. №1 (46).
[56] Тутыгин В. Искусственный интеллект в нефтегазовой индустрии как фактор развития производственной системы // SAI. 2023. №Special Issue 3.
[57] Там же.
[58] Федорова А.Э., Коропец О.А., Гази Халид Отношение работников гостиничного бизнеса к взаимодействию с коллаборативными роботизированными технологиями // УПИРР. 2022. №2.

а также возникновение новых психосоциальных отношений (человек—робот), в которых пока не всё так однозначно[59]. Не менее важна и область медицины. Ряд исследователей полагает, что использование алгоритмов искусственного интеллекта позволит улучшить систему мониторинга здоровья[60]. Технологии мониторинга, созданные на базе технологии ИИ, позволят предупредить риски развития ряда заболеваний, а также проконтролировать психофизическое состояние пациентов[61]. Есть уже и наглядные примеры использования ИИ в медицинской сфере. Например, в марте 2023 года в одном из университетов Торонто исследователи с помощью ИИ за 30 дней смогли получить данные о препарате, который в будущем сможет справиться в борьбе с одной из форм рака печени[62]. Однако и здесь вновь риски – дорогостоящие технологии, недостаток данных, требования к появлению высококлассных специалистов и высокая цена последствий получения ошибочных диагнозов и результатов. Несмотря на это, указ Президента РФ Владимира Путина, посвящённый стратегии развития ИИ, включает задачу повысить уровень доверия граждан к технологиям искусственного интеллекта в 2030 году на 30%, а также подготовить 95% приоритетных отраслей экономики к внедрению ИИ. Ещё один аспект – увеличение числа выпускников вузов по специальностям, связанным с искусственным интеллектом до 15,5 тыс. ежегодно[63].

Таким образом, развитие искусственного интеллекта порождает как много возможностей, так и много угроз. Один из способов решения этой конфликтной ситуации – открытость больших языковых моделей (далее – LLM). И этот вопрос уже активно обсуждается. Например, в марте 2024 года предприниматель Илон Маск подал в суд на компанию OpenAI и на её соучредителя Сэма Альтмана. В иске Маска говорится о том, что компания использует искусственный интеллект для увеличения прибыли компании Microsoft, а не на благо человечества[64]. Эта проблема привлекает внимание не только Илона Маска. Представители бизнеса как в России, так и за рубежом, не готов использовать LLM-модели, поскольку, во-первых, считают, что их данные будут использоваться для обучения моделей; а, во-вторых, не знают, на каких данных обучались эти модели, что не повышает доверие к искусственному интеллекту. Однако разработка собственной языковой модели чрезвычайно дорогостоящая задача. В связи с этим должны существовать открытые LLM модели – иными словами, децентрализованные. Децентрализация – один из признаков Web 3.0, о чём мы поговорим подробнее далее.

И действительно, открытость LLM решит много вопросов и позволит хотя бы частично минимизировать риски и угрозы, связанные с внедрением технологий ИИ в разные сферы жизни.

[59] Федорова А.Э., Коропец О.А., Гази Халид Отношение работников гостиничного бизнеса к взаимодействию с коллаборативными роботизированными технологиями // УПИРР. 2022. №2.
[60] Исмаилов О.М., Мирзахалилов С.С., Холдарова Г.Н. Методы применения алгоритмов искуственного интеллекта в мониторинге здоровья спортсменов во время тренировок и соревнований // SAI. 2023. №Special Issue 3.
[61] Там же.
[62] ИИ за 30 дней разработал потенциально эффективное лекарство от рака печени // Коммерсантъ. URL: https://www.kommersant.ru/doc/5887307 (дата обращения: 11.03.2024)
[63] Национальная стратегия развития искусственного интеллекта в России // Tadviser.
[64] Илон Маск подал в суд на OpenAI и ее создателя Сэма Альтмана // РБК. URL: https://www.rbc.ru/technology_and_media/01/03/2024/65e213439a7947a819b19faf (дата обращения: 11.03.2024)

Например, это позволит избежать монополизации технологий, как это произошло в случае с OpenAI. Многие компании смогут внедрять их в свою работу, не преследуя цель получить коммерческую выгоду. Каждая компания сможет развивать собственную систему, используя данные из открытого доступа. При этом это даст толчок к дополнительному развитию, поскольку такая открытость послужит поводом для внимания со стороны разработчиков, которые смогут применить свои знания и навыки для совершенствования кода по примеру того, как это обычно происходит на GitHub с другими сервисами и проектами. Таким образом, это частично решит проблему нехватки квалифицированных специалистов и глобального недоверия к данным, предоставляем ИИ. Кроме того, помимо очевидной пользы, которую может привнести ИИ в разные сферы жизни, существует и вред. Например, технологии ИИ могут использоваться мошенниками для взломов систем или обмана граждан. К примеру, сейчас мошенники в России активно используют ИИ для подмена голосов и лиц с целью выманивания денежных средств через взломанные аккаунты в социальных сетях[65]. И вновь мы возвращаемся к вопросу о внедрении технологий web 3.0, которые позволят предотвратить многие из таких случаев. Подтверждает этот тезис и недавний указ Президента РФ Владимира Путина об обновлении стратегии развития ИИ до 2030 года. Один из вызовов —прозрачность и объяснимость работы ИИ, а также недискриминационный доступ пользователей к информации об алгоритмах[66]. Этот тезис хорошо подтверждает необходимость внедрения технологий web 3.0, которые как раз и нацелены на прозрачность, открытость и доступность. Децентрализация, технологии блокчейна, смарт-контракты и NFT позволят защитить данные и справиться с угрозами там, где привычные технологии и софт уже не справляются. Кроме того, обеспечат независимость стран от политической, экономической и иных угроз развития со стороны других государств. При этом важно также рассмотреть необходимость управления децентрализацией. Централизованные технологии находятся под контролем компаний или государств, в то время как децентрализованные технологии позволяют человеку управлять процессами. Однако для того, чтобы общество могло эффективно управлять этими технологиями, необходимо использовать другие инновационные решения, такие как технологии web 3.0.

[65] Мошенники начали вымогать деньги с помощью созданных ИИ голосовых сообщений // Forbes. URL: https://www.forbes.ru/tekhnologii/503941-mosenniki-nacali-vymogat-den-gi-s-pomos-u-sozdannyh-ii-golosovyh-soobsenij (дата обращения: 11.03.2024).
[66] Национальная стратегия развития искусственного интеллекта в России // Tadviser.

Многие противники искусственного интеллекта также высказывают тезисы о том, что ИИ захватит мир, и это обернётся катастрофой для человечества. Опровержению этому тезису посвящено также немало статей[67]. По нашему мнению, на текущий момент возможности ИИ можно сравнить с возможностями стажёра или начинающего специалиста в любой области. Его можно использовать лишь как помощника, но этих мощностей, конечно же, не хватит для «захвата мира». Для развития же более «умного» ИИ потребуются большие мощности, которых сейчас ни у государства, ни у частных компаний нет. Это подтверждается тем фактом, что упомянутый ранее гендиректор OpenAI Сэм Альтман жалуется на нехватку чипов и процессоров для обучения систем ИИ, и просит привлечь $5–7 трлн в создание новых мощностей[68]. Сумма весьма значительная – для сравнения оборот рынка полупроводниковых компонентов достигнет рубежа в $1 трлн только к концу десятилетия, а совокупная капитализация Microsoft и Apple, приближается к $6 трлн[69]. Получается, что в настоящее время создание более развитого искусственного интеллекта становится невозможным из-за ограничений мощностей и бюджетов государств и компаний. Но его развитие может ускориться благодаря интеграции во все бизнес-процессы. Для этого понадобится привлечение значительного количества людей, заинтересованных в развитии технологии. Открытость системы, подобная тому, что мы наблюдаем на GitHub, играет важную роль в этом процессе. Вновь возвращаясь к теме актуальности web 3.0, решением является открытость и децентрализация.

Подводя итог, отметим ещё раз, что развитие web 3.0 поможет снизить риски злоупотребления ИИ, повысит доверие граждан к нему, а также безопасность данных компаний и пользователей. А это – первый шаг на пути к решению обозначенных нами ранее проблем, которые не позволяют ИИ глубже внедряться в различные сферы социальной, экономической и политической жизни России и других стран мира.

[67] Фантазия или реальность: готов ли искусственный интеллект захватить мир // РИАМО. URL: https://riamo.ru/article/638492/fantaziya-ili-realnost-gotov-li-iskusstvennyj-intellekt-zahvatit-mir (дата обращения: 11.03.2024).
[68] WSJ узнала о планах главы OpenAI Альтмана собрать $7 трлн для выпуска чипов для ИИ // Forbes. URL: https://www.forbes.ru/tekhnologii/505902-wsj-uznala-o-planah-glavy-openai-al-tmana-sobrat-7-trln-dla-vypuska-cipov-dla-ii (дата обращения: 11.03.2024).
[69] Глава OpenAI Сэм Альтман предложил скинуться всем миром, чтобы построить десятки новых предприятий для TSMC // 3D News. URL: https://3dnews.ru/1100045/glava-openai-sem-altman-predlagaet-skinutsya-vsem-mirom-chtobi-postroit-desyatki-novih-predpriyatiy-dlya-tsmc (дата обращения: 11.03.2024).

ЦИФРОВИЗАЦИЯ И ВНЕДРЕНИЕ ТЕХНОЛОГИЙ ДЛЯ РЕШЕНИЯ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ЛЮДЕЙ ПРОДОВОЛЬСТВИЕМ

Автор: **Филина Наталья**,
Секретарь EURALO (At-Large, ICANN)

Мы все мечтаем о гармоничном течение жизни и достатке всех ресурсов для всего человечества, воды и продовольствия в первую очередь. Катастрофой является то, что с нехваткой продовольствия и голодом сталкивается значительная часть населения земного шара.

Каковы причины? Конфликты, изменение климата, неэффективное управление экономикой и распределением продовольствия, нарушение системы поставок, недобросовестная глобальная конкуренция и искусственный запрет доступа к продовольствию…

Одна из целей ООН в области устойчивого развития - сокращение голода и недоедания в мире. Одной из самых гуманистичных и социально значимых задач научных прорывов, открытий и технологического развития, на мой взгляд, является улучшение качества жизни людей во всех аспектах. В первую очередь – обеспечение каждого живущего на планете жизненно необходимыми ресурсами и продовольствием.

В этой статье будут рассмотрены общие примеры технологических достижений, цифровизации агропромышленной и логистической индустрии, которые помогают нам бережно и с максимальным эффектом пользоваться ресурсами и сделать доступным качественное продовольствие для максимального количества людей.

***

Сегодня научно-техническое сообщество занимается поиском путей, а главное – внедрением высокотехнологичных практических решений, которые уже сейчас помогают решать продовольственные проблемы и предотвращать в будущем катастрофы и обеспечивать население едой.

Цифровизация агропромышленного комплекса

Цифровой агропромышленный комплекс – это менее затратное, прогнозируемое, эффективное производство сельскохозяйственной продукции. А значит это то, что дешевого и качественного продовольствия может и должно быть больше. Больше сытых людей.

То, что раньше было технологическим прорывом, сегодня – обыденная реальность. Широкомасштабное внедрение IoT в агросекторе (простыми словами - применение специального программного обеспечения и высокотехнологичных устройств) помогает наращивать объем производства продуктов питания, усовершенствовать логистические цепочки и правильно распределять продукцию, повысить безопасность и качество продуктов питания, и что очень важно – сделать их дешевле. Как именно?

На сегодняшнем уровне развития технологий «точное земледелие» или «точный» агропромышленный комплекс - это полный цикл производства, который на основе полученных данных не просто эффективно распределяет ресурсы, но и строит прогнозы и дает рекомендации рационального их использования в будущем.

В таком комплексе важнейшую роль выполняют данные. Собирают эти данные датчики температуры, полива, освещения, оснащения удобрениями, загружается data в системы управления фермами, теплицами. Применяется робототехника в процессе производства, переработки, перевозках (автономные транспортные средства), автоматизированное оборудование, технологии с переменной скоростью, реагирующие на внешние факторы и следующие загруженным алгоритмам.

Цифровизация может предложить и другие полезные решения. Беспилотники и спутники – это не только геодезия и картография, это еще и помощь в дистанционном уходе за почвами (зондирование, внесение удобрений с учетом неоднородности ландшафта и минерального состава почв). Контроль посевных работ мы тоже отдаем БПЛА, которые получают данные со спутников, оптимизируют маршруты сельхозтехники. А техника под управлением ПО точечно засеивает и собирает урожаи с тех земель, где период созревания агрокультур завершен, или вносит минеральные удобрения в места их дефицита. Даже с учетом инвестиций в покупку и эксплуатацию БПЛА можно значительно оптимизировать общие расходы на проект и увеличить урожайность.

Важно собрать урожай, но не менее важно его сохранить. Датчики, замеряющие и передающие данные о микроклимате места хранения продовольствия поможет уберечь его от порчи и доставить потребителю зерно, фрукты, овощи, мясо, молочную продукцию свежей. Прогнозы времени созревания и объемов сбора урожая позволяют управлять резервами и распределять продукцию с учетом рисков неурожайных сезонов или форс-мажоров.

Для всех очевидно, что роботы не смогут совершенно заменить человека, но внедрение цифровизации и использование технологий интернета вещей позволяет автоматизировать многие процессы в сельском хозяйстве и сделать возможным удаленный контроль масштабных агрокомплексов и сельхозугодий. Вот пример алгоритма самой простой цепочки информации: датчик, модем, облачный сервер, цифровая платформа.

Не менее важную роль играет верное прогнозирование. На основе данных, полученных от датчиков и сенсоров, систем сбора и анализа данных о факторах, влияющих на урожайность, состояния сельскохозяйственных угодий, данных, собираемых на животноводческих фермах (не обходится здесь без ИИ и машинного обучения), аграрии могут анализировать прошлые и текущие показатели, прогнозировать тенденции в развитии посевов, управлять урожайностью, удоями, динамикой поголовья, отслеживать факторы риска, создавать и своевременно реагировать на угрозы.

Актуальной остается и проблема ответственного потребления, ведь природные ресурсы исчерпаемы, использовать их нужно бережно. А что, если земельных ресурсов не хватает, а обеспечение логистики продуктов питания в сложно доступные районы невозможно? Здесь помогают инфраструктурные инновации сельского хозяйства: Развитие вертикального фермерства и гидропоники. Технологии позволяют выращивать продукцию в замкнутых системах без почвы, что позволяет сэкономить земельные ресурсы и производить продовольствие в условиях ограниченного пространства.

Также весьма важно усиление контроля, а, соответственно, и оценка качества потребляемой продукции: благодаря возможности отслеживать всю цепочку производства (например, от подготовки семян к посадке до упаковки и доставки на прилавки магазинов или склады дистрибьютеров), сельскохозяйственные предприятия могут повысить качество и безопасность своей продукции, что очень важно для конечных потребителей. Не просто кормить людей, но кормить их безопасной продукцией и сохранять здоровье потребителей.

Отдельно стоит упомянуть агробиотехнологии. Их внедрение помогает значительному снижению себестоимости продуктов питания, повышение плодородия почв, рентабельности сельхозпроизводства, улучшение качественных характеристик сельхозкультур и улучшению экологического состояния агроландшафтов. Это происходит посредством снижения химической нагрузки на сельскохозяйственные земли и соседние ландшафты, постоянного контроля и мониторинга параметров микробиологического состояния почв. Крупнейшие в мире экономики биотехнологий обеспечивают глобальный рынок экологически чистой продукцией. Очень важно не только накормить, но и накормить безопасной продукцией.

Локальное конкурентное развитие агробиотехнологий, увеличение научно-исследовательских разработок в стране – это еще и инструмент в маркетинговой борьбе, когда давление крупных производителей химикатов и опасных, но более доступных удобрений нивелируется и заменяется местной качественной, современной продукцией, адаптированной к локальным условиям применения.

Количество биотехнологических компаний в каждой стране во многом определяет список стран-передовиков. Есть и спорные, революционные и очень прибыльные решения: одна из развивающихся области биотехнологий – производство искусственного мяса. Мы здесь, в России, традиционно предпочитаем все настоящее, живое. Но видим, что в мире спрос на искусственные мясо (и молочные) продукты растет, растет и количество стартапов-инноваторов. Согласно исследованию Grand View Research, по состоянию на 2021 год мировая биотехнологическая индустрия уже оценивалась в 1 трлн долларов. Осторожно (или настороженно?) смотрим, насколько доверие мясоедов и любителей молока будет завоевано маркетологами, предлагающими технологично произведенные заменители. И будет ли это решением для тех слоев населения, которые реально нуждаются в продовольствии, а не просто экспериментируют.

Оптимизация и цифровизация логистики – важный элемент решения продовольственного кризиса. Грузы (семена, удобрения, топливо, готовое продовольствие, упаковка, полуфабрикаты и прочее) должны доставляться перерабатывающему предприятию, транспортной компании и потребителю в срок, максимально эффективно с минимальными затратами и с исключением ошибок навигации, с соблюдением безопасности грузов.

Сейчас уже повсеместно внедряются ИТ-платформы, которые контролируют грузовой поток, загрузку-разгрузку, хранение продукции, грузов, формирование и проверку сопровождающих документов. Это инструменты цифровой оптимизации логистики. Результат – минимальные потери при транспортировке и своевременное, максимальное обеспечение нужд тех, кто эти грузы ждет. Продовольствие должно туда, где в нем нуждаются. А аналитика данных и искусственный интеллект помогает строить прогнозы динамики спроса, оптимизировать логистику с учетом влияния внешних и внутренних факторов.

Технологии – это решение проблем обеспечения продовольствием население планеты. Передовые технологии помогают сократить расходы, переработать отходы, увеличить и удешевить производство сельскохозяйственной продукции.

Однако важно сохранять понимание того, что ни роботы, ни интерфейсы, ни платы и датчики, средства связи, сервера, дроны и спутники, а также ПО не помогут без синергии и сотрудничества на всех уровнях. Все мы являемся участниками процесса: академическое сообщество, технологи, исследователи, ИТ-корпорации и маленькие стартапы, потребители, бизнес, правительственные организации. Для успеха решения задачи накормить человечество нам нужно объединиться, социально поддерживать прогресс, инвестировать в него, просвещать население.

И помнить, что самой правильной конечной целью технологии всегда будет гуманная цель – помощь людям и улучшение жизни на нашей планете.

НЕЙРОМОРФНЫЕ ВЫЧИСЛЕНИЯ: БУДУЩЕЕ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ?

Автор: **Капитанов Александр**
аспирант факультета гуманитарных наук и социальных технологий,
Российский университет дружбы народов им. П. Лумумбы

Мы привыкли к тому, что в любой окружающей нас электронике существует универсальное устройство – традиционный процессор, который имеется во всех видах электронных аппаратов. Принципы его работы заложил американский математик, физик Джон фон Нейман в 40-е годы прошлого столетия. С тех пор до настоящего времени они не претерпели существенных изменений: процессор анализирует простые команды, обращается к памяти или регистрам (ячейкам хранения данных) и выполняет эти команды друг за другом, посылает электронный сигнал из точки А в точку Б. Ранее процессор мог выполнять лишь одну операцию за один цикл работы. В настоящий момент многие из нас используют электронные устройства, имеющие несколько ядер в процессоре, которые позволяют ему выполнять множество задач на одном процессоре за счет распределения ресурсов. Однако уже сейчас в России и за рубежом идут активные исследования в области нейроморфных вычислений и процессоров на их базе, которые могут прийти на смену традиционным аналогам.

Общая характеристика

Итак, нейроморфные вычисления – это новая форма вычислений, основной механизм функционирования которой строится на имитации принципа работы человеческого мозга.
Говоря о нейроморфных системах, необходимо обозначить две ключевых сложности имитации человеческого мозга на текущем этапе. Первое: в настоящий момент невозможно смоделировать каждый участок мозговой активности. Второе: человеческий мозг является комплексной структурой, внутренние сети которого невозможно выразить аналитически с точки зрения их низшего уровня структуры. Учитывая эти два момента, можно приступить к описанию принципов работы нейроморфного процессора.

Любой процессор состоит из электронных элементов – транзисторов, используемых в целях управления электрическим током. Любое электронное устройство содержится огромное количество таких элементов. Подобным же образом функционирует и человеческий мозг, состоящий из нейронов, которых насчитываются десятки миллиардов. Существует междисциплинарная область исследований на стыке биологии, физики, информатики и математики – нейроморфный инжиниринг, целью которого является создание искусственной системы, позволяющей анализировать информацию подобно человеческому мозгу. Основным инструментом нейроморфных вычислений являются искусственные нейронные сети, представляющие собой математические модели, имитирующие принцип работы человеческого мозга[70].

Отличия нейроморфных процессоров от традиционных

Необходимо отметить, что основной целью нейроморфного процессора, в отличие от традиционного процессора, выполняющего арифметические и логические вычисления, является воспроизведение структуры человеческого мозга[71]. Нейроморфные процессоры используются в узкоспециализированный области по сравнению с традиционной вычислительной архитектурой: развитие и работа нейронных сетей.

Ключевыми отличиями нейроморфных процессоров по сравнению с традиционными процессорами на архитектуре фон Неймана состоят в следующем:

[70] Ежов В. «Нейроморфные системы как инструмент реализации искусственного интеллекта», Электроника, № 2 (00203), 2021, 1 с.
[71] Электронный ресурс: «A mind of their own: we need to talk about neuroprocessors». URL: https://www.kaspersky.com/blog/neuromorphic-processor-motive/44736/. (Дата обращения: 19.01.2024).

- высокая производительность[72];
- низкое энергопотребление[73];
- малые габариты и низкая стоимость[74];
- высокая отказоустойчивость[75].

Развитие нейроморфных процессоров в России и за границей: истоки и современность

История появления нейроморфных вычислений берет свое начало еще в 40-х годах прошлого века, когда американские ученые Уолтер Питтс и Уоррен Мак-Каллок предложили модель нейрона и сформулировали его роль в человеческом мозге[76]. Их труд оказал фундаментальное влияние на развитие нейронных сетей.

В 80-е годы XX столетия ученые приступили к исследованию потенциала нейроморфных вычислений для прикладных целей в робототехнике и технологиях искусственного интеллекта. Пионером в области нейроморфных вычислений является американский ученый Карвер Мид, который в 1980-е занимался исследованиями в области вычислений с использованием моделей биологии[77].

Создание американской компанией IBM в 2014 г. нейроморфного процессора «TrueNorth»[78] ознаменовало прорыв в области нейроморфных вычислений. Данный процессор использовался для таких функций, как распознавание лиц и обработка естественного лица.

В 2017 году американская компания «Intel» представила нейроморфный процессор «Loihi», который содержит 131 тыс. искусственных нейронов и 131 млн. синапсов[79]. Архитектура данного процессора искусственно тождественна нейронной сети, где создается взаимосвязь между нейронами посредством передачи импульсов в синапсах.

В 2021 г. «Intel» создала нейроморфный процессор следующего поколения «Loihi 2». Появились существенные изменения по сравнению с предыдущим поколением: количество нейронов в новом процессоре выросло почти в 10 раз, сократилась рабочая площадь, а также расширились его возможности «обучения».

Развитие нейроморфных процессоров в ЕС[80]

В 2015 г. в Гейдельберском университете в рамках научно-исследовательского проекта «Human Brain Project» были завершены работы по созданию нейроморфного процессора «BrainScaleS»[81]. Целью проекта являлось исследование в области вычислительной нейробиологии. Основными особенностями данного процессора являются: использование аналоговых схем, позволяющих имитировать физические модели нейронных связей в целях повышения скорости функционирование процессора; обеспечение указанного ускорения в целях доставки искусственных нейронов, которые можно соединить друг с другом[82].

Развитие нейроморфных процессоров в Великобритании.

В 2018 г. ученые-исследователи Манчестерского университета запустили гигантский суперкомпьютер на основе нейроморфных процессоров «SpiNNaker», способный выполнять более 200 трлн действий в секунду. Его производительность составляет 1% от масштаба человеческого мозга. Ученые-исследователи, стоящие за созданием «SpiNNaker», планируют смоделировать с его помощью работу до 1 млрд нейронов.

[72] Электронный ресурс: «Intel launches its next-generation neuromorphic processor - so, what's that again?». URL: https://arstechnica.com/science/2021/09/understanding-neuromorphic-computing-and-why-intels-excited-about-it/. (Дата обращения: 19.01.2024).
[73] Электронный ресурс: «В России разрабатывают нейроморфные процессоры. Чем они лучше обычных и где понадобятся?». URL: https://trashbox.ru/link/nejromorfnye-processory-v-rossii?ysclid=lspxumbx4s665445451. (Дата обращения: 19.01.2024).
[74] Там же.
[75] Там же.
[76] Kunze H. «Engineering, Mathematics and Artificial Intelligence: Foundations, Methods and Applications», CRC Press, 2023, 213 p.
[77] Furber S. «Large-scale neuromorphic computing systems», Journal-scale neuromorphic computing systems, 2016, 2-3 p.
[78] Indiveri G. «Introducing Neuromorphic Computing and Engineering», Neuromorphic Computing and Engineering, 2021, 3 p.
[79] Абдулин Т.Х., Зеленский А.А. «Проблема обеспечения производительности доверенных систем управления с глубинным обучением», 2022, 62 с.
[80] Электронный ресурс, «Intel Loihi 2. Нейроморфный процессор, следующее поколение». URL: https://habr.com/ru/companies/intel/articles/583006/. (Дата обращения: 19.01.2024).
[81] Электронный ресурс: «Brain-inspired multiscale computation in neuromorphic hybrid systems». URL: https://cordis.europa.eu/project/id/269921/results. (Дата обращения: 19.01.2024).
[82] Электронный ресурс: «Самые яркие проекты по созданию нейроморфных процессоров [part 3]». URL: https://habr.com/ru/companies/yadro/articles/648119/. (Дата обращения, 19.01.2024).

Цель данного суперкомпьютера заключается в изучении строения человеческого мозга. Уже имеются первые успехи: смоделирован участок коры головного мозга, состоящий из 80 тыс. нейронов. В настоящий момент ведется работа по созданию новой версии суперкомпьютера «SpiNNaker 2», которая повысит его производительность примерно в 10 раз[83].

Развитие нейроморфных процессоров в России

В России АО «Лаборатория Касперского» и ООО «Мотив НТ» в 2022 г. представили отечественный нейроморфный процессор «Алтай»[84]. По своим техническим характеристикам отечественный процессор уступает американскому «Loihi». Однако «Алтай» имеет одно преимущество – неограниченная масштабируемость, что означает способность системы увеличивать свою производительность (на текущий момент она составляет ~67 млрд действий в секунду). Необходимо заметить, что для данного процессора разработано отечественное ПО, что позволит упростить задачу нашим ученым-исследователям по интеграции нейроморфных процессоров в различные системы. Разработчики подчеркивают, что к 2025 г. планируется выпуск коммерческой версии данного процессора[85].

Также над созданием собственного нейроморфного процессора активно работает НИЦ «Курчатовский институт». По словам президента Центра М.В. Ковальчука, технологии, связанные с нейроморфными процессорами, нуждаются в регуляторной этике[86].

Указом Президента Российской Федерации от 15.02.2024 г. № 124 внесены существенные изменения в Национальную стратегию развития искусственного интеллекта на период до 2030 года: Россия ставит задачу развить массовое производство отечественных микропроцессоров (включая нейроморфные процессоры), применяемых в области искусственного интеллекта[87].

Сферы использования нейроморфных процессоров

- IoT (Internet of Things - «Интернет вещей») является комплексной системой, объединяющей в себе огромное количество устройств. Использование нейроморфных процессоров в Интернете вещей позволит повысить скорость обработки данных и, как следствие, подключить еще больше электронных устройств; при этом производительность системы в целом не подвергнется замедлению[88].
- Умное видеонаблюдение: нейроморфные процессоры в умных камерах ускорят обработку данных. В целях повышения уровня безопасности и более быстрого реагирования на возможные инциденты нейроморфные процессоры принесут пользу в местах массового пребывания людей: железнодорожные вокзалы и автовокзалы, аэропорты, метро[89].
- Кибербезопасность: в целях нивелирования угроз нейроморфные процессоры позволят системам безопасности выйти на качественной новый уровень и оперативнее проводить анализ опасностей[90].
- Автоматизация: нейроморфные процессоры расширят количество выполняемых задач и гибкость автоматизированных систем. Так, одного условного робота можно использовать в качестве сборщика деталей на заводе, а при необходимости он выполнит функции, к примеру, водителя[91].

[83] Электронный ресурс: «В Великобритании запустили самый большой в мире нейроморфный суперкомьютер» - https://strana-rosatom.ru/2018/12/27/intellekt-desyati-myshej/?ysclid=lsrsuw5e4n167798773 (дата обращения: 19.01.2024).
[84] Электронный ресурс: «Лаборатория Касперского» инвестировала в создание первого нейроморфного чипа в России» - https://www.kaspersky.ru/about/press-releases/2022_laboratoriya-kasperskogo-investirovala-v-sozdanie-pervogo-nejromorfnogo-chipa-v-rossii?ysclid=lsrt9yzgqg32185243 (дата обращения: 19.01.2024).
[85] Электронный ресурс: «В России разрабатывают нейроморфные процессоры. Чем они лучше обычных и где понадобятся?». URL: https://trashbox.ru/link/nejromorfnye-processory-v-rossii?ysclid=lspx-umbx4s665445451. (Дата обращения: 19.01.2024).
[86] Электронный ресурс: «Курчатовский институт работает над созданием нейроморфного компьютера» - https://ria.ru/20230929/nauka-1899511445.html?ysclid=lspzvgat33722501937 (дата обращения: 19.01.2024).
[87] Указ Президента Российской Федерации от 15.02.2024 N 124 "О внесении изменений в Указ Президента Российской Федерации от 10 октября 2019 г. N 490 "О развитии искусственного интеллекта в Российской Федерации" и в Национальную стратегию, утвержденную этим Указом" // Собрание законодательства Российской Федерации, 2019, № 41, ст. 5700). Официальный интернет-портал правовой информации: http://pravo.gov.ru/ - 2024. - 15 января.
[88] Электронный ресурс: «В России разрабатывают нейроморфные процессоры. Чем они лучше обычных и где понадобятся?». URL: https://trashbox.ru/link/nejromorfnye-processory-v-rossii?ysclid=lspx-umbx4s665445451. (Дата обращения: 19.01.2024).
[89] Там же.
[90] Электронный ресурс: «В России разрабатывают нейроморфные процессоры. Чем они лучше обычных и где понадобятся?». URL: https://trashbox.ru/link/nejromorfnye-processory-v-rossii?ysclid=lspx-umbx4s665445451. (Дата обращения: 19.01.2024).
[91] Там же.

- Медицина: внедрение нейроморфных процессоров позволит повысить точность формулирования диагноза, что поможет уменьшить нагрузку на медицинский персонал. При интеграции нейроморфных процессоров в медицинское оборудование текущее состояние пациента будет всесторонне анализироваться, а также появится возможность прогнозировать возможные рецидивы болезни или ее дальнейшее развитие[92].

Что показывает статистика?

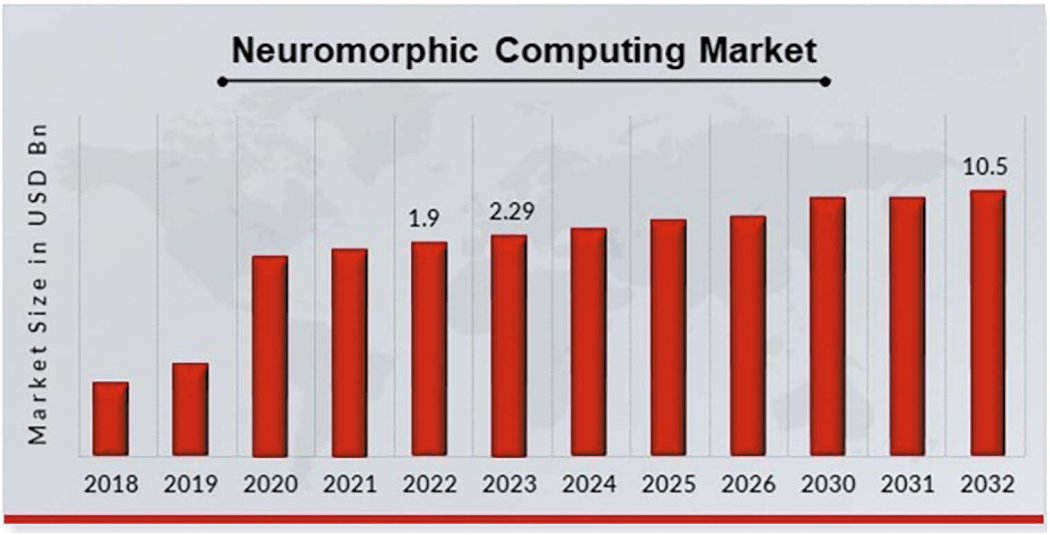


Рисунок 1. Прогнозируемая динамика глобального рынка нейроморфных компьютеров.
Источник: https://www.marketresearchfuture.com/reports/neuromorphic-computing-market-5110\

В 2022 г. объем мирового рынка нейроморфных вычислений составлял около 2 млрд долларов США. Прогнозируется, что к 2030 г. такой объем достигнет более 10 млрд долларов США, т.е. совокупный среднегодовой темп роста за 7 лет составит 21% (Рис. 1). Драйвером роста использования нейроморфных процессоров является повышенный спрос на применение технологий искусственного интеллекта[93].

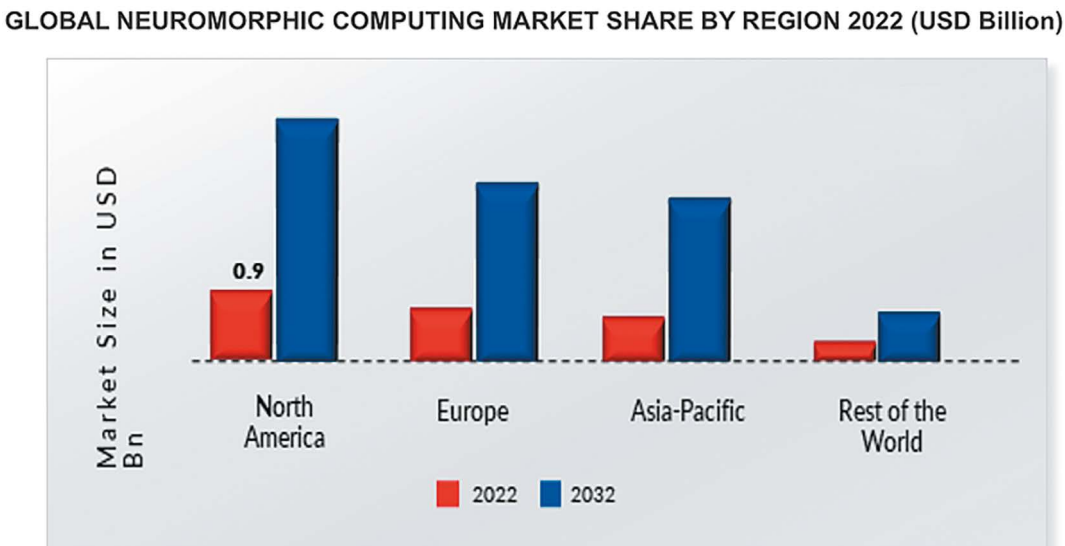


Рисунок 2. Прогнозируемая динамика рынка нейроморфных компьютеров по макрорегионам
Источник: https://www.marketresearchfuture.com/reports/neuromorphic-computing-market-5110\

[92] Электронный ресурс: «В России разрабатывают нейроморфные процессоры. Чем они лучше обычных и где понадобятся?». URL: https://trashbox.ru/link/nejromorfnye-processory-v-rossii?ysclid=lspx-umbx4s665445451. (Дата обращения: 19.01.2024).
[93] Электронный ресурс: «Neuromorphic Computer Market Overview» URL: https://www.marketresearchfuture.com/reports/neuromorphic-computing-market-5110. (Дата обращения: 19.01.2024).

Рассматривая региональный аспект рынка, следует отметить, что в 2022 г. на общемировом уровне доминировала Северная Америка с объемом около 1 млрд долларов США. На втором месте расположилась Европа. Третье место занимает Азиатско-Тихоокеанский регион. В аналогичной последовательности прогнозируется и рост указанного рынка к 2032 г.[94](Рис. 2)

Будущее с нейроморфными процессорами

Подводя итог, стоит подчеркнуть, что традиционные процессоры на архитектуре фон Неймана, осуществляя линейную обработку данных, выполняют и продолжат на принципе последовательности выполнять широкий спектр задач в различных областях, в то время как нейроморфные процессоры, имеющие возможность параллельно производить вычисления, используются в узкоспециализированный области: развитие и работа нейронных сетей, что в идеальном варианте, приведет к имитации структуры функционирования человеческого мозга.

В настоящий момент нейроморфные процессоры активно используются в приложениях с технологиями искусственного интеллекта. Системы, основанные на таких технологиях, могут учиться в режиме настоящего времени. Нейроморфные вычисления представляют собой платформу для указанных систем, которые ускорят анализ данных и повысят эффективность и станут более точными в принятии решений.

Нейроморфные вычисления обеспечат более высокую производительность и ускоренную работу вычислений. Они помогут снизить энергопотребление, что выгодно как для бизнеса, так и для государственного сектора.

Технологии на основе нейроморфизма имеют огромный потенциал прикладного применения. Данный тип вычислений может быть использован в различных сферах жизнедеятельности человека: от бытовой сферы до здравоохранения и образования. Вопрос состоит лишь в том, готовы ли мы доверить нейроморфным процессорам сферы, где требуется человеческое и социальное понимание ситуации.

[94] Электронный ресурс: «Neuromorphic Computer Market Overview» URL: https://www.marketresearchfuture.com/reports/neuromorphic-computing-market-5110. (Дата обращения: 19.01.2024).

Библиографический список:

1. Абдулин Т.Х., Зеленский А.А. «Проблема обеспечения производительности доверенных систем управления с глубинным обучением», 2022, 62 с.
2. Ежов В. «Нейроморфные системы как инструмент реализации искусственного интеллекта», Электроника, № 2 (00203), 2021, 1 с.
3. Furber S. «Large-scale neuromorphic computing systems», Journal-scale neuromorphic computing systems, 2016, 2-3 p.
4. Indiveri G. «Introducing Neuromorphic Computing and Engineering», Neuromorphic Computing and Engineering, 2021, 3 p.
5. Kunze H. «Engineering, Mathematics and Artificial Intelligence: Foundations, Methods and Applications», CRC Press, 2023, 213 p.
6. Указ Президента Российской Федерации от 15.02.2024 N 124 “О внесении изменений в Указ Президента Российской Федерации от 10 октября 2019 г. N 490 «О развитии искусственного интеллекта в Российской Федерации» и в Национальную стратегию, утвержденную этим Указом” // Собрание законодательства Российской Федерации, 2019, № 41, ст. 5700). Официальный интернет-портал правовой информации: http://pravo.gov.ru/ - 2024. - 15 января.
7. Электронный ресурс: «В Великобритании запустили самый большой в мире нейроморфный суперкомьютер» - https://strana-rosatom.ru/2018/12/27/intellekt-desyati-myshej/?ysclid=lsrsuw5e4n167798773 (дата обращения: 19.01.2024).
8. Электронный ресурс: «В России разрабатывают нейроморфные процессоры. Чем они лучше обычных и где понадобятся?». URL: https://trashbox.ru/link/nejromorfnye-processory-v-rossii?ysclid=lspxumbx4s665445451 (дата обращения: 19.01.2024).
9. Электронный ресурс: «Курчатовский институт работает над созданием нейроморфного компьютера» - https://ria.ru/20230929/nauka-1899511445.html?ysclid=lspzvgat33722501937 (дата обращения: 19.01.2024).
10. Электронный ресурс: «Лаборатория Касперского» инвестировала в создание первого нейроморфного чипа в России» - https://www.kaspersky.ru/about/press-releases/2022_laboratoriya-kasperskogo-investirovala-v-sozdanie-pervogo-nejromorfnogo-chipa-v-rossii?ysclid=lsrt9yzgqg32185243 (дата обращения: 19.01.2024).
11. Электронный ресурс: «Самые яркие проекты по созданию нейроморфных процессоров [part 3]». URL: https://habr.com/ru/companies/yadro/articles/648119/ (дата обращения, 19.01.2024).
12. Электронный ресурс: «A mind of their own: we need to talk about neuroprocessors». URL: https://www.kaspersky.com/blog/neuromorphic-processor-motive/44736/ (дата обращения: 19.01.2024).
13. Электронный ресурс: «Brain-inspired multiscale computation in neuromorphic hybrid systems». URL: https://cordis.europa.eu/project/id/269921/results (дата обращения: 19.01.2024).
14. Электронный ресурс: «Intel launches its next-generation neuromorphic processor - so, what’s that again?». URL: https://arstechnica.com/science/2021/09/understanding-neuromorphic-computing-and-why-intels-excited-about-it/ (дата обращения: 19.01.2024).
15. Электронный ресурс, «Intel Loihi 2. Нейроморфный процессор, следующее поколение». URL: https://habr.com/ru/companies/intel/articles/583006/ (дата обращения: 19.01.2024).
16. Электронный ресурс: «Neuromorphic Computer Market Overview» URL: https://www.marketresearchfuture.com/reports/neuromorphic-computing-market-5110 (дата обращения: 19.01.2024).

ОСОБЕННОСТИ ЛОКАЛИЗАЦИИ ВИДЕОИГР В КОНТЕКСТЕ ВОПРОСОВ КИБЕРБЕЗОПАСНОСТИ

Автор **Лебедева Марина Владимировна**,
к.п.н., доцент, Нижегородский государственный лингвистический университет имени Н.А. Добролюбова

Автор **Лескин Илья Владиславович**
Нижегородский государственный лингвистический университет имени Н.А. Добролюбова

Автор **Служеникин Дмитрий Игоревич**
Автономная некоммерческая организация «Цифровая экономика»,
г. Москва

Аннотация. В данной статье раскрыты подходы к локализации видеоигр на основе взаимосвязей между вопросами языковой адаптации текста контента к культурному контексту страны и возможными рисками и киберугрозами в индустрии цифровых развлечений. Рассмотрены основные принципы и способы предотвращения киберугроз в переводческой деятельности и определены ориентиры совершенствования профессиональных компетенций переводчика, планирующего начать свой карьерный путь в сфере локализации видеоигр.

Ключевые слова: локализация видеоигр, переводческая деятельность, кибербезопасность, киберугроза, стриминговые сервисы.

Обеспечение устойчивого социально-экономического развития общества и государства во многом зависит от обеспечения защищенности его граждан от внутренних и внешних информационных опасностей и киберугроз в условиях нарастания количества и скорости процессов конвергенции виртуальной и социокультурной реальностей, что в свою очередь стимулирует развитие направлений в области цифровых развлечений, в частности индустрии видеоигр [4,5].

Многие общественные деятели и исследователи в области цифровых технологий считают, что видеоигры способствует развитию цифровых компетенций, социальных навыков и аналитическому мышлению. При этом все единодушно отмечают, что к индустрии видеоигр, которая является «огромным многомиллиардным бизнесом», необходимо относиться серьезно, потому что именно здесь присутствуют угрозы, определяющие поведенческие и моральные аспекты геймсреды [4,5].

Наиболее распространенные угрозы, которые отмечают специалисты в области кибербезопасности, зачастую связаны с несоблюдением элементарных правил информационной безопасности в киберпространстве. Однако особую тревогу вызывает скрытая угроза, обусловленная качеством перевода видеоигр и содержанием цифрового контента стриминговых сервисов, используемых для продвижения видеоигр.

В настоящее время видеоигры по своему влиянию на человека значительно превзошли телевидение, при этом популяризации видеоигр способствует активное применение современных стриминговых сервисов, интерес к которым постоянно возрастает, а вместе с тем и растет их влияние на аудиторию. Индустрия видеоигр и стриминговых сервисов сегодня является мощным инструментом не только пропаганды и агитации, но что особенно настораживает, представляет собой стратегический ресурс формирования образа мышления целого народа.

Актуальность исследования определяется тем, что явлению широкого распространения и доступности видеоигр и стриминговых сервисов сопутствуют нарастающие процессы, угрожающие кибербезопасности, а именно:

через содержание видеоигр и самих игроков продвигаются идеи, определяющие изменения познавательной способности субъекта к расшифровке значений языковых и речевых практик, необходимых для восприятия и осознания «данности мыслящим субъектом», что в итоге ведет к трансформации мировоззрения, в первую очередь, молодежной аудитории, наиболее активно вовлеченной в геймплей [1].

Отсутствие в настоящее время единого стандарта по локализации видеоигр в России и в мире, с одной стороны, и недостаточное осознание специалистами сферы переводческих услуг действительной сущности перевода в условиях нарастания киберугроз в индустрии цифровых развлечений, с другой, снижает качество перевода игрового контента, что в свою очередь создает проблемы: для переводчиков-практиков – слабо проявляется культурная составляющая самого перевода (зачастую это связано с ускоренными сроками вывода видеоигры на рынок цифровых продуктов и необходимостью скорейшего ее продвижения посредством стриминговых сервисов), что является причиной постепенной трансформации языковой картины мира в сознании пользователя видеоигры; для пользователей видеоигр – ошибки в переводе содержания видеоигр и их тиражирование на стриминговых сервисах порождают угрозы, ориентированные на распространение идей и смыслов, которые могут стать причиной разрушения доступности и целостности информации о содержании традиционных национальных ценностей целого народа.

Таким образом, новым трендом кадрового дефицита в цифровой индустрии становится востребованность в специалистах-переводчиках, осознающих действительную сущность перевода в условиях непрерывно нарастающих угроз в киберпространстве.

В контексте представленной работы мы опираемся на понятия «локализация видеоигр» и «переводческая деятельность», рассматриваемые в тесной связи с понятиями «кибербезопасность» и «киберугроза». В нашем исследовании понятие «локализация» рассматривается как «перевод высокого уровня», неотделимый от культурной адаптации текста, то есть адаптации к культурному контексту страны, на язык которого делается перевод содержания видеоигр, при этом «переводческая деятельность» должна способствовать формированию безопасного киберпространства для аудитории [2].

Понятие «кибербезопасность» трактуется специалистами этой области как «обеспечение конфиденциальности, целостности и доступности информации в киберпространстве», а под «киберугрозой» подразумеваются преднамеренные действия, «которые могут нанести ущерб информации, программе или системе», «преднамеренная реализация угрозы называется атакой на информационную систему» [4,5,6].

В контексте нашего исследования особенности «локализации видеоигр» рассматриваются прежде всего относительно цифрового контента, адаптированного к культурному контексту страны, на язык которого делается перевод содержания видеоигр, отличающегося целостностью смысловой составляющей в контексте традиционных национальных ценностей народа и доступностью в неискаженном идеологическом формате на стриминговых сервисах. В этой связи под киберугрозой мы понимаем преднамеренные или непреднамеренные действия переводчиков и(или) стримеров, оказывающие влияние на снижение качества перевода видеоигр и(или) его искажение, что является потенциальной угрозой для мировоззренческой безопасности аудитории.

Исследование построено на следующей гипотезе: понимание переводчиком основных трудностей в области локализации видеоигр, их причин и взаимосвязей с тенденциями развития и угрозами в индустрии цифровых

развлечений позволит определить эффективные подходы в переводческой деятельности, способствующие переопределению текущих тенденцией на переводческом рынке в сторону достижения «высокого качества перевода», а значит, предотвращению киберугроз, ориентированных на трансформацию языковой картины мира в сознании пользователя видеоигры [2].

Популяризация видеоигр и трансляция их на стриминговых сервисах определяет необходимость выработки практических и теоретических знаний, применяемых в локализации видеоигр в условиях глобализации рынка цифровой индустрии, и определения стандартной структуры самого процесса локализации с учетом поведенческих и моральных аспектов.

В настоящее время, на рынке стриминга большая часть аудитории охвачена платформами Twitch и YouTube, потому что они предлагают не только трансляцию видеоигр, но и иной развлекательный контент. Стриминговые платформы завоевывают аудиторию также благодаря инструментальным возможностям для общения пользователей с популярными стримерами в режиме реального времени. Однако настораживает низкая культура создателей контента, стримеров, имеющих миллионы подписчиков и фанатов.

Риски и киберугрозы в индустрии видеоигр и стриминга (Таблица 1)

Виды возможных киберугроз	Описание
Привязка игроков к аккаунтам в соцсетях	В мобильных играх необходима обязательная привязка игроков к аккаунтам в соцсетях, и это является источником информации о профилях пользователей не только для владельцев сервисов, но и злоумышленников.
Вредоносное программное обеспечение	Когда пользователи через неофициальные платформы загружают стриминговые приложения, то это становится причиной загрузки вредоносного программного обеспечения.
Нарушения авторских прав	Часто на стриминговых платформах наблюдается транслирование контента без согласия авторов.
Дезинформация с использованием инструментов создания контента	Игровые платформы и стриминговые сервисы являются для злоумышленников удобным ресурсом для создания и распространения дезинформации.
Язык цифрового контента как средство пропаганды	Язык для создания цифрового контента видеоигр и стримов отличается наличием различных способов пропаганды и (или) вербовки игроков и пользователей.
Риски правовой неопределенности в области видеоигр	Отсутствие четких правовых установок для разработчиков видеоигр – это причина наличия киберугроз в игровом пространстве для всех его участников.

Несмотря на то, что индустрия видеоигр и стриминга развивается в сторону улучшения технических условий для стримеров и их аудитории, она содержит множество скрытых опасностей и киберугроз. Рассмотрим основные риски и киберугрозы, сопутствующие развитию индустрии видеоигр и стриминга, приведенные в Таблице 1 (см. выше).

В связи с обязательной привязкой игроков к аккаунтам в соцсетях на большинстве современных игровых платформ и стриминговых сервисах профилирование пользователей видеоигр и стриминговых платформ через логи во время игрового процесса или в процессе коммуникации позволяет агрегаторам платформенных решений получать огромное количество данных, которые в дальнейшем используются для улучшения содержания продукта и его функциональных возможностей. Однако доступ к данным могут получить злоумышленники и использовать их для влияния на аудиторию.

Различные виды вредоносного и нежелательного программного обеспечения, а также фишинговые страницы и поддельные веб-сайты часто маскируются под известные стриминговые платформы. При обращении к таким ресурсам для загрузки стриминговых приложений пользователи часто сталкиваются со шпионскими программами и назойливыми рекламными программами.

На стриминговых платформах часто отмечаются случаи нарушения авторских прав при трансляции видеоигр и(или) создания на их основе иного цифрового контента. Необходимы более строгие меры контроля и ограничений, чтобы защитить права интеллектуальной собственности.

Переводчики, занимающиеся локализацией видеоигр, должны знать об основных видах киберугроз при использовании видеоигр и стриминговых сервисов. При этом наиболее важным является понимание переводчиком содержательной составляющей контента, которая должна быть ориентирована на предотвращение создания и распространения дезинформации в киберпространстве, недопущение и(или) нейтрализацию манипулятивных приемов и средств, способов пропаганды и вербовки пользователей видеоигр и стримов.

Повышению рисков и киберугроз в игровом киберпространстве для всех его участников способствует отсутствие нормативно-правовых установок для разработчиков видеоигр.

Кибербезопасность в сфере переводческой деятельности в процессе локализации видеоигр подразумевает защиту, прежде всего, аудитории от возможных киберугроз в явном и(или) скрытом виде, оказывающих воздействие на умы.

Рассмотрим основные принципы предотвращения киберугроз в переводческой деятельности:

- Принцип минимума идентичности процедур. Этот принцип предполагает исключение общих для нескольких пользователей паролей при обращении к платформам видеоигр и(или) стриминговым сервисам и, таким образом, предотвращает возможность хакерской атаки на персональный аккаунт и несанкционированное внесение изменений в контент, созданный переводчиком.
- Принцип целостности. Информация, хранение которой осуществляется на техническом устройстве и(или) в облаке, должна быть защищена от изменений или искажений, провоцирующих при локализации видеоигр нарушение целостности и достоверности традиционных нравственных ориентиров народа страны, на язык которой осуществляется перевод.
- Принцип конфиденциальности. Доступ к результатам переводческой деятельности предоставляется заказчику, владельцу видеоигры, и(или) его представителям (издателям, маркетологам и т.д.) по правилу

«минимальной необходимой осведомленности». Другими словами, предоставляется право доступа только к той части информации, которая необходима для выполнения субъектом его служебных обязанностей в рамках проекта. Также продукт переводческой деятельности должен храниться, обрабатываться и передаваться по надежным каналам связи.

Соблюдать основные принципы предотвращения киберугроз в переводческой деятельности рекомендуется такими способами:

- использовать разные пароли при обращении к платформам и сервисам;
- вести журнал доступа к данным (логирование обращений пользователей);
- запретить передачу данных в мессенджерах, социальных сетях и т. д.;
- запретить подключения рабочего компьютера в общественную сеть;
- запретить загрузки файлов из подозрительных источников;
- установить и регулярно обновлять антивирусное программное обеспечение;
- создать защищенные каналы связи;
- запретить установку программного обеспечения с функциями захвата экрана (создания скриншотов или видео), записи аудио;
- установить запрет на несанкционированное копирование данных;
- проводить регулярно аудит безопасности персональных ИТ-систем;
- проводить регулярно анализ и фильтрацию сетевого трафика;
- ограничить доступ к камере и микрофону для установленных программ;
- использовать системы контроля переписки [3,4].

Выводы. Непрерывное совершенствование профессиональных компетенций в области кибербезопасности и соблюдение основных принципов предотвращения киберугроз в условиях интенсивно развивающегося киберпространства позволят практику-переводчику:

– во-первых, избежать ошибок в процессе локализации видеоигр, хотя при этом потребуется достаточное количество времени для проработки качественного перевода; достаточный объем контекста для лучшего понимания ситуаций, предоставляемый разработчиком видеоигры; понимание особенностей пары языков, на основе которых осуществляется перевод; понимание местных культурных особенностей, различий в менталитете того народа, на язык которого осуществляется перевод содержания продукта;

– во-вторых, создать условия для продвижения видеоигры, в том числе и на основе стриминговых сервисов, в которых будут минимизированы возможные несанкционированные или случайные изменения и(или) искажения идейной целостности контента видеоигр, то есть реализована предварительная нейтрализация возможных манипулятивных приемов и способов воздействия на аудиторию пользователей видеоигр и стримов.

Процесс локализации видеоигр является уникальным явлением в сфере переводческой деятельности в связи с привлечением различных методов адаптации текста с учетом понимания культуры страны, где производится видеоигра, и страны, на язык которой осуществляется ее локализация.

Переводчик, планирующий начать свой карьерный путь в сфере локализации видеоигр, должен быть осведомлен о возможных рисках и киберугрозах в индустрии видеоигр, знать и уметь применять способы соблюдения основных принципов предотвращения киберугроз в индустрии видеоигр.

Библиографический список:

1. Лебедева М.В., Раевская Е.Л. Особенности профессиональных компетенций переводчиков в лингвистическом вузе. Подготовка переводчиков: анализ систем и подходов в странах мира: Сборник тезисов Второй Международной научной конференции. НГЛУ, 2022. С. 47-49
2. Сдобников В. В. Новые тенденции в переводоведении / В. В. Сдобников // Казанский вестник молодых ученых Педагогические науки. Перевод в XXI веке: вызовы эпохи и перспективы развития. – 2018. – том 2 № 4 (7) – С. 72-79.
3. О дополнительных мерах по обеспечению информационной безопасности Российской Федерации: Указ Президента Российской Федерации от 01.05.2022 № 250 – URL: http://www.kremlin.ru/acts/bank/47796 (дата обращения: 22.02.2024)
4. Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента Российской Федерации от 05.12.2016 № 646 – URL: http://www.kremlin.ru/acts/bank/41460 (дата обращения: 22.02.2024)
5. О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации: Указ Президента Российской Федерации от 30.03.2022 № 166 – URL: http://www.kremlin.ru/acts/bank/47688 (дата обращения: 22.02.2024)

МЕДИАЖУРНАЛИСТИКА В ШКОЛЬНЫХ И МОЛОДЕЖНЫХ ПРЕСС-ЦЕНТРАХ КАК РЕСУРС РАЗВИТИЯ МЕДИА- И ЦИФРОВОЙ ГРАМОТНОСТИ

Автор: **Лескина Ирина Николаевна**
к.п.н., доцент, Нижегородский институт развития образования,

Автор: **Канянина Татьяна Ивановна**
к.п.н., доцент, Нижегородский институт развития образования

Аннотация. В настоящей статье рассмотрены особенности развития школьной и молодежной журналистики как ресурса формирования и развития медиа- и цифровой грамотности детей и молодежи.

Раскрыты основные подходы к организации единого безопасного образовательного медиапространства для школьных и молодежных СМИ и предложена модель реализации преемственности между наставниками и молодежью в свете актуализации вопросов грамотного применения современных медиатехнологий в цифровом обществе.

Представлен региональный опыт в области медиаобразования на основе кооперации усилий наставников и молодежи в вопросах информационного и методического сопровождения деятельности школьных и молодежных пресс-центров.

Ключевые слова: медиа- и цифровая грамотность, медиатехнологии, наставничество, школьная и молодежная медиажурналистика.

Школьная и молодежная медиажурналистика сегодня представляет собой важнейший ресурс, ориентированный на формирование и укрепление гражданской позиции детей и молодежи посредством их осознанного участия в медиасреде и медиакультуре [1].

Тенденция массового использования возможностей социальных сетей, которые привлекают пользователей не только разнообразием готового контента, но и непрерывно совершенствующимися инструментальными возможностями для его создания:

- с одной стороны, оказала положительное влияние на развитие медийной школьной и молодежной журналистики: улучшилось качество продуктов пресс-центров и расширился их перечень – кроме привычных печатных изданий, телевидения, радио, появилась и активно развивается мобильная журналистика;
- с другой стороны, стала причиной проблемы стихийного развития «блогерства» в детской и молодежной среде, что, в свою очередь, повлияло на увеличение некачественного контента в информационном пространстве, и, что особенно важно, продвижения молодыми блогерами идей, которые искажают традиционные национальные нравственные ценности.

Рост числа популярных блогеров, у которых подписчиков больше, чем у профессиональных журналистов, разнообразие так называемых «лиг», «холдингов», «медиашкол», отличающихся кратковременным сроком действия и(или) узкой направленностью в сфере журналистики, зачастую реализующих «непрозрачные» цели и задачи и не имеющие компетентного кадрового ресурса – все это актуализирует вопрос создания в России единого образовательного медиапространства для школьных и молодежных СМИ и единой системы сопровождения формирования и развития медиа- и цифровой грамотности детей и молодежи.

Гипотеза нашего исследования состоит в том, что эффективное решение обозначенной проблемы возможно только на основе объединения усилий в области медиаобразования представителей сферы образования, профессиональных СМИ и общественных организаций, что позволит успешно решать вопросы, направленные на:

- создание условий для защиты детей и молодежи от внешнего деструктивного информационно-психологического воздействия, пресечение деятельности, направленной на разрушение традиционных национальных ценностей;
- реализацию профориентационной работы среди детей и молодежи в области грамотного использования современных медиатехнологий.

Положительный опыт наставничества представителей сферы образования, профессиональных средств массовой информации и общественных организаций по сопровождению развития школьных и молодежных СМИ сложился в Нижегородской области, где действует «Сообщество школьных и молодежных СМИ» (https://vk.com/public173379003).

Основная цель организации Сообщества: формирование и развитие единого образовательного медиапространства, способствующего формированию гражданской позиции и укреплению патриотизма всех его участников (взрослых, детей и молодежи) на основе выявления и тиражирования лучших практик медиаобразования в работе пресс-центров образовательных организаций региона.

По инициативе ГБОУ ДПО «Нижегородский институт развития образования» (кафедры информационных технологий) в 2008 году стартовал инновационный проект «Школьные СМИ Нижегородской области», объединивший школьные пресс-центры Нижегородской области [2].

К 2024 году масштабы проекта расширились: участниками Сообщества являются представители пресс-центров школ, учреждений дополнительного образования детей и среднего профессионального образования. Более 90% муниципалитетов и городских округов региона представлены в объединении школьных и молодежных СМИ.

Основные партнеры и наставники «Сообщества школьных и молодежных СМИ Нижегородской области»: Союз журналистов Нижегородской области, Институт филологии и журналистики ННГУ им. Н.И. Лобачевского, Нижегородский областной информационный центр, Штаб общественной поддержки по Нижегородской области,

Нижегородская государственная областная телерадиокомпания «ННТВ», Государственная телевизионная и радиовещательная компания «Нижний Новгород», муниципальные редакционно-издательские радиовещательные центры.

Основные направления деятельности Сообщества:

- для педагогических работников: образовательные семинары, практические мастерские, пресс-конференции, интенсивы, курсы;
- для обучающихся: практические мастер-классы, тематические смены в лагере, журналистские проекты, экскурсии, конкурсы, фестивали [3].

В рамках ежегодного Межрегионального фестиваля школьных и молодежных медиацентров (в 2024 году состоится 17 фестиваль) принимают участие представители пресс-центров Алтайской, Волгоградской, Ивановской, Калининградской, Кировской, Ростовской, Чувашской, Ярославской областей, а также с Республикой Башкортостан и Удмуртской Республикой, с которыми сотрудничает Сообщество школьных и молодежных СМИ Нижегородской области.

Регулярно проводится межрегиональная мастерская в формате обучающих вебинаров, интерактивных мастер-классов, где в роли «мастеров» выступают лучшие коллективы пресс-центров образовательных организаций субъектов Российской Федерации.

Нижегородский институт развития образования с 2008 года реализует программы дополнительного профессионального образования для педагогических работников по вопросам медиаобразования. В 2024 году кафедрой информатики и информационных технологий реализуется программа «Современные медиатехнологии в работе пресс-центра образовательной организации» (72 часа). Обучение проводят научные работники и профессиональные журналисты, специалисты в области информационной безопасности и эксперты по вопросам медиаобразования.

Координационным органом Сообщества по вопросам сопровождения развития школьных и молодежных СМИ Нижегородской области является Совет, действующий с 2008 года, в состав которого входят руководители пресс-центров, опорных площадок объединения. Инициативная группа Совета при поддержке наставников и партнеров Сообщества реализует сопровождение полного цикла каждого мероприятия: от идеи до обработки результатов реализации [4].

В коллективах пресс-центров поддерживается преемственность между наставниками и молодежью, что позволяет не только сохранять школьные и молодежные СМИ, но и осваивать новые направления журналистики в условиях непрерывного развития современных медиатехнологий. Так постепенно появился Молодежный Совет Сообщества, участниками которого являются студенты и молодые специалисты в сфере образования, журналистики и коммуникаций.

Молодежный Совет – это инициативная творческая группа медиапедагогов, журналистов и студентов, неравнодушных к вопросам сохранения национальной культуры, традиций, языка, популяризирующих вопросы грамотного использования современных медиатехнологий и основы кибергигиены в цифровом обществе.

Одно из важных направлений деятельности Молодежного Совета при поддержке наставников и партнеров «Сообщества школьных и молодежных СМИ Нижегородской области» является информационное и методическое сопровождение мероприятий, ориентированных на формирование и развитие медиа- и цифровой грамотности взрослых, детей и молодежи.

С 2023 года Сообществом реализуется проект «Школьные и молодежные СМИ – территория безопасного медиапространства», в рамках которого регулярно проводятся практические мастерские и семинары по вопросам грамотного применения возможностей социальных сетей в работе пресс-центра. При этом особое внимание уделяется вопросам соблюдения цифровой этики, безопасной работы в социальных сетях и освоению правилам кибергигиены.

В 2023-2024 учебном году состоялся региональный Конкурс школьных и молодежных СМИ, в рамках которого была объявлена новая номинация: «Школьные и молодежные СМИ о кибергигиене в детской и молодежной среде». В качестве экспертов материалов пресс-центров выступили профессионалы в области кибербезопасности. Лучшие работы участников Конкурса транслируются в ВК ресурсе Сообщества: https://vk.com/public173379003.

За период с апреля 2023 по февраль 2024 года Молодежным Советом проведено 11 региональных практических мастерских для школьников, студентов и педагогических работников, на которых были представлены такие вопросы, как: принципы ведения социальных сетей и их визуальное наполнение, особенности работы пресс-центра в соцсетях, создание контента от идеи до публикации, визуализация контента и создание личного бренда, основы безопасной работы в социальных сетях.

В рамках проекта «Школьные и молодежные СМИ – территория безопасного медиапространства» благодаря тесному сотрудничеству наставников и молодежи трансляция опыта организации и проведения практических мастерских, способствующих формированию и развитию медиа- и цифровой грамотности участников пресс-центров, реализуется на основе «каскадной модели»: региональная площадка – муниципальная опорная площадка – пресс-центр образовательной организации. Таким образом, значительно увеличился охват руководителей пресс-центров и начинающих журналистов направлениями медиаобразования, ориентированными на грамотное применение возможностей соцсетей и цифровых сервисов.

Основным результатом кооперации ресурсов и действий наставников и молодежи в направлениях, ориентированных на формирование и развитие медиа- и цифровой грамотности участников «Сообщества школьных и молодежных СМИ Нижегородской области», является создание социальных механизмов, обеспечивающих процесс формирования субъектности личности, способной не только потреблять, но и создавать необходимую информацию, воплощать ее в качественный продукт медиакультуры или действие, способствующие достижению «экологии» средств массовой информации.

Выводы. Создание регионального объединения пресс-центров образовательных организаций и тиражирование лучших практик медиаобразования через кооперацию усилий наставников и молодежи – это основной фактор развития единого безопасного образовательного медиапространства для школьных и молодежных СМИ, а значит, и для защиты детей и молодежи от внешнего деструктивного информационно-психологического воздействия.

В свою очередь, развитие системы информационного и методического сопровождения совершенствования медиа- и цифровой грамотности участников пресс-центров (педагогических работников и обучающихся) и привлечение в качестве наставников высококвалифицированных специалистов научных и общественных организаций, информационных, редакционно-издательских и телевизионных центров – это важная составляющая развития соответствующих компетенций юных журналистов и блогеров (взрослых и детей), а значит, улучшение качества контента медиасреды, сохранение и укрепление традиционных национальных нравственных ценностей.

Современная цифровая эпоха предоставляет человеку много возможностей для собственного развития, но при этом заключает в себе угрозу манипулирования разумом не только отдельной личности, но и общества в целом. Это обуславливает значимость развития школьной и молодежной медиажурналистики как стратегического ресурса, способствующего «выращиванию человеческого капитала будущего непосредственно в процессе построения этого будущего» [3].

Библиографический список:

1. Журналистика и медиаобразование в XXI веке / под редакцией А. П. Короченского. – Белгород: изд-во Белгородского гос. ун-та. – 2006. – С. 368.

2. Канянина. Современные медиатехнологии в работе школьного пресс-центра: учебно-методическое пособие / Т. И. Канянина, В. Б. Клепиков, И. Н. Лескина: // под общей редакцией И. Н. Лескиной. – Нижний Новгород: Нижегородский институт развития образования. – 2022. – С. 130

3. Лескина, И. Н. Школьные СМИ Нижегородской области / И. Н. Лескина, Л. А. Шевцова. – Нижний Новгород: Нижегородский институт развития образования. – 2013. – С. 136

4. Шевцова, Л. А. Школьные СМИ как ресурс предпрофессиональной подготовки журналистских кадров / Л. А. Шевцова, И. Н. Лескина // Вестник Нижегородского университета имени Н. И. Лобачевского. – 2014. – № 2. Часть 2. – С. 502—504.

NAVIGATING INTERNET FRAGMENTATION: STRATEGIES FOR UPHOLDING TECHNOLOGICAL SOVEREIGNTY

Author: **Miloš Jovanović**
PhD, Professor at the Belgrade Metropolitan University and University of Kragujevac

Keywords: Internet fragmentation, digital environment, technological sovereignty, national defense.

Introduction

In the interconnected world, the concept of internet fragmentation has become a significant issue for countries globally. Internet fragmentation involves dividing the Internet into networks due to various factors like technical restrictions, political motives, and regulatory differences. This situation has implications for the unity of the environment and raises important concerns about technological independence and national defense.

Understanding Internet Fragmentation

Internet fragmentation is when the global internet is separated into networks due to factors such as political or economic influences (Shannon et al., 2002). This division can create difficulties in maintaining an interconnected environment that affects information flow and services across various regions (Pohle & Thiel 2020). The reasons behind internet fragmentation are diverse. Can arise from factors, like government intervention, technical constraints, and varying regulatory structures. When governments interfere with the aspects of the internet it can lead to differences, in how governance is approached causing fragmentation issues. Moreover, the absence of an agenda for managing the internet can worsen fragmentation problems creating difficulties in maintaining a unified online environment (Broeders, 2016).

Impact of Disconnected Networks on Independence

The repercussions of disconnected networks on independence can be significant as they affect a nation's control over its digital infrastructure and data movements. Fragmentation may obstruct efforts to establish an approach to internet governance potentially resulting in disputes over data control and cybersecurity measures. Furthermore, fragmented networks may impede the exchange of information and services impacting a country's self-reliance on technology and its ability to harness tools for economic and social progress (Pohle & Thiel 2020). To protect independence countries can adopt measures like strengthening cybersecurity protocols promoting digital literacy, among their populace nurturing local technological advancement, and advocating for policies that keep data within national borders. By investing in infrastructure improving frameworks and supporting local tech industries nations can boost their authority, over digital technologies and data flows safeguarding their technological independence in an increasingly interconnected world (Edelman & Schwarz 2011).

Policy Frameworks for Addressing Internet Fragmentation

Dealing with internet fragmentation necessitates the creation of policy frameworks that encourage collaboration, standardization of protocols, and adherence to common governance principles. By embracing approaches like the NEW IP protocol, aimed at enhancing address allocation efficiency and addressing fragmentation challenges countries can strive for an interoperable internet environment (Chen et al., 2020). These policy frameworks should emphasize cooperation among stakeholders and alignment of strategies. Safeguarding digital rights to mitigate the adverse effects of internet fragmentation on technological sovereignty.

Enhancing National Digital Infrastructures: Investments and Innovations

Investments in infrastructures play a vital role, in nurturing technological independence. By dedicating resources to developing networks nations can bolster their technological capabilities enhance connectivity and foster innovation. In this age advancements, in technology and investments in research and development play a role in helping countries establish strong and secure digital infrastructures that drive economic progress and technological self-reliance (Martin & Matlay 2003). To address cybersecurity risks in networks a comprehensive strategy is needed. This includes implementing encryption methods improving threat intelligence capabilities and promoting collaboration on cyber defense. Through initiatives like cybersecurity awareness campaigns, effective incident response protocols and enhanced information sharing among stakeholders' nations can enhance their resilience against cyber threats within environments (Chin & Li 2021). Furthermore, taking steps such as security assessments and compliance checks can help reduce risks and protect technological sovereignty amidst evolving cyber challenges.

Promoting International Collaboration

In order to address the problem of internet fragmentation and maintain independence, partnerships are crucial. By coordinating efforts, exchanging best practices, and collaborating to set standards, nations, international organizations, and stakeholders can collaborate to build a more integrated digital ecosystem. Collaborative organizations that foster communication, encourage cooperation, and align rules are essential to lessen the effects of downed networks on Internet management (Lubell et al., 2010). In order to address the causes of internet fragmentation and establish a cohesive digital ecosystem, different parties must collaborate. Together, governments can endeavor to create frameworks for governance, enhance interoperability, and foster international confidence in order to meet the problems presented by dispersed networks. These initiatives aim at enhancing collaboration upholding rights and protecting technological independence in an increasingly interconnected world (Chin & Li 2021).

Initiatives for Interoperability Standards and Protocols

To ensure communication and connectivity across digital networks, collaborative projects that concentrate on establishing standards and protocols for interoperability are crucial. Nations can enhance interoperability, simplify data sharing, and promote a more integrated digital environment by pursuing efforts to develop technological standards (Lubell et al., 2010). By bridging the gaps across systems, technologies, and networks, these projects hope to improve information and service sharing's efficiency and compatibility.

Building Partnerships for Collaborative Efforts

Building partnerships for collaborative efforts involves creating alliances among governments, international organizations, and private sector entities to tackle issues related to internet division and technological independence. By nurturing relationships countries can combine resources, exchange knowledge, and coordinate actions to address division boost cybersecurity measures, and uphold rights. These partnerships facilitate efforts, in developing shared strategies advocating practices and creating a more unified and secure digital environment that protects technological independence globally (Basupi et al., 2019).

Strengthening Cybersecurity Measures and Resilience

In fragmented digital environments, strengthening cybersecurity measures and resilience against cyber threats requires a diversified approach. Protecting data in digital systems requires the use of encryption techniques, such as sophisticated encryption algorithms and updated cryptographic ciphers. Fortifying cybersecurity defenses requires implementing machine learning-based intrusion detection systems (IDS) and improving threat intelligence capabilities through ongoing investment and innovation (Shobarani, 2023). Stakeholder information exchange is essential to improving cybersecurity procedures. Collective resilience against cyber threats can be greatly increased by establishing public-private partnerships

between industry and governmental entities and encouraging the sharing of cyber-threat information through game-theoretic methodologies. Furthermore, encouraging information sharing via rational procedures and decision-theoretic methods might promote proactive threat mitigation and a collaborative culture (Hsu et al., 2021). Protocols for incident response are essential for lessening the effects of cyberattacks. The effectiveness and agility of response efforts can be improved by creating strong incident response strategies, which can include quick detection methods for ransomware detection, such as file entropy analysis, and using blockchain platforms to manage cybersecurity certification and information (Neisse et al., 2020). Innovative tactics to strengthen cybersecurity postures include investigating how quantum computing might improve encryption techniques and implementing self-healing mechanisms to withstand ransomware attacks. Organizations may strengthen their cybersecurity defenses and resilience in the face of changing cyber threats within complex digital ecosystems by combining encryption techniques, threat intelligence capabilities, incident response mechanisms, and encouraging information sharing among stakeholders.

Fostering Diplomatic Relations and Multilateral Cooperation

To address internet fragmentation and preserve technological sovereignty, it is imperative to promote diplomatic connections and global cooperation. To foster collaboration, exchange best practices, and create shared policies for managing fractured networks and preserving digital independence, nations might form alliances, hold diplomatic discussions, and take part in international forums. To address cybersecurity issues and promote cyber stability, multilateral institutions and international cooperation are essential. According to Yeo et al. (2016), state players need to cooperate together to create a multilateral, continuous network that ensures collective cybersecurity and protects the cyber commons. A global legislative framework for cybersecurity collaboration is something that the world community is interested in creating (Aanelyan & Gulyaeva, 2020). Furthermore, such multilateral projects can learn from the collaboration of the Visegrad Four nations under the Central European Cyber Security Platform. Navigating the complexity of international relations with regard to cybersecurity requires diplomatic initiatives. Geopolitical tensions and competing national interests hinder the success of state-driven diplomacy. The relevance of inter-Arab and global cooperation in cybersecurity is highlighted by the research of Arab countries' cooperation in digital security within multilateral and bilateral frameworks (Valiakhmetova & Tsukanov, 2022). Furthermore, Japan's strategies for international cybersecurity cooperation emphasize the value of multilateral efforts in combating cyberthreats.

Conclusion

In an interconnected world, maintaining technical sovereignty and guaranteeing national defense present formidable hurdles when navigating the fragmentation of the internet. Political interference, technological limitations, and regulatory differences are some of the factors that have caused the internet to fragment into disparate networks, endangering the unity of the digital environment and undermining national control over digital infrastructure and data movements. Strategies centered on preserving independence and fostering international cooperation are crucial for addressing these issues. Within fragmented digital ecosystems, investments in cybersecurity, innovation, and digital infrastructure are essential for boosting technological capabilities and resistance against cyber-attacks. To combat internet fragmentation and protect digital rights, policy frameworks that promote cooperation, standardization of protocols, and adherence to shared governance principles are required. Furthermore, in order to encourage cooperation, share best practices, and develop common policies for managing broken networks, it is imperative to cultivate diplomatic connections and multilateral cooperation. Nations can cooperate to manage the difficulties of internet fragmentation and maintain technological sovereignty on a worldwide basis by building alliances, taking part in international forums, and launching diplomatic initiatives. To effectively address the difficulties created by internet fragmentation, a coordinated effort involving stakeholders from governments, international organizations, and the commercial sector is required. Nations may avert the negative consequences of disjointed networks, maintain digital independence, and guarantee a safe and cohesive digital environment going forward by implementing all-encompassing policies and encouraging cooperation.

References:

1. Basupi, L., Dougill, A., & Quinn, C. (2019). Institutional challenges in pastoral landscape management: towards sustainable land management in Ngamiland, Botswana. Land Degradation and Development, 30(7), 839-851. https://doi.org/10.1002/ldr.3271

2. Broeders, D. (2016). The public core of the internet: an international agenda for internet governance. https://doi.org/10.26530/oapen_610631

3. Chen, Z., Wang, C., Li, G., Lou, Z., Jiang, S., & Galis, A. (2020). New IP framework and protocol for future applications. https://doi.org/10.1109/noms47738.2020.9110352

4. Chin, Y. and Li, K. (2021). Sovereignty in the cyberspace: contestation of concepts and policies. Aoir Selected Papers of Internet Research. https://doi.org/10.5210/spir.v2021i0.12153

5. Edelman, B. and Schwarz, M. (2011). Pricing and efficiency in the market for IP addresses. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.1934217

6. Lubell, M., Henry, A., & McCoy, M. (2010). Collaborative institutions in an ecology of games. American Journal of Political Science, 54(2), 287-300. https://doi.org/10.1111/j.1540-5907.2010.00431.x

7. Lubell, M., Henry, A., & McCoy, M. (2010). Collaborative institutions in an ecology of games. American Journal of Political Science, 54(2), 287-300. https://doi.org/10.1111/j.1540-5907.2010.00431.x

8. Martin, L. and Matlay, H. (2003). Innovative use of the internet in established small firms: the impact of knowledge management and organizational learning in accessing new opportunities. Qualitative Market Research an International Journal, 6(1), 18-26. https://doi.org/10.1108/13522750310457348

9. Pohle, J. and Thiel, T. (2020). Digital sovereignty. Internet Policy Review, 9(4). https://doi.org/10.14763/2020.4.1532

10. Shannon, C., Moore, D., & Claffy, k. (2002). Beyond folklore: observations on fragmented traffic. Ieee/Acm Transactions on Networking, 10(6), 709-720. https://doi.org/10.1109/tnet.2002.805028

11. Shobarani, R. (2023). Securing the future., 383-402. https://doi.org/10.4018/978-1-6684-9317-5.ch019

12. Neisse, R., Hernandez-Ramos, J., Matheu, S., Baldini, G., & Skarmeta, A. (2019). Toward a blockchain-based platform to manage cybersecurity certification of IoT devices. https://doi.org/10.1109/cscn.2019.8931384

13. Hsu, C., Yang, C., Cheng, H., Setiasabda, P., & Leu, J. (2021). Enhancing file entropy analysis to improve machine learning detection rate of ransomware. Ieee Access, 9, 138345-138351. https://doi.org/10.1109/access.2021.3114148

14. Yeo, S., Birch, A., & Bengtsson, H. (2016). The role of state actors in cybersecurity., 217-246. https://doi.org/10.4018/978-1-4666-9661-7.ch013

15. Valiakhmetova, G. and Tsukanov, L. (2022). Digital challenge for the Arab world: integration or differentiation factor? Vestnik RUDN International Relations, 22(2), 303-319. https://doi.org/10.22363/2313-0660-2022-22-2-303-319

16. Danelyan, A. and Gulyaeva, E. (2020). International legal aspects of cybersecurity. Moscow Journal of International Law, (1), 44-53. https://doi.org/10.24833/0869-0049-2020-1-44-53

TECHNOLOGICAL SOVEREIGNTY IN A MULTIPOLAR WORLD: NAVIGATING THE ROLE OF ARTIFICIAL INTELLIGENCE

Author: Stefan Jančić
Master's student, University of Belgrade School of Electrical Engineering and BScEECS, University of Defense Military Academy

Keywords: Artificial Intelligence, Technological Sovereignty, National development, Foreign Technology

The Evolving Landscape of Technological Sovereignty

The term «technological sovereignty», in basic terms, refers to a state's ability to use technology and technological knowledge in ways that are deemed appropriate, proper, and preferable. Over the past decades, digitalization and worldwide networking have led to an IT-technological upheaval that goes hand in hand with a change in the framework conditions for state action. The classic concept of sovereignty-as every politically relevant unit, the state is free from external intervention and enjoys absolute, sole, and indivisible power is put to the test in a digital world. Decisions in the analogue world increasingly depend on digital processes and technologies. Due to high complexity, technical opacity, networking, and dependency on foreign IT technology, it is expected that state and administrative action will increasingly be influenced, channeled, and potentially infringeable. This is where the term «technological sovereignty» comes into play: States are losing control over digital key technologies that shape and control the digital everyday life of the people, and solutions are often provided by US companies (Uber, Amazon, Google, Facebook) and frequently from China (Huawei, Inspur, Tencent). This is seen as a challenge for Europe to assert itself in the «global digital competition» (Sadowski, 2020). It is important to understand that the term «technological sovereignty» cannot merely be equated with claims to politicians or individual countries for technical independence or freedom from foreign IT technology (Iivari et al.2020). Rather, it is decisive for the term that it's not just about the technical functionalities of the digital infrastructure, even though these do form the base. True technological sovereignty can only become effective when technologies are linked to one's own value-justice understanding, people's concrete needs of a digital society, and longer-term development goals (Borodina et al., 2023). The term therefore describes not only a technical-political claim to shaping the digital world but also an ethical mission for a future worth living in a digital society.

Challenges of Technological Dependence

One of the main challenges in this growing ecological debate is the over-reliance that many societies have on other countries or companies for certain technologies. This is particularly true in the medical sector, where artificial intelligence and machine learning are beginning to be employed more and more for disease diagnosis and treatment selection (Xu et al.2021). In November 2018, the first ever medical facility powered exclusively by artificial intelligence was opened by the power company NVIDIA in the US (Chen & Decary, 2020). This represents a significant step in the incorporation of artificial intelligence into everyday medical practices and signals the direction that we can expect the field to take in the future. However, if the United States company NVIDIA were to ever withdraw support, important medical services in spaces such as the Winship Cancer Institute in Atlanta would be greatly compromised. Professor Andrew Eder, from the School of Health Sciences, has highlighted the potential seriousness of a situation such as this. «In such a situation, it is likely that both new and existing patients wouldn't be able to access the standard of care that they have a right to expect...a patient's condition may deteriorate and they won't be able to benefit from the many lives prolonging as well as some potentially life-saving interventions,» he said (Lin & Alvarez, 2021). But the issue isn't limited to the hardware and software of medical machinery. Data analysis and management systems are a huge factor in the technological

independence of one's own country and these are often outsourced to private companies. An article written for Nature Biotechnology by a number of researchers from institutions such as Harvard and MIT expressed concern over such systems in the context of DNA data storage. This is a method of digital data storage founded upon the principles of data reading and writing to DNA. The article calls for the need to develop open-source data standards and objective, reproducible testing systems. These researchers, despite being from the United States, have chosen to publish their work surrounding technological sovereignty in a European biology journal nature.com.

Technological Sovereignty Concerns in Case Studies

This sort of model perceives that to address worries about national self-rule and innovation, we need government and foundation-based reactions, working connected at the hip with scholastic freedoms and gathering yet in addition all the more extensively with the business and social areas (Wagner et al.2020). By and by, in the event that you take a gander at certain nations, for instance, Germany, restrictive credits on the Internet there exclusively in German and Spain have received an alternate strategy where conditions are forced upon stages like Facebook, restrictions on the capacity to run and focused on promoting (Rochefort, 2020). These are instances of methodologies looking to keep up social and social uprightness within the advanced circle and to test the sort of all inclusive, prominent commercialization that we find in stages based via online media. These are approaches which have been contended to be endeavors to epitomize a specific thought of public innovation sovereignty, a thought that worries about the conceivable impact of external innovation organizations and about keeping up at any rate a type of administrative self-governance (De Blasio & Selva, 2021).

This model mirrors the thought of innovative power on local self-rule: the way that the utilization of AI and information instruments by one state or a political development might straightforwardly influence the opportunities, equilibrium, and protection. The traditionalists at the Heritage Foundation and comparative associations are currently advancing an administration housed arrangement of University's either a self-governing focus or inside an innovation and media organization. This would offer subsidizing and mastery to build political proficiency and help come up and checked the utilization of man-made brainpower in political settings (Dwivedi et al.2021).
In the most recent American presidential political race, much was expounded on the effect of social media, particularly the focused-on publicizing and the utilization of counterfeit insight in focusing on electors and endeavoring to impact casting a ballot designs (Schippers, 2020). This has gotten one of the principle worries in how synthetic insight information examination was utilized in the race and in future races and whether there ought to be greater administration or oversight of how such advancements are utilized. (Assibong et al.2020).

National Approaches to Developing Indigenous Technological Capabilities

Traditionally, the majority of the indigenous firms in the technology-intensive sectors and services are small and medium-sized. The technology policy of developing countries today is dominated by the idea of catching up with the advanced countries. Different from the catching-up approaches, which emphasize the technology import, the indigenous innovation approach focuses on developing the technology capacity and technological capability of the enterprises and institutions through enhancing endogenous linkages between the new knowledge and economic value creation (Baark, 2021). Indigenous innovation integrates the efforts of developing technology capacity and promoting the endogenous transition from learning and imitation to original innovation. However, it often gives rise to debates over international technology transfer and trade (Baark et al., 2021). In the modern knowledge-based economy, there is a general consensus about the key role of technology, particularly the development of indigenous technological innovation in national development. These concepts are reflected in the policy documents and official discourses from many countries. According to a recent report from the World Intellectual Property Organization, technology plans have multiple objectives including developing human resource, improving the effectiveness of research activities, strengthening the

technology transfer, and increasing local capability in invention and innovation through intellectual property rights. Such kind of long-term strategy could be recognized as a particular national system of innovations in the sense that the domestic institutions and organizations are more emphasized in enhancing the indigenous learning capacity and economic innovation through science and technology. This kind of technology strategy has also been introduced and adopted by many developing countries, particularly in East and Southeast Asia, which have been eager to promote technological innovation in the emerging dynamic economic and technological environment. For example, as one part of the national medium- to long-term technology innovation programs, the Chinese government has adopted the indigenous innovation products accreditation measures since 2007, aiming to encourage and enhance the protection of indigenous intellectual property as well as to increase the marketability of domestic products.

The accreditation measures have clearly proposed the fundamental principles of indigenous innovation. The development focusses on increasing the market share of the indigenous products in China, enhancing international competitiveness of China's technology and products, freeing China from the unreasonable and discriminatory practices related to the technology import and market access, and safeguarding China from being the low-end manufacturing base. On the other hand, the measures have also proposed the criteria for accrediting an invention, emphasizing the leading role of the inventor and clearly differentiating the invention from the service. Most importantly, the measures have included the IP creation into the evaluation of behavior of the technology. These essential ideas would have a great influence on the national patent and IP laws as well as the future technology policies in China. Based on the official discourses, the concept of indigenous innovation has been deeply embedded in the Chinese technological and social developmental plan. The current technology policy of China is grand and ambitious; nevertheless, going through different stages of shifting from learning to leapfrogging and from investment-driven to innovation-driven, although it is suggested that the requirement of openness should be critically integrated with the demand for innovation and creation in the process (Pusceddu, 2020).

Conclusion

When negotiating the role of artificial intelligence (AI) in a multipolar world, the idea of technological sovereignty is crucial. As global dynamics are shaped by technology breakthroughs, states encounter difficulties in retaining control over digital infrastructure and data movements. The dynamic terrain of technical sovereignty underscores the imperative for nations to establish authority over pivotal technologies and curtail reliance on external agents. Technological dependence presents issues in a number of areas, such as healthcare, where reliance on foreign technology jeopardizes national security and sovereignty. Case studies highlight the significance of national strategies for fostering the development of domestic technological capabilities and the necessity of laws that uphold intellectual property rights and encourage innovation. Governments must prioritize funding for research and development, encourage cooperation between the public and private sectors, and implement laws that uphold the interests of the country while fostering innovation in order to address these issues. In an increasingly interconnected world, countries can preserve their technological sovereignty and assure national prosperity by strengthening their own technological capacities and decreasing their need on foreign corporations. In addition, legislative frameworks need to be modified to take into account the sociological and ethical ramifications of AI technology. Establishing norms and procedures that support ethical AI development and application while defending individual liberties and rights requires international cooperation. Essentially, managing artificial intelligence in a multipolar world necessitates a comprehensive strategy that strikes a balance between national interests and ideals and scientific growth. By promoting indigenous innovation, fostering collaboration, and enacting appropriate regulatory measures, nations can effectively navigate the challenges and opportunities presented by AI in the pursuit of technological sovereignty and national development.

References:

1. Sadowski, J. (2020). Too smart: How digital capitalism is extracting data, controlling our lives, and taking over the world. MIT Press. DOI: 10.7551/mitpress/12240.001.0001

2. Iivari, N., Sharma, S., & Ventä-Olkkonen, L. (2020). Digital transformation of everyday life–How COVID-19 pandemic transformed the basic education of the young generation and why information management research should care?. International Journal of Information Management, 55, 102183. DOI: 10.1016/j.ijinfomgt.2020.102183

3. Borodina, M., Idrisov, H., Kapustina, D., Zhildikbayeva, A., Fedorov, A., Denisova, D., ... & Solovyanenko, N. (2023). State Regulation of Digital Technologies for Sustainable Development and Territorial Planning. International Journal of Sustainable Development & Planning, 18(5). DOI:10.18280/ijsdp.180533

4. Xu, Y., Liu, X., Cao, X., Huang, C., Liu, E., Qian, S., ... & Zhang, J. (2021). Artificial intelligence: A powerful paradigm for scientific research. The Innovation, 2(4). DOI:10.1016/j.xinn.2021.100179

5. Chen, M. & Decary, M. (2020). Artificial intelligence in healthcare: An essential guide for health leaders. Healthcare Management Forum. DOI: 10.1177/0840470419873123

6. Lin, R. Y. & Alvarez, J. B. (2021). Industry perspectives and commercial opportunities of artificial intelligence in medicine. Artificial Intelligence in Medicine. DOI: 10.1016/B978-0-12-821259-2.00024-7

7. Wagner, B., Rozgonyi, K., Sekwenz, M. T., Cobbe, J., & Singh, J. (2020, January). Regulating transparency? Facebook, twitter and the German network enforcement act. Proceedings of the 2020 conference on fairness, accountability, and transparency, 261-271. DOI: 10.1145/3351095.3372856

8. Rochefort, A. (2020). Regulating social media platforms: A comparative policy analysis. Communication Law and Policy. DOI: 10.1080/10811680.2020.1735194

9. De Blasio, E. & Selva, D. (2021). Who is responsible for disinformation? European approaches to social platforms' accountability in the post-truth era. American Behavioral Scientist. DOI:10.1177/0002764221989784

10. Dwivedi, Y. K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., ... & Williams, M.D. (2021). Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. International Journal of Information Management, 57, 101994. DOI: 10.1016/j.ijinfomgt.2019.08.002

11. Assibong, P. A., Wogu, I. A. P., Sholarin, M. A., Misra, S., Damasevičius, R., & Sharma, N. (2020). The politics of artificial intelligence behavior and human rights violation issues in the 2016 US presidential elections: An appraisal. In Data Management, Analytics and Innovation: Proceedings of ICDMAI 2019, Volume 2, 295-309. DOI:10.1007/978-981-13-9364-8_22

12. Schippers, B. (2020). Artificial intelligence and democratic politics. Political Insight. DOI:10.1177/17816858211061791

13. Baark, E., Hofman, B., & Qian, J. (2021). Innovation and China's global emergence.nus.edu.sg ISBN: 978-981-325-148-9

14. Pusceddu, P. (2020). Hic Sunt Dracones? Mapping the legal framework of China's innovation policy: Standardization and IPRs. IIC-International Review of Intellectual Property and Competition Law, 51(5), 559-593. DOI: 10.1007/s40319-020-00945-8

REVERSE SHELL DETECTION METHOD FOR VOICE OVER IP (VOIP), INTERNET CONTROL MESSAGE PROTOCOL (ICMP) BASED ON MACHINE LEARNING ALGORITHMS

Author: Enofogha Gabriel Urhukpaghogho
Faculty of Secure information technologies, Ministry of Science and Higher education of the Russian Federation, ITMO University

Keywords: Cyber threat, Intrusion Detection System (IDS), Voice Over IP (VoIP), Internet Control Message Protocol (ICMP), Machine Learning algorithms, Reverse Shell detection.

The aim of this research was to find the best possible model and the implementation for it to develop a system of machine learning algorithm for optimum security. And most importantly, reduce the false positive by searching multiple existing network IDS models that uses ML and decide on the most suitable Model that needs to be adapted to this specific research of the security threat. This was done by creating personal dataset with multiple features in the lab environment to test the newly crafted ML implementation of the ML application. This research's main approach for developing such ML application was to first try to understand the existing models as much as possible that were implemented in the cybersecurity sphere, mainly the ones that concentrate on analyzing the network protocols as it is parameter for the main model.

The machine learning algorithm that fits perfectly with the reverse shell VoIP, ICMP and other encapsulation techniques is random forest classifier with the combination of cross correlation and Fourier transform. Due to the nature of the dataset as network traffic, the solution was an analysis of intermediate signal-processing and statistics to feed the parameters of a machine learning model (Random Forest machine learning algorithm) and most importantly to find a way to fit all the data in the range of the machine learning parameter. For the proposed machine learning model (packet number, packet size, detection time) as the (x,y,z) axis. encapsulate more data into the max period of the signal in network connections as it fuses both size and time into a single parameter.

A larger simulation was also needed in a big data environment to create larger data set so the model can be put in production and test of a real-world scenario. Hence, it was decided to create a virtual environment with two virtual operating system, one is for the target machine Windows 10, and the other would be the attacker machine like kali Linux which will issue the CMD shell commands, the connection was monitored by Wireshark for generating raw PCAP files which in turn was processed using python programming language for filtering and labelling data as a supervised learning method for generating dataset which will be used to test the efficiency of the machine learning algorithms.

To provide a complete evaluation of the NB-Opcode approach, a comparison against real tools is provided by comparing three popular web shell detection tools: D-Shield, Web shell Killer, and Web Shell Detector. These three tools support PHP code upload detection. After uploading a web shell to determine the effectiveness of these three tools, we observed a lower detection rate compared with the proposed NB-Opcode approach. In addition, unlike the NB-Opcode, none of the three detection tools analyzed use the opcode sequence, which ensures that the detection of obfuscated web shells is almost impossible. The NB-Opcode-based detection method was superior to the other three detection tools.

Considering the previous ML model for processing http data, it was decided to use Fourier transform for feature extraction of the ICMP and VoIP since they rely more on frequency-based signals rather than text mining pattern recognition like TF-IDF, feeding the FT signals to Random Forest, Random forest is an easy to use machine learning tool since it is relatively straightforward to understand its' internal mechanism given the data distribution, especially when dealing with a high dimensional dataset.

For the purpose of checking the quality of the proposed solution, we first considered our own special dataset that was created in the lab environment, mainly network traffics in form of PCAP files that contain both normal benign traffics and malicious network traffic that contains the hidden reverse shell encapsulated and encoded inside regular network traffics like VoIP and ICMP to be stealthier, using automated tools like Metasploit and Empire to generate multiple-features reverse shell payload, also including our own programming for the reverse shell and encapsulate it inside network protocols such as ICMP and VoIP for the purpose of encoding the traffics to further test the effectiveness of the solution. In addition to increasing the scope of the machine learning implementation, the FIRST from first.org dataset that was provided in the 23rd European Symposium on Research in Computer Security was included. It is a collection of 4.4 GB P CAP files containing normal as well as malicious traffic. Traffic is composed from Reverse Shell shellcode connections, website defacing attacks, ransomware downloaded attack cryptolocker and a command and conquer exploit attack (C2) over SSL that takes over the victim machine. The PCAPs that contain the reverse shell connections that will be an auxiliary data to further benefits our testing of the ML efficiency were mainly included.

Fourier transform was used for feature extraction of the ICMP and VoIP and reverse shell in general since they rely more on frequency-based signals rather than text mining pattern recognition like TF-IDF. The feature extraction was done by using Wireshark to capture traffics and then combine python programming to reduce and filter the unwanted traffics, and then the relevant data are used for the purpose of Fourier transform feature extraction. This tool allowed us to encapsulate more data into the max 'period' as it fuses both size and time into a single parameter. This allowed better separation and feature importance showed that it was one of the top features.

For a data analysis tool that is expected to parse big data captures, process the data with mathematical functions such as FFT, and visually present the results, Python offers very sophisticated and efficient third-party libraries. For this work, five modules were utilized as the main source for additional functionality which includes scapy, numpy, matplotlib, pandas and scikit-learn.

The first step was to filter PCAP files that was captured by Wireshark to obtain the relevant information which helped in creating the needed dataset. ScaPy was used to manipulate and read packet, and PrettyTables was for illustration purposes to have a first look on what are we getting from a simple read operation to the PCAP files, the final tool used is a built-in module Counter for counting packets. win_kali_rs.pcap is file capture for a reverse shell between Windows and Kali Linux VM.

Next step was graphing data over time to have a better understanding of the nature of the packets. At first this might seem very easy - just create a list of timestamps and bytes and you are done. The problem is that we will have thousands of packets which are hard to view and most of them will be at or close to your max MTU (usually 1500 bytes).
It is critical to mention that FFT assumes a signal that is sampled evenly over time. Some tweaks were needed in order to aid the FFT at its' task. One attempt to overcome this issue was to manually imitate the FFT process by placing each packet in a different bucket. Bucketing the packets, as each bucket would represent a different period and the number of

packets within each bin would represent the period's magnitude. So, the next thought was to group the data into bins of a set time. This was done by using Pandas library in the code. Plotly for plotting and data visualizing, and Python Datetime module comes built into Python for managing the time.

The FFT cross correlation was calculated to fingerprint the reverse shell connection. When dealing with an SER (Send-Execute-Return) signal of a reverse shell, the max value of the cross-correlation is expected to have a high peak at some special point in time, which was used to distinguish between a reverse shell SER signal and a regular benign signal.
Now that the FFT has been extracted from the PCAP and the cross correlation has been calculated, Tshark, a great tool was used to convert PCAP file or live capture into CSV file that would be easy to load into python model for extracting further features from the PCAP and convert them to csv file to store the dataset that will be fed to the machine learning.

In order to clean the data, the raw data that was captured from Tshark and loaded with respect to the following 2 rules:

- To convert IPv4 address to be numeric (at the end it is not useful as causes overfitting), and
- To change the empty field be 0, so it is able to load into python mode.

Updated CSV file from clean data script exporting, so in add label script the identified label was added.
Last step is to train the dataset that were gathered and compare algorithms to understand feature importance. This was done by importing the necessary libraries.

Running the previous script for data training and algorithms comparison showed the random forest classifier RFC accuracy of 0.999998%.

Because cyber attacking dataset size is normal compared to real world large dataset, this caused some bias, once building for production, we are going to have opportunity to test it with huge dataset in a real-world environment, but for now the results are promising and indicate that this model has the potential to be efficient enough for deployment compared to other types of algorithms.

The result of using FFT for feature extraction with random forest classifier was promising compared to other algorithms, the accuracy is 0.999998%. However, the result is somehow biased because it needs to be tested in more progressive large real world big data environment to be absolutely sure of the results. It was concluded that the higher the value of maximum features of the dataset the more the accuracy and recall being higher as well.

The main advantages of the proposed model are that it has the ability to detect the reverse shell that was encoded in benign network traffics like Internet Control Message Protocol (ICMP) and Voice Over IP (VIOP), and produced higher accuracy and recall than the other existing methods. It was also concluded that the more features the dataset has the higher recall rate. The main shortcoming of the proposed model was that it needs a simulation in real world environment so get rid of any bias in the implementation.

A reverse shell detection method is crucial in the field of cybersecurity. By developing effective detection techniques, we can identify and mitigate the risks associated with reverse shell attacks. In summary, this study is vital for advancing cybersecurity. It contributes to improved threat detection, strengthens incident response capabilities, enhances network security, drives knowledge advancement, and fosters collaboration within the industry.

References:

1. Bongard, M. I. D. (2019). Reverse Shell via Voice (SIP, Skype): дис. – HSR Hochschule für Technik Rapperswil.
2. Katsikas, S. K. (2019). Computer Security: ESORICS 2018 International Workshops, CyberICPS 2018 and SECPRE 2018, Barcelona, Spain, September 6–7, 2018, Revised Selected Papers. – Springer, 11387.
3. Hochreiter, S. and Schmidhuber, J. (2017). Long short-term memory //Neural computation. 9 (8): 1735-1780.
4. Guo, Y., Marco-Gisbert, H. and Keir, P. (2020). Mitigating webshell attacks through machine learning techniques // Future Internet. 12(1): 12.
5. Althouse, J. B., Salusky, W. R. and Atkinson J. S. (2019). Reverse shell network intrusion detection: пат. 10135847 США.
6. Wu, Y. (2019). Session-based webshell detection using machine learning in web logs //Security and Communication Networks.
7. Pratomo, B. A., Burnap, P. and Theodorakopoulos, G. (2020). Blatta: Early exploit detection on network traffic with recurrent neural networks //Security and Communication Networks.
8. Apruzzese, G. (2018). On the effectiveness of machine and deep learning for cyber security 10th international conference on cyber Conflict (CyCon). – IEEE, 371-390.
9. Bereziński, P. (2016). Detection of multistage attack in federation of systems environment //Military Communication Institute.
10. Dumont, P. (2019). Detection of malicious remote shell sessions 11th International Conference on Cyber Conflict (CyCon). – IEEE, 900: 1-20.
11. Hughey, R. and Krogh, A. (2016). Hidden Markov models for sequence analysis: extension and analysis of the basic method //Bioinformatics. 12 (2): 95-107.
12. Sato, M. and Yamaki, H. (2012). Takakura H. Unknown attacks detection using feature extraction from anomaly-based ids alerts IEEE/IPSJ 12th International Symposium on Applications and the Internet. – IEEE, 273-277.
13. Schuller, B. and Rigoll, G. (2013). Lang M. Hidden Markov model-based speech emotion recognition //2003 IEEE International Conference on Acoustics, Speech, and Signal Processing, 2003. Proceedings. (ICASSP'03). 2(2): 1.

A BLUEPRINT FOR THE FUTURE: THE EU AI ACT'S ROLE IN SHAPING AI, CYBERCRIME, AND MEDTECH SECURITY

Author: Gabriella Marcelja
President of SIRIUS GLOBAL - Academic Diplomacy 4.0 and the International Medical Community (Rome, Italy)

The European Union's AI Act marks a significant milestone as the first comprehensive regulation aimed at governing the development, deployment, and use of Artificial Intelligence (AI) systems. With the rapid advancement of AI technologies, the regulation addresses the pressing need for a legal framework that balances innovation with ethical considerations, security, and accountability. This article delves into the EU AI Act's implications, the challenges of AI-powered cybercrimes, and the specific impact on the medtech sector.

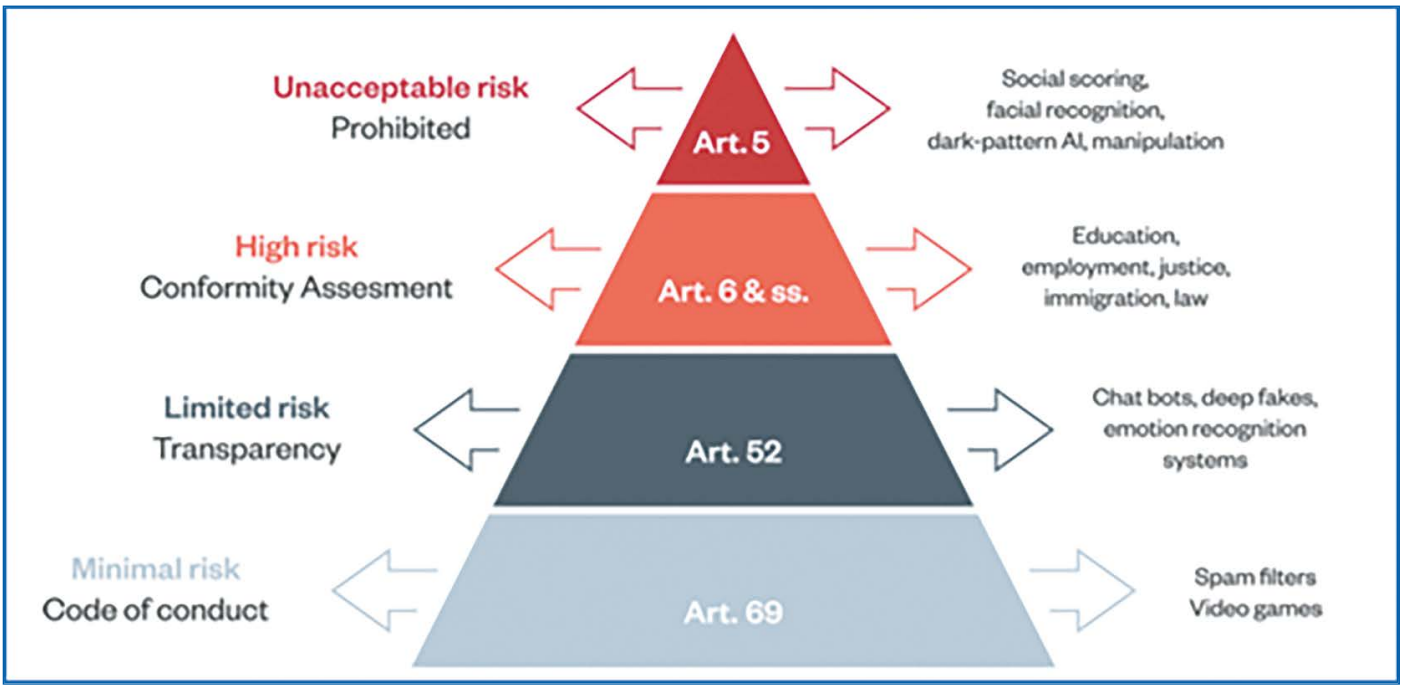
***

Almost three years following the European Commission's initial proposal for a regulatory framework governing artificial intelligence (AI), the European Parliament has given its conclusive approval to the EU AI Act. The vote, which took place on 13 March 2024, saw the regulation being passed with a majority of 523 to 46 votes in favor. This act, known as the "EU AI Act", represents the first binding worldwide horizontal regulation on AI, setting a common framework for the use and supply of AI systems within the European Union (EU). In terms of legal enforceability and following the European Parliament's approval, the legislative journey of the AI Act is nearing its conclusion. The Act is set to become effective 20 days subsequent to its announcement in the Official Journal, anticipated around May or June 2024. The majority of its stipulations will be enforceable two years subsequent to the Act's activation.

The EU AI Act introduces a risk-based approach to AI regulation, categorizing AI systems into unacceptable risk, high-risk, limited risk, and minimal risk categories, with different obligations for each.

Unacceptable risk AI practices are prohibited, high-risk AI systems are subject to stringent requirements, limited risk AI systems face transparency obligations, and minimal risk AI systems have no additional obligations. For instance, some key changes the Act will bring include:

- Prohibiting certain 'unacceptable risk' AI practices, such as social scoring and real-time remote biometric identification. These practices will be banned outright.
- Subjecting 'high-risk' AI systems (used in critical infrastructure, education, employment, and access to essential services) to strict requirements. These requirements include conformity assessments, risk management, and transparency.
- Imposing transparency obligations on 'limited-risk' AI systems, like chatbots and deepfakes, to ensure users are aware they are interacting with an AI.
- Ensuring 'minimal risk' AI systems have no additional obligations, reflecting their lower risk profile.



Source: Ada Lovelace Institute (2022)

The individuals and entities subject to obligations under the EU AI Act are predominantly 'providers', which refers to those who develop an AI system with the intent of placing it on the market or putting it into service under their own name or trademark. However, obligations also or alternatively fall on 'users' - defined as any natural or legal person using an AI system under their authority, such as a local authority implementing a fraud detection scheme or an employer adopting an automated hiring system. Moreover, importers and distributors also have obligations, akin to those within the product safety regime, intended to prevent dangerous products built outside the EU from entering its market.

This Act aims to protect individuals by introducing enhanced safeguards against harmful AI practices and increasing transparency in AI interactions, thereby fostering trust. It specifically targets the risks associated with AI technologies, such as discrimination, privacy breaches, and the need for human oversight, and lays out measures to mitigate these concerns. By banning manipulative AI practices and imposing stringent requirements on high-risk AI systems, the Act ensures these technologies are transparent, secure, and respect fundamental rights. For example, the Act prohibits specific AI applications that infringe upon citizen rights. These include systems that categorize individuals by sensitive traits and the indiscriminate harvesting of facial images from online sources or surveillance cameras (CCTV) to compile facial recognition databases. Moreover, the deployment of emotion recognition technology in workplaces and educational institutions, societal scoring systems, predictive policing that relies solely on personal profiling, and AI designed to control human behavior or exploit vulnerabilities is also banned. Moreover, the new legal framework forbids the employment of biometric identification by law enforcement, with narrowly carved exceptions

for meticulously specified scenarios. 'Real-time' biometric identification (RBI) is permissible under stringent conditions, such as temporal and geographical limitations and necessary approval from judicial or administrative authorities. These exceptions might apply to cases like searching for a missing individual or thwarting terrorist activities. Retrospective biometric identification is classified as high-risk and contingent on judicial sanction linked to a specific criminal act.

Furthermore, high-risk AI systems, identified by their substantial potential to harm health, safety, fundamental rights, the environment, democracy, and legal order, are bound by explicit obligations. High-risk applications span various sectors, including critical infrastructure, educational and vocational sectors, employment, and essential services like healthcare and finance. These sectors also encompass law enforcement, immigration, and judicial systems, as well as democratic processes such as elections. Such AI must undergo risk mitigation, maintain detailed usage records, ensure operational transparency and accuracy, and incorporate human oversight. Citizens are entitled to lodge grievances regarding AI systems and to receive explanations for decisions made by high-risk AI that affect them.

When it comes to transparency obligations, general-purpose AI systems, including their underlying models, must adhere to transparency protocols, including abiding by EU copyright laws and disclosing comprehensive summaries of their training data. The most impactful general-purpose AI models, which could pose systemic risks, will face additional scrutiny, including model assessments, systemic risk evaluations, and incident reporting. Moreover, content that has been artificially altered or fabricated, known as «deepfakes,» must be clearly identified as such.

Nonetheless, the AI Act facilitates the establishment of regulatory sandboxes and real-world testing environments, offering a controlled setting where innovative AI systems can be trialed for a limited period. This provision aims to promote innovation among companies, SMEs, and startups. Additionally, the Act includes provisions that allow providers to show compliance through voluntary codes of practice, akin to the GDPR model. Such flexibility may enable the exploration of novel approaches. Ultimately, with the future implementation of the EU AI Act, there will undoubtedly be opportunities for new technologies within the regulatory framework of the law. The Act is designed to foster innovation while ensuring that AI technologies are developed and utilized in a manner that is safe and respects fundamental rights. For companies outside the EU looking to operate within its market, there are several key considerations to bear in mind. Indeed, the AI Act has extraterritorial implications, applying to any organization, even those based outside the EU, if their AI systems are introduced into the EU market or impact individuals within the EU. For instance, a Swiss bank utilizing an AI system for assessing the creditworthiness of EU citizens would be required to adhere to the Act. Such companies will need to fulfill obligations including conducting conformity assessments, establishing risk management systems, and ensuring transparency for users. In summary, the EU is attempting to balance the benefits of AI with the associated risks. Companies, both within and outside the EU, must navigate this new regulatory environment thoughtfully. Nevertheless, the Act still allows for innovation and adaptability.

When it comes to cybercrime, the EU AI Act addresses the phenomenon through its provisions on cybersecurity and risk management for high-risk AI systems. Providers of high-risk AI systems are required to ensure appropriate levels of accuracy, robustness, and cybersecurity by establishing a quality management system for compliance; consequently, tracking and documenting serious incidents is mandatory. This also includes obligations to report serious incidents and malfunctioning of AI systems that could pose risks to health, safety, or fundamental rights. The Act's focus on cybersecurity aims to mitigate the risks associated with the use of AI in critical sectors, including preventing the exploitation of AI systems for malicious purposes. By imposing these requirements, the EU AI Act plays a significant role in combating cybercrime related to AI technologies, ensuring that AI systems are secure and resilient against cyber threats.

For medtech companies and specifically the medical field, the EU AI Act carries significant implications: AI-based medical devices are categorized as «high-risk» and will require conformity assessments. To this end, the EU AI Act integrates with the existing EU Medical Devices Regulation (MDR), focusing specifically on AI medical devices. The Act emphasizes the protection of patients' fundamental rights, such as privacy and non-discrimination, areas which the current EU Medical Devices Regulation (MDR) does not sufficiently address. While the MDR already classifies medical devices based on risk, the AI Act introduces additional considerations for AI applications in healthcare, emphasizing fundamental rights and the quality of data used in AI systems. In fact, enhancements in algorithmic transparency and data quality are crucial for the genuine protection of patient rights within healthcare AI. Medtech companies must ensure that their AI medical devices, now classified as high-risk, meet both MDR and AI Act requirements, including thorough risk management, data governance, and conformity assessments. These measures aim to prevent patient harm from biases or errors in AI systems and improve transparency and accountability in AI's use in healthcare. The focus on data quality and human oversight under the AI Act directly impacts how patient data is used in AI applications, ensuring that data is representative, error-free, and managed according to strict governance practices. Nonetheless, many health-related AI applications may still remain outside the AI Act's purview, indicating a potential need for additional regulation.

Conclusion

In summary, the EU AI Act stands as a pivotal regulation in the realm of AI technologies, establishing a precedent for global AI governance. The Act not only creates a regulatory environment that prioritizes safety, fundamental rights, and transparency but also provides a structured framework for the introduction and application of new technologies. Consequently, companies from outside the EU should diligently monitor these regulatory developments to ensure compliance upon entering the EU market, thus seizing the opportunities for innovation and development within a secure and rights-respecting framework. Additionally, as AI-powered cybercrimes continue to evolve, the Act's risk-based approach offers a flexible yet rigorous framework for addressing these challenges effectively. The active participation of stakeholders will be essential in continually adapting and refining these regulations to align with the rapidly evolving technological landscape.

References:

1. European Parliament, EU Artificial Intelligence Act, accessed on 13 March 2024: https://www.europarl.europa.eu/doceo/document/TA-9-2024-03-13-TOC_EN.html

2. European Parliament, Press Release on “Artificial Intelligence Act MEPs Adopt Landmark Law”, accessed on 13 March 2024:https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landmark-law

3. Lilian Edwards, The EU AI Act: a summary of its significance and scope, Ada Lovelace Institute, 11 April 2022, accessed on 28 March 2024: https://www.adalovelaceinstitute.org/wp-content/uploads/2022/04/Expert-explainer-The-EUAI-Act-11-April-2022.pdf

www.cgitc.ru

125009, г. Москва, Тверской бульвар, д. 14, стр. 1