

УДК 32.09.5

К. А. Татаринов<sup>1</sup>  
Н. Н. Аникиенко<sup>2</sup>  
С. М. Музыка<sup>3</sup>

## **Влияние современных технологий на международную среду**

<sup>1</sup>ФГБОУ ВО «Байкальский государственный университет»,  
г. Иркутск

*e-mail:tatarinov723@gmail.com*

<sup>2</sup>ФГБОУ ВО «Иркутский государственный аграрный  
университет имени А.А. Ежевского», Иркутский район  
*e-mail:anikienkonikolai@mail.ru*

<sup>3</sup>ФГБОУ ВО «Иркутский государственный аграрный  
университет имени А.А. Ежевского», Иркутский район,  
*e-mail:ignitmuz@mail.ru*

**Аннотация.** В геополитическом измерении доступ к современным технологиям влияет на возможность проецирования силы, а также наращивает политическую и военную мощь страны. Информация — это атрибут и инструмент государственной силы, направляемы внутрь и вовне, с большим потенциалом геополитических последствий. Роль информации сегодня постоянно возрастает в связи с развитием технологий, управляемых данных, и их проникновением в обыденную жизнь. В исследовании говорится о нарастании цифрового противостояния между США и Китаем, которое ведет к мировому киберсуверенитету и геополитической напряженности. Установлено, что страны-лидеры в использовании больших данных и искусственного интеллекта получают неоспоримые геоэкономические, политические и военные преимущества, в отличие стран-аутсайдеров.

**Ключевые слова:** цифровые технологии, цифровые данные, большие данные, цифровизация, киберсуверенитет.

### **Введение**

Новой сферой соперничества между странами в третьем десятилетии XXI века, которая определит исход игры за мировое господство, станут цифровые технологии. Технологическая гонка касается не только производства товаров и оказания услуг, она определяет положение отдельных стран в цифровом мире и трансформирует мировую экономику, создавая совершенно новые факторы роста. Появляются новые связи между производителями и конечными потребителями и это дает странам шанс занять более высокое положение в глобальных цепочках создания стоимости. «Цифровые регионы» получают более быстрое экономическое развитие, более быструю социальную модернизацию и более быстрое процветание. *Актуальность настоящего исследования*, определяется тем, что успешная конкуренция в «цифровой битве» не только меняет экономический и военный потенциал государства, но и его международное положение и способность влиять на другие страны. *Цель статьи* — дать комплексную оценку того, как широкое внедрение цифровых технологий может повлиять на геополитическую ситуацию в мире. *Обзор литературы.* Проблемам изучения современных технологий и их влияния на общественную жизнь посвящены работы российских исследователей: влияние цифровизации на

экономику [1, 2, 5, 8, 10, 17, 18, 19, 20, 22], развитие искусственного интеллекта [7, 11], датаизации [7, 9, 13, 15] и кибербезопасности [3, 4, 6, 14, 16, 21].

### **Материалы и методы**

В исследовании использована информация современных российских ученых, имеющих непосредственное отношение к проблемам инновационного развития мира. Методическую основу исследования составляют общенаучные методы: анализ и синтез, сравнение и обобщение.

### **Результаты и обсуждение**

#### **Цифровые технологии как элемент мощности сил**

События последнего десятилетия ясно показывают, что цифровые технологии стали одной из самых ожесточенных областей борьбы между сверхдержавами — США и Китаем. В августе 2020 года госсекретарь США Майк Помпео объявил о расширении программы «Чистая сеть», которая должна обеспечить защиту частной жизни граждан и конфиденциальную информацию бизнеса от «агрессивных вторжений злоумышленников». Это сделано для того, чтобы обеспечить блокировку китайских технологических компаний к рынку и сетям США. В ответ, коллега Помпео в Китае, Ван И призвал технологические компании не создавать бэкдоры, которые незаконно собирают данные. Технологический конфликт между США и Китаем вписывается в более широкое геополитическое соперничество двух стран и играет в нем центральную роль. Использование кибероружия в наступательных целях является результатом геополитических процессов, происходивших в первых двух десятилетиях XXI века. Например, в 2013 году Эдвард Сноуден разоблачил созданную США систему глобальной электронной слежки и шпионажа или в 2016 году происходили манипуляции во время президентских выборов в США. Экспоненциальный скачок в использовании цифровых технологий в 2022 году во всех аспектах социально-экономической деятельности общества (генерация, неотличимых от фотографий, картинок для новостей; использование кибероружия в военных конфликтах; качественный автоподбор аудитории в интернет-рекламе), показал нам многообразие уязвимостей цифрового мира, в котором мы будем дальше жить. Лидеры всех континентов открыто говорят о цифровом суверенитете своих стран, а аналитики предупреждают, что происходит перманентное разделение цифрового мира на два блока. Процессы управления цифровыми технологиями являются полем настоящей геополитической борьбы. Чтобы демократическим обществам найти свое место в этом быстро меняющемся мировом ландшафте, нужно понять последствия, которые несут технологические прорывы для международной безопасности. Построение точной картины социальной реальности и осознание происходящих изменений — это отправная точка дискуссий, которые помогут политическим лидерам правильно ориентироваться в этом все более многообразном технологическом мире.

Цифровая революция, как когда-то в девятнадцатом веке паровой двигатель и механизация производства, ведет к экономическому буму, меняет облик национальных экономик и формирует совершенно другие международные отношения. Наряду с инновационными решениями цифровая революция несет в

себе риски обеспечения технологической безопасности. Масштаб этой проблемы делает целесообразным сотрудничество государства, коммерческого сектора и общественных организаций в этой сфере. В прошлом веке ядерные программы «звездных войн» прямо влияли на международную ситуацию и резко меняли баланс сил между СССР и США, но они лишь были инструментами политики. Сегодня же, наоборот именно политические процессы зависят от технологий. Одним из главных атрибутов государства всегда был контроль над самым опасным оружием. Сегодня самое опасное и эффективное оружие, основанное на искусственном интеллекте, находится в руках крупных технологических компаний, бюджеты которых находятся на уровне государственных. Цифровизация принесла миру огромную пользу, она поддерживает эффективные бизнес-модели, позволяет заботиться о малообеспеченных и изолированных группах населения и внедрять в жизнь концепцию непрерывного образования. Все эти изменения основывались на базовых ценностях демократического мира, таких как: уважение принципов демократии, право на свободу волеизъявления, уважение свободы личности. Цивилизация, ориентированная на человека, подразумевает, что он всегда находится в центре науки, политики и культуры. Возможен и другой путь развития, когда с помощью технологий мы сможем добиться того, чего не удавалось сделать никаким тоталитарным режимам (полного контроля над обществом и ограничения свободы личности). Экосистема, в которой каждый имеет право на достоверную информацию, на бесперебойное и конфиденциальное электронное общение и на использование открытого Интернета, должна быть основана на мировом партнерстве.

Политические аспекты использования данных — это одна из осей разделения цифрового мира (табл. 1).

Таблица 1

**Правила кибербезопасности**

Страна	Правила размещения данных
Китай	Закон Китая о кибербезопасности и облачных вычислениях требует, чтобы информация о китайских гражданах или информация, имеющая отношение к национальной безопасности, хранилась на внутренних серверах. Например, компания Apple вынуждена была передать данные китайских граждан из своего облака в облако местной компании, а Amazon продала свой центр обработки данных китайскому конкуренту.
Россия	Российские законы налагают большие штрафы за несоблюдение правил локализации персональных данных граждан. Например, блокировка LinkedIn за несоблюдение правил по локализации данных.
Иран	Халальный иранский Интернет, официально именуемый Национальной информационной сетью насчитывает около 500 одобренных правительством национальных сайтов, имеющих более высокую входящую скорость и более низкие цены для пользователей.
Северная Корея	Северокорейская версия внутренней интрасети Kwangmyong не подключена к глобальному Интернету и предоставляет ограниченную версию Интернета немногим избранным в стране.

Составлено по [6, 12, 20]

Данные являют огромным источником информации о деятельности человека, его поведении и привычках, а их агрегирование и анализ позволяет решать огромное количество проблем, с которыми сталкивается современное общество: от дорожно-транспортных происшествий до обращения с бытовыми отходами. В настоящее время полный спектр возможностей Big Data изучен не

полностью. Большие объемы данных нужны для обучающихся систем искусственного интеллекта (ИИ). Обязанность частных компаний сотрудничать с органами национальной безопасности позволяет создать синергию между технологическими гигантами и собирать огромные объемы данных для правительства Китая, а оно в свою очередь включает китайские компании в проекты по развитию интеллектуальных государственных услуг, что создает вторичные комфортные условия для сбора еще больших массивов данных. Результатом такого симбиоза является более быстрый темп китайской цифровой революции, чем американской или европейской. Политическая воля играет большую роль во внедрении цифровых технологий в реальную жизнь. Например, мобильные платежи в WeChat и в других социальных сетях способствовали впечатляющему развитию целых отраслей бизнеса и получению огромных прибылей для дальнейшего ее реинвестирования в технологические стартапы. Китай рассматривает цифровые технологии в качестве государственного властного инструмента. Для этого потребуется модернизировать китайскую промышленность за счет создания интеллектуальных производственных систем [11]. Политические решения, направленные на независимость Китая от иностранных поставщиков, предусматривают присвоение наиболее прибыльных звеньев в глобальных цепях поставок, через поглощение иностранных компаний. Китай хочет стать технологически самодостаточным, крупнейшим в мире поставщиком новых технологий и важнейшим источником инноваций. ИИ-решения, на фоне стареющего населения, экологических проблем и дефицита природных ресурсов, должны создать умные города, умные производства, умную медицину и умное сельское хозяйство. Как указывает бывший президент Google China КайФу Ли, Китай будет самым большим бенефициаром развития ИИ на основе «глубокого обучения». Китайские технологические компании инвестируют в иностранные стартапы и нацелены на создание локализованного продукта, адаптированного под запросы локального потребителя. Данную инициативу поддерживает государство в виде так называемого цифрового шелкового пути. В области квантовых вычислений Китай добился значительных успехов, продемонстрировав в 2017 году связь между двумя наземными центрами через спутник, зашифровав информацию с помощью квантовой запутанности.

США ни в коем случае не рассматривают себя проигравшими в борьбе с Китаем. Они по-прежнему мировой лидер в цифровых областях, а американские IT-компании занимают стабильные позиции на мировых рынках. Например, доля американских компаний (Intel, Google, AMD и др.) на рынке микропроцессоров более 40 %. Эта та область, в которой США и их союзники доминируют. Рынок микропроцессоров ИИ будет расти на 30 % в год и к 2027 году достигнет 80 млрд. \$. Американское федеральное правительство предусматривает широкий спектр мероприятий в этой области: от расширения сотрудничества между государственными и коммерческими центрами разработки ИИ до повышения компетенций в этой области среди рядовых сотрудников. Вашингтон видит в технологических амбициях Пекина угрозу его национальной безопасности, поэтому на законодательном уровне запрещает использовать в оборонной промышленности оборудование, произведенное китайскими компаниями (Huawei и ZTE), поскольку эти компании являются одними из ведущих поставщиков оборудования для построения сети 5G, на которой будет базироваться критическая инфраструктура будущего.

Разрыв глобальных цепочек добавленной стоимости в сфере технологий — это важнейший элемент американских действий против Китая [15]. В первой половине 2020 года этот процесс ускорился из-за пандемии, в результате которой правительства почти всех стран (особенно Китая) закрыли свои границы и глобальные потоки людей, товаров и услуг были остановлены. В конечном итоге это привело к срыву продаж новейшего технологического оборудования. Пандемия показала зависимость ведущих экономик мира от транснациональных цепочек поставок технологического оборудования, что усилило беспокойство США и Европы по поводу китайских инновационных инвестиций. Вашингтон повсеместно создает партнерские отношения, чтобы исключить китайских производителей оборудования для построения сети 5G и не допустить шпионской деятельности со стороны КНР.

### **Господство цифровых данных**

Кровеносной системой функционирования цифрового мира является цифровая инфраструктура, которая состоит из оптоволоконных кабелей, радиопередатчиков, сетевых компьютеров и другого оборудования. Эти устройства используются организациями, действующими в рамках различных политических режимов, что делает контроль над цифровой инфраструктурой геополитическим. Манипулирование этими устройствами — это вопрос национальной безопасности и государственного суверенитета. Поэтому службы безопасности, вооруженные силы, хакерские группы и террористические организации соревнуются в контроле киберпространства для достижения собственных целей. Развитие новых цифровых технологий, таких как сеть пятого поколения, ускорит развитие Интернета-вещей. Это ускорит умную трансформацию городов в сфере промышленности, транспорте и логистике. В то же время, каждый новый датчик увеличивает вероятность враждебных манипуляций, способных потенциально нанести ущерб человеку. Будущие квантовые вычисления смогут легко взломать самые сложные протоколы безопасности и шифрования данных, что приведет к асимметрии вычислительных мощностей между государствами с квантовыми возможностями и без них. Искусственный интеллект (ИИ) и далее продолжит автоматизацию и роботизацию социально-экономических процессов, меняя не только сферу общественной жизни, но и военную. Начиная от способности автономно идентифицировать и атаковать цели, до получения ценных данных для разведки, путем автоматизированного анализа больших объемов данных. Поэтому использование ИИ в военной сфере стало предметом международной гонки вооружений. Развитие ИИ позволит государству отслеживать, контролировать и вмешиваться в такие сферы личной жизни граждан, которые до сих пор оставались вне досягаемости даже для наиболее тоталитарных режимов.

Свободный поток данных в невообразимом масштабе привел к демократизации всех форм использования и применения информации. Государство лишилось монополии на получение доходов от продажи информации и ему приходится конкурировать с частными корпорациями в разработке новых технологий. Эта тенденция вызвала ответную реакцию со стороны государств и их стремление к реализации концепции цифрового суверенитета, который должен определять вектор контроля действий государственных институтов над киберпространством. Европейский Союз определяет цифровой суверенитет как стратегическую автономию, которая охватывает деятельность от обороны до

политики в области здравоохранения (особенно во время пандемий). Концепция китайского цифрового суверенитета играет ключевую роль в технологической политике государства. Интернет рассматривается как ключевой процесс глобализации, поэтому требует управления для обуздания негативных последствий его использования. Пекин поддерживает усилия ООН по управлению Интернетом и стремится узаконить цифровой политический консенсус, в котором правила игры будут устанавливать национальные правительства. То есть государство вправе устанавливать суверенные границы в Интернете и полностью подчинять цифровые технологии своим интересам. Действия пользователей и поставщиков цифровых услуг вне зависимости от территориального расположения должны быть подчинены национальным органам законодательной и исполнительной власти. Логика «киберсуверенитета» привела к созданию брандмауэра «Золотой щит», который идентифицирует VPN-трафик и «режет» соединение, предотвращая его подключение к внешним серверам. Мировая тенденция к установлению полного цифрового суверенитета может привести к созданию Сплинтернета, в котором глобальная сеть будет разделена на локальные сети, контролируемые политическими институтами государств (табл. 2).

**Таблица 2**

**Уровни цифрового суверенитета**

Стремление к автономии данных	Страны
Собственный национальный интернет	Иран, Северная Корея, Бруней
Запрет на передачу всех отраслевых данных	Китай, Россия, Нигерия
Запрет на передачу данных по отдельным отраслям	Германия, ОАЭ, Турция, Австралия, Монако
Обязательное локальное копирование данных перед передачей	Индия, Вьетнам
Локальный контроль передачи данных	Европейский Союз, Бразилия, Колумбия, Перу, Аргентина

*Составлено по [4, 11, 22]*

Каждое правительство будет решать, что, когда и как можно делать в сети — какой контент публиковать, какие веб-сайты посещать и какую информацию отправлять. Разные правила использования сети и разные законы о безопасности передачи информации приведут к тому, что универсальный Интернет исчезнет и не будет больше глобальной агоры, позволявшей ранее каждому взаимодействовать со всеми и свободно говорить то, что хочешь. Фрагментация Интернета — это отражение трансформации современной международной системы, которая все более многополярна, а власть в ней территориально децентрализованная. Соперничество между крупными мировыми державами происходит не только из-за различия во взглядах на организацию Интернета, но на всю роль цифровых технологий в мире.

Влияние цифровых технологий на экономику революционно. Дешевые и доступные виртуальные цифровые мощности, гигантские возможности передачи данных с малыми задержками по сети 5G будут способствовать динамичному развитию автоматизации производства и рынку Интернет-вещей. Цифровизация катализирует развитие других секторов экономики, например, беспилотный транспорт, 3D-печать, биомедицина и диагностические устройства. Масштабы передачи данных нарастают беспрецедентными темпами, например, по IP в 1992

передавалось 100 гигабайт (ГБ) в сутки, а в 2022 году — уже 150700 ГБ в секунду, и это только начало цифровой революции. На США и Китай в 2020 году приходилось 75 % патентов, связанных с технологией блокчейн, 50 % расходов на IoT, более 75 % рынка общедоступных облачных вычислений, в то время как европейская доля в этих сегментах составляла менее 4 %. Устойчивая корреляция между экономическим ростом и увеличением проникновения Интернета во все сферы жизни сильнее проявляется в развивающихся странах, чем в развитых. Теперь в любой цепочке создания стоимости можно собирать, хранить и анализировать данные, а это дает большое конкурентное преимущество, так как данные — это ядро всех цифровых технологий (AI, IoT, блокчейн, облачные вычисления). Лидерство США в сфере обработки данных бесспорно (Google — 90 % рынка интернет-поиска, Amazon — 40 % розничного рынка электронной коммерции, Meta — 70 % рынка социальных сетей, Microsoft — 78 % рынка операционных систем). WeChat или Alibaba, несмотря на внушительное количество пользователей, ориентированы в основном на внутренний рынок.

Рост генерируемых и передаваемых через Интернет данных в геометрической прогрессии, а также их геоэкономическое и геополитическое значение приведет к тому, что в будущем международные конфликты также примут форму борьбы за данные. Доступ к большим массивам данных и их соответствующий анализ создаст преимущество на поле боя. Благодаря ИИ данные будут быстро трансформироваться в качественную информацию, которая найдет применение в общественной деятельности, процессах принятия стратегических решений и в военных действиях. Большие массивы данных — это вопрос стратегической автономии и цифрового суверенитета стран, их геотехнологическое положение, а, следовательно, геополитическое и геоэкономическое преимущество государства. Поэтому данные сегодня — это значимый и привлекательный геополитический ресурс. Консолидация данных среди транснациональных корпораций ведет к еще большим прибылям, чем сейчас. Так как сбор, анализ и использование данных является неременным условием будущей политической, экономической и военной мощи стран, развивающиеся и слаборазвитые страны еще больше углубляют свое отставание. ООН призывает к разработке соответствующих правил, с тем чтобы цифровая экономика приносила пользу не только некоторым странам, а и всему миру. Страны с ограниченными возможностями по обработке данных в высококачественную информацию для бизнеса находятся в невыгодном положении, когда речь идет о создании ценности. Такие страны в последствие могут стать цифровыми колониями, а бизнес в них скорее всего обанкротится.

Цифровые данные — это машиночитаемая информация, дополняющая физический мир. Объем данных, генерируемых устройствами, в будущем будет расти в геометрической прогрессии из-за прогрессирующей цифровизации экономики в рамках четвертой промышленной революции (более 90 % всех данных будут промышленные). Если провести анализ карты цифрового мира, то большая концентрация этого нового экономического ресурса наблюдается в США и Китае. Эти страны получают наибольшие геоэкономические выгоды, которые можно капитализировать также как в политическом, так и в военном плане. При использовании цифровых продуктов остаются цифровые следы личной, социальной или деловой активности. Датаификация, заключающаяся в создании цифровых двойников реального мира отображает окружающий мир с почти

зеркальной точностью и знакомит нас с виртуальным миром, который можно назвать «зеркальной» реальностью. Однако важен не только объем генерируемых данных (к 2025 году их будет около 463 экзабайтов), но и возможность подняться по цепочке создания стоимости данных (от сбора необработанных данных, через высококачественную информацию, до трансформации ее в знания) и их монетизации. Источников данных очень много, но наиболее ценны те данные, которые генерируются отдельными пользователями Интернета. То есть чем больше население страны и процент людей, имеющих доступ в Интернет, тем «естественнее» данные. Другим ценным источником являются геопространственные, метеорологические и статистические показатели, а также данные с носимых сенсорных устройств. Развитие цифровой экономики происходит не только из-за технологически стимулируемого роста данных, но и за счет развития облачных сервисов и технологий ИИ.

### **Выводы**

В последнее десятилетие цифровые технологии превратились в центральную область глобального соперничества между США и Китаем. Оба государства стремятся освободиться от взаимной технологической зависимости, так как ИИ, 5G и квантовые вычисления, воспринимаются ими как угроза национальной безопасности и как средство изменения глобального баланса сил. Обострившийся политический и экономический конфликт между сверхдержавами привел к тому, что Китай уже несколько лет подряд ускоренными темпами наращивает свою собственную технологическую мощь. Поэтому сегодня геэкономическое положение страны зависти от эффективности цифровой трансформации экономики (адаптация системы образования к вызовам цифрового мира; основанное на данных, частно-государственное партнерство в технологической сфере; долгосрочные стратегии развития цифровой инфраструктуры; институционально-правовая система для поддержки экосистемы инноваций).

### **Литература**

1. Балашов Е. Л., Зубович К. Е. Цифровые и нецифровые факторы, влияющие на развитие цифровой экономики Севастополя // Ученые записки Крымского федерального университета имени В. И. Вернадского. Экономика и управление. 2019. Т. 5(71). № 2. С. 3–7.
2. Баржанов А. Б. Цифровизация в отрасли: вызовы, ключевые сдерживающие факторы, направления цифровизации // Школа Науки. 2021. № 5(42). С.15–16.
3. Бойченко О. В., Гунько А. В. Информационная безопасность цифровизации экономики Республики Крым // Ученые записки Крымского федерального университета имени В.И. Вернадского. Экономика и управление. 2019. Т. 5(71). № 2. С. 17–25.
4. Воинова Я. Е., Карпович Ю. В. Цифровая экономика и кибербезопасность – противоречия и перспективы развития // Вектор экономики. 2021. № 7 (61). С. 12–17.
5. Воронина Т. В., Евченко Н. Н., Яценко А. Б. Состояние и стратегии развития цифровой экономики стран ЕАЭС // Ученые записки Крымского федерального



- университета имени В.И. Вернадского. Экономика и управление. 2018. Т. 4(70). № 4. С. 36-45.
6. Головенчик Г., Краско Г., Головенчик М. Проблемы кибербезопасности умных городов // Наука и инновации. 2020. № 12 (214). С. 51-57.
  7. Денисова О. Ю., Мухутдинов Э. А. Большие данные – это не только размер данных // Вестник Технологического университета. 2015. Т.18. № 4. С. 226-230.
  8. Дубовик Е. С., Брянская Н. А. Развитие цифровой экономики как одно из направлений активизации предпринимательской деятельности // Global and Regional Research. 2019. Т. 1. № 3. С. 218-224.
  9. Житников А. В., Ярош А. С. О развитии цифровизации в современной России // Вестник научного центра по безопасности работ в угольной промышленности. 2021. № 3. С. 65-72.
  10. Захарченко Е. С., Решетникова Н. Н. Современные тенденции цифровизации мировой экономики с учетом развития «зеленой» экономики в условиях пандемии COVID-19 // Научный вестник: финансы, банки, инвестиции. 2021. № 4 (57). С. 132-142.
  11. Колесниченко А. Е. Экономика КНР: современные тренды и перспективы развития в условиях цифровизации мирового пространства // Via Scientiarum - Дорога знаний. 2019. № 2. С. 18-24.
  12. Коньков А. Е. Цифровизация политики vs политика цифровизации // Вестник Санкт-Петербургского университета. Международные отношения. 2020. Т. 13. № 1. С. 47-68.
  13. Кузнецов А. В. Цифровизация как новый этап глобализации / А. В. Кузнецов // Философия хозяйства. 2021. № 4 (135). С. 76-97.
  14. Мийзамов А. А., Енин В. М., Матющенко И. А. Актуальные вопросы кибербезопасности // International Journal of Advanced Studies in Computer Engineering. 2021. № 1. С. 17-21.
  15. Муха Д. В. Влияние индустрии 4.0 на глобальные цепочки создания стоимости, бизнес-модели и прямые иностранные инвестиции // Экономическая наука сегодня. 2021. № 13. С. 75-84.
  16. Николаев Е. Н. Проблемы информационной безопасности в аспекте развития искусственного интеллекта // Инновации. Наука. Образование. 2021. № 48. С. 1428-1434.
  17. Пожарицкая И. М. Цифровой менеджмент: концепция или инструментарий? // Baikal Research Journal. 2021. Т. 12. № 2.
  18. Полуэктова Н. Р. Цифровая экономика: сущность, проблемы, подходы к управлению изменениями // Ученые записки Крымского федерального университета имени В.И. Вернадского. Экономика и управление. 2018. Т.4 (70). № 4. С. 121-128.
  19. Сафиуллина, А. Л., Камалов А. Р. Цифровизация мировой экономики: ключевые секторы // Научный электронный журнал Меридиан. 2021. № 2 (55). С. 210–212.
  20. Симченко Н. А., Нестеренко Е. С. Институциональные вызовы развития цифровой экономики в России // Ученые записки Крымского федерального университета имени В.И. Вернадского. Экономика и управление. 2017. Т. 3(69). № 3. С. 108–114.

21. Феткулин Р. Р., Арюков А. К. Преступления в сфере цифровой информации: понятие и виды // *Baikal Research Journal*. 2019. Т. 10. № 3. С. 17-22.
22. Ячменева В. М., Ячменев Е. Ф. Цифровое пространство как необходимое и достаточное условие цифровизации экономики // *Baikal Research Journal*. 2020. Т. 11. № 3. С. 2-12.

**К. А. Tatarinov**<sup>1</sup>  
**N. N. Anikienko**<sup>2</sup>  
**S. M. Musica**<sup>3</sup>

---

### ***Influence of modern technologies on the international environment***

---

<sup>1</sup>Baikal State University, Irkutsk  
*e-mail:tatarinov723@gmail.com*

<sup>2</sup>Irkutsk State Agrarian University named after A.A. Yezhevsky,  
Irkutsk district  
*e-mail:anikienkonikolai@mail.ru*

<sup>3</sup>Irkutsk State Agrarian University named after A.A. Yezhevsky,  
Irkutsk district  
*e-mail:ignitmuz@mail.ru*

**Abstract.** *In the geopolitical dimension, access to modern technology affects the ability to project power, and also increases the political and military power of the country. Information is an attribute and tool of state power, directed inward and outward, with great potential for geopolitical consequences. The role of information today is constantly increasing due to the development of technologies, managed data, and their penetration into everyday life. The study notes the growing digital confrontation between the US and China, which leads to global cyber sovereignty and geopolitical tensions. It has been established that the leading countries in the use of big data and artificial intelligence receive undeniable geo-economic, political and military advantages, unlike outsider countries.*

**Keywords:** *digital technologies, digital data, big data, digitalization, cyber sovereignty.*

### ***References***

1. Balashov E. L., Zubovich K. E. Digital and non-digital factors influencing the development of the digital economy of Sevastopol // *Uchenye zapiski V.I. Vernadsky. Economics and Management*. 2019. Т. 5 (71). №. 2. P. 3-7. (in Russian)
2. Barzhanov A. B. Digitalization in the industry: challenges, key constraints, areas of digitalization // *School of Science*. 2021. №. 5 (42). P. 15-16. (in Russian)
3. Boichenko O. V., Gunko A. V. Information security of the digitalization of the economy of the Republic of Crimea // *Uchenye zapiski Crimean Federal University named after V.I. Vernadsky. Economics and Management*. 2019. Т. 5 (71). №. 2. P. 17-25. (in Russian)
4. Voinova Ya. E., Karpovich Yu. V. Digital economy and cybersecurity — contradictions and development prospects // *Vector of Economics*. 2021. №. 7 (61). P. 12-17. (in Russian)
5. Voronina T. V., Evchenko N. N., Yatsenko A. B. Status and development strategies of the digital economy of the EAEU countries // *Uchenye zapiski V.I. Vernadsky. Economics and Management*. 2018. Т. 4 (70). №. 4. P. 36-45. (in Russian)

6. Golovenchik G., Krasko G., Golovenchik M. Problems of cybersecurity of smart cities // Science and Innovations. 2020. №. 12 (214). P. 51-57. (in Russian)
7. Denisova O. Yu., Mukhutdinov E. A. Big data is not only the size of data // Bulletin of the Technological University. 2015. T. 18. №. 4. P. 226-230. (in Russian)
8. Dubovik E. S., Bryans N. A. Development of the digital economy as one of the directions of business activity activation // Global and Regional Research. 2019. V. 1. №. 3. P. 218-224. (in Russian)
9. Zhitnikov A. V., Yarosh A. S. On the development of digitalization in modern Russia // Bulletin of the scientific center for the safety of work in the coal industry. 2021. №. 3. P. 65-72. (in Russian)
10. Zakharchenko E. S., Reshetnikova N. N. Modern trends in the digitalization of the world economy, taking into account the development of the "green" economy in the context of the COVID-19 pandemic // Scientific Bulletin: Finance, Banks, Investments. 2021. №. 4 (57). P. 132-142. (in Russian)
11. Kolesnichenko A. E. Economy of China: modern trends and development prospects in the context of digitalization of the world space // Via Scientiarum — The Road of Knowledge. 2019. №. 2. P. 18-24. (in Russian)
12. Konkov A. E. Digitalization of politics vs digitalization policy // Bulletin of St. Petersburg University. 2020. T. 13. №. 1. P. 47-68. (in Russian)
13. Kuznetsov A. V. Digitalization as a new stage of globalization // Philosophy of economy. 2021. №. 4 (135). P. 76-97. (in Russian)
14. Miyzamov A. A., Enin V. M., Matyushchenko I. A. Actual issues of cybersecurity // International Journal of Advanced Studies in Computer Engineering. 2021. №. 1. P. 17-21. (in Russian)
15. Mukha D. V. Influence of Industry 4.0 on global value chains, business models and foreign direct investment // Economics today. 2021. №. 13. P. 75-84. (in Russian)
16. Nikolaev E. N. Problems of information security in the aspect of the development of artificial intelligence // Innovations. The science. Education. 2021. №. 48. P. 1428-1434. (in Russian)
17. Pozharitskaya I. M. Digital management: concept or tools? // Baikal Research Journal. 2021. T. 12. №. 2. (in Russian)
18. Poluektova N. R. Digital economy: essence, problems, approaches to change management // Uchenye zapiski V.I. Vernadsky. Economics and Management. 2018. T. 4 (70). №. 4. P. 121-128. (in Russian)
19. Safiullina A. L., Kamalov A. R. Digitalization of the world economy: key sectors // Scientific electronic journal Meridian. 2021. №. 2 (55). P. 210-212. (in Russian)
20. Simchenko N. A., Nesterenko E. S. Institutional challenges for the development of the digital economy in Russia // Uchenye zapiski V.I. Vernadsky. Economics and Management. 2017. T. 3 (69). №. 3. P. 108-114. (in Russian)
21. Fetkulin R. R., Aryukov A. K. Crimes in the field of digital information: concept and types // Baikal Research Journal. 2019. T. 10. №. 3. P. 17. (in Russian)
22. Yachmeneva V. M., Yachmenev E. F. Digital space as a necessary and sufficient condition for the digitalization of the economy // Baikal Research Journal. 2020. T. 11. №. 3. P. 2–12. (in Russian)

*Поступила в редакцию 20.04.2023г.*