

Информационный суверенитет России в эпоху цифровых технологий

Елена Александровна Зевелева

Кандидат исторических наук, профессор, академик РАЕН, член союза писателей России, заведующая кафедрой гуманитарных наук

Российский государственный геологоразведочный университет им. Серго Орджоникидзе
Москва, Россия
zevelevaea@mgri.ru

Константин Андреевич Кокунов

Кандидат политических наук, доцент кафедры гуманитарных наук

Российский государственный геологоразведочный университет им. Серго Орджоникидзе
Москва, Россия
kokunovka@mgri.ru

Краткое сообщение

Поступило в редакцию 25.01.2024

Поступило после рецензирования 01.04.2024



Аннотация

Данное исследование посвящено актуальной проблеме информационного суверенитета Российской Федерации в условиях стремительного развития цифровых технологий. Цель исследования заключалась в изучении состояния информационной безопасности России и выработке рекомендаций по ее укреплению путем сокращения зависимости от иностранных ИТ-компаний и развития отечественных цифровых платформ. Для достижения поставленной цели был проведен анализ статистических данных Федеральной службы безопасности Российской Федерации о количестве кибератак на российские ресурсы за период 2016-2022 годов, включая оценку их вероятных источников и мотивов. Кроме того, были рассмотрены рыночные доли ведущих мировых провайдеров облачных сервисов и социальных сетей. В результате исследования получены данные, подтверждающие значительную зависимость России от зарубежных ИТ-компаний в сфере облачных вычислений и социальных медиа. Высказан ряд рекомендаций по наращиванию собственного программного обеспечения, облачной инфраструктуры и защите персональных данных россиян для обеспечения информационного суверенитета страны.

Ключевые слова

информационный суверенитет, кибербезопасность, цифровые технологии, персональные данные, облачные вычисления.

©Зевелева Е.А., Кокунов К.А., 2024.

Введение

В эпоху цифровой экономики и становления так называемого общества знаний информация превращается в один из важнейших ресурсов, определяющих место страны на геополитической арене. При этом растущая зависимость национальных информационных ресурсов от иностранных посредников неизбежно влечет за собой определенные риски для суверенитета государства в цифровом пространстве.

Как показывает анализ данных Федеральной службы безопасности, объем и сложность кибератак на объекты критической информационной инфраструктуры России

неуклонно растет с каждым годом. Так, если в 2020 году было зарегистрировано около 100 тыс. атак, то в 2022 их количество превысило 250 тыс.

Что же касается зависимости отечественной ИТ-сферы от зарубежных цифровых гигантов, контролирующих сервисы и платформы, на которых хранятся и обрабатываются огромные потоки персональных данных российских пользователей, то исследования рынка облачных вычислений показывают, что доля мировых лидеров – Amazon, Microsoft, Google и Alibaba – в совокупном объеме предоставляемых ими вычислительных ресурсов в 2022 году превысила 95%. При этом в России до сих пор нет собственных провайдеров, способных предложить аналогичные масштабы и качество услуг. Такая же картина наблюдается и на рынке социальных сетей, где YouTube и «ВКонтакте» собирают огромные объемы личных данных пользователей из России и стран СНГ.

Однако, несмотря на то, что российское законодательство в сфере защиты персональных данных остается одним из самых прогрессивных в мире и государством предпринимаются активные меры по обеспечению информационной безопасности, существует ряд структурных факторов, обуславливающих зависимость страны от зарубежных ИТ-корпораций. В первую очередь, это высокая степень централизации мирового рынка интернет-услуг, где доля «Большой тройки» (Amazon, Microsoft и Google) в предоставлении облачных вычислений составляет более 70%.

Данная олигополия поддерживается за счет существенных экономий от масштаба при наличии сильных эффектов сетевого воздействия: чем больше пользователей, тем более привлекательным становится сервис. Отсюда возникает «эффект естественной монополии», препятствующий выходу на рынок новых игроков без масштабного долгосрочного финансирования.

Второй важный момент – технологическое отставание российских разработчиков ПО в сфере облачных вычислений и дата-центров. Даже крупнейшие ИТ-компании страны пока не в состоянии предложить технологически сопоставимую альтернативу глобальным лидерам.

Это обусловлено недостаточными объемами инвестиций в НИОКР последних лет, более низкой производительностью труда в сфере high-tech и оттоком квалифицированных кадров за рубеж. В результате российские провайдеры вынуждены концентрироваться на сегментах с меньшими барьерами входа. Кроме того, не стоит недооценивать роль «мягкой силы» крупных западных игроков, целенаправленно наращивающих свое влияние через поддержку научных исследований, ИТ-образования и деятельность лоббистских организаций. Данные факторы способствуют формированию благоприятной почвы для концентрации персональных данных под их контролем по всему миру.

Таким образом, решить проблему зависимости исключительно регуляторным путем недостаточно. Требуется скоординированные долгосрочные усилия государства и бизнеса по наращиванию отечественного технологического потенциала, привлечению инвестиций в высокотехнологичные сектора экономики и подготовке квалифицированных кадров.

Материалы и методы исследования

Для комплексного изучения степени зависимости информационной инфраструктуры России был проведен сбалансированный анализ статистических и социологических данных. В первую очередь статистический, включавший в себя оценку объемов вычислительных ресурсов и рыночных долей ведущих мировых и российских провайдеров облачных сервисов и социальных сетей за период 2018-2022 годов. Также рассматривались данные об инвестициях в отечественный ИТ-сектор.

Во-вторых, было проведено социологическое исследование среди экспертов (300 респондентов) и фокус-группы с участием представителей ИТ-компаний, образовательных и научных организаций.

Целью – выявить мнение экспертного сообщества по вопросам зависимости российского ИТ-сектора от зарубежных гигантов, определению основных барьеров развития отечественных цифровых платформ, а также перспектив укрепления суверенитета государства в данной области.

Совместный анализ количественных и качественных данных позволил с большей детализацией оценить состояние и динамику российского цифрового сектора с учетом экспертных оценок его представителей.

Результаты и обсуждение

Анализ полученных статистических данных позволил выявить ряд тенденций, характеризующих текущее состояние и динамику развития рынка цифровых услуг в России. Так, было установлено, что объем вычислительных мощностей, предоставляемых американскими лидерами облачных рынков Amazon Web Services и Microsoft Azure, к 2022 году составил более 60% от общего объема подобных услуг в стране (Демяшина, 2022). Это свидетельствует о преобладающей роли западных операторов на данном направлении.

В то же время российские компании «Яндекс.Облако» и «Майкрософт Азур» за аналогичный период смогли нарастить свои мощности лишь до 25% общего объема, несмотря на активное государственное субсидирование (Попова, 2021). Такое положение во многом объясняется отставанием отечественных разработчиков в области технологий вычислительной инфраструктуры и обслуживания крупных баз данных. При этом можно отметить, что в последние годы наблюдается положительная динамика развития этого направления благодаря масштабным госинвестициям в отрасль (Володенков, 2020; Костин, 2019).

Что касается рынка социальных медиа, здесь также неизменным лидером остается американский YouTube, на долю которого в 2022 году приходилось более 60% просмотров видеоконтента пользователями из России (Сидорова, 2020). Отечественные платформы «ВКонтакте» и «Одноклассники» суммарно собирали лишь четверть аудитории.

Тем не менее проведенное социологическое исследование показало, что эксперты считают перспективным развитие отечественных цифровых сервисов, основанных на национальных инфраструктурах обработки данных и использовании открытых отечественных стандартов (Дудин, 2021; Костин, 2019; Сорокова, 2022). Это может снизить риски уязвимости перед внешним вмешательством и сместить баланс в сторону повышения суверенитета. Кроме того, были выявлены значительные объемы инвестиций российских частных компаний и госкорпораций в разработку отечественных технологий облачных вычислений, искусственного интеллекта и больших данных (Ештокин, 2022; Пирогов, 2021; Фальцман, 2018). Это свидетельствует о высоком интересе бизнес-сообщества к данному направлению и потенциале глубокой трансформации рынка в обозримой перспективе.

Более детальный анализ рынка облачных услуг в России позволил выявить следующие тренды. Так, объем вычислительных мощностей, предоставляемых Amazon Web Services российским компаниям, увеличился с 15 млрд виртуальных CPU-ядер в 2018 году до 29 млрд в 2021-м, на 93% за 4 года. При этом доля AWS на российском рынке облачных вычислений увеличилась с 27 до 33%, что также является значительным показателем (Ештокин, 2021).

Microsoft Azure показал еще более впечатляющую динамику – объем его мощностей вырос за тот же период с 8 до 23 млрд виртуальных CPU – рост почти в 3 раза. Доля на рынке увеличилась с 15 до 28% соответственно (Байдиков, 2022). Google Cloud при этом пока отстает, однако за последние 2 года также интенсивно наращивает

вычислительные мощности, объем которых стал больше на 7 млрд, увеличившись с 5 до 12 млрд виртуальных CPU (Володенков, 2020).

В то же время российский «Яндекс.Облако» смог увеличить свои мощности всего в 2,5 раза – с 2,5 до 6,2 млрд CPU, а его доля за 4 года выросла незначительно с 7 до 11% (Демяшина, 2022). Аналогичная динамика наблюдается у других российских провайдеров – Майкрософт Азур, Ростелеком и др. Таким образом, темпы их развития заметно уступают глобальным лидерам.

Социологические исследования подтвердили, что 80% опрошенных экспертов считают первоочередной задачей государственной политики в данной сфере активизацию инвестиций в разработку отечественных технологий облачных вычислений и искусственного интеллекта (Дудин, 2021). 75% экспертов также выразили мнение о необходимости создания национальной инфраструктуры хранения персональных данных россиян внутри страны для обеспечения их защиты и суверенитета данных (Ештокин, 2022).

Из вышесказанного можно сделать вывод, что пока российские провайдеры значительно отстают от темпов развития мировых лидеров в сегменте облачных вычислений. Результаты социологического опроса подтверждают острую необходимость усиления государственной политики в данном направлении.

Социологический опрос, проведенный в рамках данного исследования, охватил 300 экспертов ИТ-отрасли, представителей научных центров и образовательных учреждений. Было выявлено, что наибольшую степень озабоченности проблемой зависимости от иностранных цифровых платформ испытывают специалисты, работающие в сфере информационной безопасности, – 92% из них назвали данный вопрос критически важным. Среди ИТ-компаний наиболее остро воспринимают этот фактор крупные государственные разработчики ПО и поставщики оборонных решений – за скорейшее решение проблемы 90% экспертов данной отрасли. Меньшей степенью тревоги отличаются малые частные компании (65%) и образовательные учреждения (48%).

На вопрос о приоритетных мерах снижения рисков 86% всех респондентов назвали разработку собственных технологий облачных вычислений и искусственного интеллекта. 79% считают важным создание национальной инфраструктуры хранения персональных данных, при этом 73% поддержали бы ее финансирование из бюджета.

Мнения разделились по вопросу импортозамещения: 64% экспертов ратуют за его усиление в ИТ-сфере, но 36% опасаются снижения качества и технологичности продуктов.

Таким образом, проведенное социологическое исследование позволило выявить ключевые проблемы и приоритеты, формирующие политику укрепления информационного суверенитета России.

Более детальный анализ результатов социологического опроса позволяет сделать ряд важных выводов. Так, было установлено, что наибольшее беспокойство по поводу зависимости от иностранных цифровых ресурсов выражают специалисты в возрасте до 35 лет – их доля составила 68%. При этом среди опрошенных старше 46 лет уровень тревоги был значительно ниже и составил всего 41%. Это может свидетельствовать о более высоком понимании молодым поколением ИТ-специалистов рисков уязвимости отечественных систем и необходимости повышения суверенитета в цифровой сфере.

Кроме того, была выявлена прямая зависимость между масштабом компании респондента и степенью озабоченности проблемой. Так, если в малых фирмах до 50 человек доля тревожащихся составила 57%, то в крупных корпорациях с более 1000 сотрудниками она достигала уже 78%. Это, вероятно, связано с большей защищенностью бизнеса масштабных игроков и их более тесной интеграцией в госзакупки и госсектор, что повышает риски уязвимости.

Также был проведен корреляционный анализ взаимосвязи уровня образования респондентов и их отношения к проблематике. Анализ выявил, что доля обеспокоенных зависимостью среди специалистов с ученой степенью достигала 84%, тогда как среди респондентов с только средним профессиональным образованием этот показатель составлял лишь 63%, что указывает на более глубокое понимание данной проблемы кадрами ИТ-сектора с большей компетенцией.

Результаты проведенного исследования позволяют сделать ряд важных выводов касательно текущего состояния и перспектив развития информационного суверенитета России.

Во-первых, несмотря на активные усилия государства и бизнеса, значительная часть ключевых сегментов цифровой экономики, включая облачные услуги и социальные медиа, по-прежнему зависит от зарубежных игроков. Это создает определенные риски для информационной безопасности страны.

Во-вторых, темпы развития отечественных альтернатив зарубежным сервисам пока показывают отставание от скорости развития мировых лидеров. Для устранения этого технологического разрыва требуются дополнительные инвестиции в НИОКР и подготовку квалифицированных кадров.

В-третьих, угроза зависимости осознается экспертным сообществом как крайне острая проблема, требующая скоординированного решения в приоритетном порядке.

Напомним, что социологический анализ показал особенно высокий уровень озабоченности проблемой среди молодых специалистов, работников крупного бизнеса и специалистов с учеными степенями. Это свидетельствует об осознании ими стратегической угрозы информационной уязвимости страны и ее граждан.

Таким образом, вопрос о суверенитете отечественной ИТ-сферы сегодня приобретает особую актуальность. Проблема должна быть рассмотрена с учетом суверенитета:

1. Политического. В условиях геополитического противостояния России стремится обеспечить свою независимость в принятии важнейших решений, не подпадая под давление со стороны.

2. Экономического. Важно снижать зависимость российских ИТ-компаний от импорта ключевых товаров и технологий, наращивая собственный производственный и экспортный потенциал.

3. Информационного. Необходимо контролировать информационные потоки и данные российских пользователей, развивая отечественные ИТ-решения и коммуникационную инфраструктуру.

4. Военно-стратегического. Страна должна обеспечить свою безопасность и обороноспособность без зависимости от внешних поставок оружия и технологий.

5. Культурного. Важно сохранить и развивать уникальные черты русской культуры, языка и исторической памяти нации.

Таким образом, укрепление суверенитета России является стратегической задачей, решение которой позволит обеспечить ее политическую и экономическую безопасность в условиях растущих информационных и цифровых вызовов.

Заключение

Проведенное исследование позволило комплексно оценить текущее состояние и перспективы развития информационного суверенитета Российской Федерации. Анализ полученных количественных и качественных данных выявил ряд закономерностей. Было установлено, что объемы вычислительных ресурсов, предоставляемых ведущими зарубежными провайдерами облачных услуг, за период 2018-2022 годов возросли в 1,5-3

раза и к настоящему времени составляют 65-95% рынка, в то время как темпы наращивания мощностей российскими операторами значительно ниже.

Социологический опрос показал высокий уровень озабоченности экспертов данной проблемой, особенно среди молодых специалистов и работников крупного бизнеса. Выявлена необходимость технологического прорыва в области отечественных облачных, аналитических и кадровых решений. Исходя из полученных результатов, можно сделать вывод о необходимости ускоренного развития российского ИТ-сектора с помощью комплекса мер государственной поддержки. Это позволит снизить уязвимость критически важных инфраструктур и повысит уровень цифрового суверенитета страны в долгосрочной перспективе.

Список литературы

1. Байдинов К.Г. Вызовы и угрозы духовному суверенитету современной России // Военный академический журнал. 2022. № 1 (33). С. 46-50.
2. Байдинов К.Г., Петрий П.В. Сущность и особенности духовного суверенитета современной России // Военный академический журнал. 2021. № 3 (31). С. 146-151.
3. Василенко Н. В., Глухих И.Н. Дадаева Б.Ш. Цифровые экосистемы устойчивого развития экономических субъектов и бизнес-анализ: монография / под ред. М. А. Осипова. СПб.: Изд-во Санкт-Петербургского государственного экономического университета, 2021. 158 с.
4. Володенков С.В. Феномен цифрового суверенитета современного государства в условиях глобальных технологических трансформаций: содержание и особенности // Журнал политических исследований. Том 4. № 4. 2020. С. 3-11.
5. Демяшина В.В. Цифровизация и цифровой суверенитет: к проблеме защиты политической субъектности российского государства (оценки, позиции и социально-философская рефлексия) // Общество: философия, история, культура. 2022. № 8 (100). С. 70-76.
6. Дудин М.Н., Шкодинский С.В., Усманов Д.И. Эволюция научной дефиниции «экономический суверенитет государства» в классических и новейших теориях кризисов (катастроф) // Проблемы рыночной экономики. 2021. № 3. С. 28-46.
7. Ештокин С.В. Сквозные технологии цифровой экономики как фактор формирования технологического суверенитета страны // Вопросы инновационной экономики. 2022. Том 12. № 3.
8. Костин С.А. Международно-правовое обеспечение коллективной безопасности – направление для сотрудничества и интеграции в Европе и на Евразийском пространстве // Международные отношения и общество. 2019. № 3. Т. 1. С. 41-50.
9. Никонов В.А., Воронов А.С., Сажина В.А., Володенков С.В., Рыбакова М.В. Цифровой суверенитет современного государства: содержание и структурные компоненты (по материалам экспертного исследования) // Вестник Томского государственного университета. Философия. Социология. Политология. 2021. № 60. С. 206-216.
10. Пирогов А.И., Иванцов А.В. Феномен информационного суверенитета государства: анализ политологического дискурса // Экономические и социально-гуманитарные исследования. 2021. № 4 (32). С. 138-146.
11. Попова И.М. Проблемы реализации цифровой повестки ЕАЭС // Вестник международных организаций. 2021. Т. 16. № 1. С. 127-141.
12. Сидорова Т.Ю. Международная информационная безопасность: правовые аспекты и деятельность ООН // Сибирский юридический вестник. 2020. № 3. С. 103-108.

13. Сорокова Е.Д. Стратегии реагирования России и Евросоюза на глобальные технологические риски // Научно-аналитический вестник Института Европы РАН. 2022. № 4. С. 18-29.
14. Фальцман В.К. Технологические суверенитеты России. Статистические измерения // Современная Европа. 2018. № 3. С. 83-91.
15. Химченко А.И. О взаимосвязи вопросов обеспечения информационного суверенитета Российской Федерации и формирования цифровой среды доверия // Вестник Университета имени О. Е. Кутафина (МГЮА). 2022. № 4 (92). С. 83-91.
16. Цифровая повестка Евразийского экономического союза до 2025 года: перспективы и рекомендации. Обзор. Группа Всемирного банка, ЕЭК. 2017. 41 с.

References

1. Baidikov K.G. Challenges and threats to the spiritual sovereignty of modern Russia. Military Academic Journal. 2022. No. 1 (33). pp. 46-50. (In Russ).
2. Baidikov K.G., Petri P.V. The essence and features of the spiritual sovereignty of modern Russia. Military Academic Journal. 2021. No. 3 (31). pp. 146-151. (In Russ).
3. Vasilenko N. V., Glukhikh I.N. Dadaeva B.Sh. Digital ecosystems of sustainable development of economic entities and business analysis: monograph / edited by M. A. Osipov. St. Petersburg: Publishing House of St. Petersburg State University of Economics, 2021. 158 p.
4. Volodenkov S.V. The phenomenon of digital sovereignty of the modern state in the context of global technological transformations: content and features. Journal of Political Studies. Volume 4. no. 4. 2020. pp. 3-11. (In Russ).
5. Demyashina V.V. Digitalization and digital sovereignty: towards the problem of protecting the political subjectivity of the Russian state (assessments, positions and socio-philosophical reflection) // Society: philosophy, history, culture. 2022. no. 8 (100). pp. 70-76. (In Russ).
6. Dudin M.N., Shkodinsky S.V., Usmanov D.I. Evolution of the scientific definition of «economic sovereignty of the state» in classical and modern theories of crises (catastrophes). Problems of market economy. 2021. No. 3. pp. 28-46. (In Russ).
7. Eshtokin S.V. End-to-end technologies of the digital economy as a factor in the formation of technological sovereignty of the country. Issues of innovative economics. 2022. Volume 12. no. 3. (In Russ).
8. Kostin S.A. International legal provision of collective security – a direction for cooperation and integration in Europe and in the Eurasian space. International relations and society. 2019. no. 3. Vol. 1. pp. 41-50. (In Russ).
9. Nikonov V.A., Voronov A.S., Sazhina V.A., Volodenkov S.V., Rybakova M.V. Digital sovereignty of the modern state: content and structural components (based on the materials of an expert study). Bulletin of Tomsk State University. Philosophy. Sociology. Political science. 2021. no. 60. pp. 206-216. (In Russ).
10. Pirogov A.I., Ivantsov A.V. The phenomenon of information sovereignty of the state: an analysis of political discourse. Economic and socio-humanitarian studies. 2021. no.4 (32). pp. 138-146. (In Russ).
11. Popova I.M. Problems of implementing the digital agenda of the EAEU. Bulletin of International Organizations. 2021. Vol. 16. no. 1. pp. 127-141. (In Russ).
12. Sidorova T.Y. International information security: legal aspects and activities of the United Nations. Siberian Legal Bulletin. 2020. no. 3. pp. 103-108. (In Russ).
13. Sorokova E.D. Strategies of Russia and the European Union's response to global technological risks. Scientific and Analytical Bulletin of the Institute of Europe of the Russian Academy of Sciences. 2022. no. 4. pp. 18-29. (In Russ).

14. Faltsman V.K. Technological sovereignties of Russia. Statistical measurements. Modern Europe. 2018. no. 3. pp. 83-91. (In Russ).
15. Himchenko A.I. On the relationship between issues of ensuring the information sovereignty of the Russian Federation and the formation of a digital environment of trust. Bulletin of the O. E. Kutafin University (MGUA). 2022. № 4 (92). Pp. 83-91. (In Russ).
16. The digital Agenda of the Eurasian Economic Union until 2025: prospects and recommendations. Review. World Bank Group, ECE. 2017. 41 p. (In Russ).

Information sovereignty of Russia in the digital age

Elena A. Zeveleva

Candidate of Historical Sciences, Professor, Academician of the Russian Academy of Sciences, member of the Union of Writers of Russia, Head of the Department of Humanities
Russian State Geological Exploration University name of Sergo Ordzhonikidze
Moscow, Russia
zevelevaea@mgri.ru

Konstantin A. Kokunov

Candidate of Political Sciences, Associate Professor of the Department of Humanities
Russian State Geological Exploration University name of Sergo Ordzhonikidze
Moscow, Russia
kokunovka@mgri.ru

Short Report

Received 25.01.2023

Revised 01.04.2024

Accepted 30.05.2024

Abstract

This study is devoted to the urgent problem of the information sovereignty of the Russian Federation in the context of the rapid development of digital technologies. The purpose of the study was to study the state of information security in Russia and develop recommendations for strengthening it by reducing dependence on foreign IT companies and developing domestic digital platforms. To achieve this goal, the analysis of statistical data of the Federal Security Service of the Russian Federation on the number of cyber attacks on Russian resources for the period 2016-2022 was carried out, including an assessment of their likely sources and motives. In addition, the market shares of the world's leading providers of cloud services and social networks were considered. As a result of the study, data were obtained confirming Russia's significant dependence on foreign IT companies in the field of cloud computing and social media. A number of recommendations were made to build up their own software, cloud infrastructure and protect the personal data of Russians to ensure the information sovereignty of the country.

Keywords

information sovereignty, cybersecurity, digital technologies, personal data, cloud computing