

Вестник Евразийской науки / The Eurasian Scientific Journal <https://esj.today>

2024, Том 16, № s3 / 2024, Vol. 16, Iss. s3 <https://esj.today/issue-s3-2024.html>

URL статьи: <https://esj.today/PDF/21FAVN324.pdf>

5.2.3. Региональная и отраслевая экономика (экономические науки)

Ссылка для цитирования этой статьи:

Авдийский, В. И. Взаимосвязь цифрового суверенитета и цифрового пространства: новые вызовы и перспективы / В. И. Авдийский, А. В. Иванов, А. В. Царегородцев // Вестник евразийской науки. — 2024. — Т. 16. — № s3. — URL: <https://esj.today/PDF/21FAVN324.pdf>

For citation:

Avdiysky V.I., Ivanov A.V., Tsaregorodtsev A.V. Interrelation of digital sovereignty and digital space: new challenges and prospects. *The Eurasian Scientific Journal*. 2024;16(s3): 21FAVN324. Available at: <https://esj.today/PDF/21FAVN324.pdf>. (In Russ., abstract in Eng.)

Статья подготовлена по результатам исследований, выполненных за счет бюджетных средств по государственному заданию Финансового университета

УДК 338

Авдийский Владимир Иванович

ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации», Москва, Россия
Факультет «Экономики и бизнеса»
Профессор кафедры Экономической безопасности и управления рисками
Доктор юридических наук, профессор
E-mail: VAvdiyskiy@fa.ru
ORCID: <https://orcid.org/0000-0002-6685-3589>

Иванов Анатолий Викторович

ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации», Москва, Россия
Институт цифровых технологий
Главный научный сотрудник
Доктор социологических наук, профессор
E-mail: AIVanov@fa.ru
ORCID: <https://orcid.org/0000-0002-0316-1518>

Царегородцев Анатолий Валерьевич

ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации», Москва, Россия
Институт цифровых технологий
Главный научный сотрудник
Доктор технических наук, профессор
E-mail: Anvtsaregorodtsev@fa.ru
ORCID: <https://orcid.org/0000-0002-8447-3352>

Взаимосвязь цифрового суверенитета и цифрового пространства: новые вызовы и перспективы

Аннотация. Актуальность статьи обусловлена сложившимися проблемами в области взаимосвязи цифрового суверенитета и цифрового пространства. К их числу следует отнести: недостаток единой методологии измерения цифрового суверенитета и его воздействия на цифровое пространство; проблема баланса между обеспечением цифрового суверенитета государства и свободным развитием цифрового пространства для инноваций; неоднозначность в понимании понятий цифрового суверенитета и цифрового пространства среди различных исследователей и практиков; вопросы кибербезопасности и защиты данных в контексте обеспечения цифрового суверенитета и развития цифрового пространства; проблема глобализации и влияния транснациональных корпораций на цифровое пространство при

стремлении государств к обеспечению цифрового суверенитета. Исследование данных проблем обозначили их актуальность, такие как: значимость исследования проблем цифрового суверенитета и цифрового пространства в контексте глобализации и цифровизации в этой связи обеспечение цифрового суверенитета становится ключевым приоритетом для государств в условиях усиления цифровых угроз и кибератак; развитие цифрового пространства требует учета особенностей цифрового суверенитета с целью обеспечения безопасности, свободы и инноваций в интернет-среде; влияние цифрового суверенитета на цифровое пространство оказывает воздействие на экономическое и социальное развитие общества, требуя новых стратегий и политик в области цифровой трансформации. Учитывая эти аспекты, статья об исследовании взаимосвязи цифрового суверенитета и цифрового пространства представляет собой актуальное и важное направление исследований. Новизна статьи заключается в подробном анализе последних исследований и публикаций по теме цифрового суверенитета, который дает основание для новых выводов и рекомендаций. Предложение новых концепций и моделей, которые позволяют глубже понять и проанализировать динамику цифровой трансформации. Оригинальные выводы и рекомендации, вытекающие из исследования влияния цифрового суверенитета на развитие цифрового пространства, которые могут быть полезны для практиков и исследователей. Анализ и представление этих аспектов помогут подчеркнуть новизну статьи и важность ее вклада в академическое и профессиональное сообщество.

Ключевые слова: цифровой суверенитет; цифровое пространство; взаимосвязь цифрового суверенитета и цифрового пространства; информационные данные; информационные системы; информационная инфраструктура; социальные сети; киберугрозы; киберпреступления; кибербезопасность

Введение

Значимость научной статьи по исследованию взаимосвязи цифрового суверенитета и цифрового пространства обусловлена сложившимися в этой области проблемами, как законодательного, так и технического характера. К их числу следует отнести: недостаток единой методологии измерения цифрового суверенитета и его воздействия на цифровое пространство; проблема баланса между обеспечением цифрового суверенитета государства и свободным развитием цифрового пространства для инноваций; неоднозначность в понимании понятий цифрового суверенитета и цифрового пространства среди различных исследователей и практиков; требуют решения вопросы, связанные с кибербезопасностью и защитой данных в контексте обеспечения цифрового суверенитета и развития цифрового пространства; проблема глобализации и влияния транснациональных корпораций на цифровое пространство при стремлении государств к обеспечению цифрового суверенитета. Исследование данных проблем обозначили их актуальность, такие как: значимость изучения проблем цифрового суверенитета и цифрового пространства в контексте глобализации и цифровизации, так как обеспечение цифрового суверенитета становится ключевым приоритетом для государств в условиях усиления цифровых угроз и кибератак; развитие цифрового пространства требует учета особенностей цифрового суверенитета с целью обеспечения безопасности, свободы и инноваций в интернет-среде, что требует новых стратегий и политик в области цифровой трансформации.

Современный этап развития России направлен на дальнейшее совершенствование мероприятий, направленных на обеспечение цифрового суверенитета государства. Подтверждением данному тезису является Послание Президента Российской Федерации Федеральному Собранию от 29 февраля 2024 года,¹ в котором определены стратегические

¹ Президент России. Послание Президента Федеральному Собранию — Режим доступа — <http://www.kremlin.ru/vents/president/transcripts/73585> (дата обращения: 08.06.2024).

задачи развития страны до 2030 года. Президент Российской Федерации поручил подготовить национальный проект по формированию экономики данных, отметив важность перевода экономики, социальной сферы, органов власти на качественно новые принципы работы, а также внедрение управления на основе больших данных, что расширит возможности различных секторов экономики и позволит запускать удобные и эффективные сервисы для граждан. Например, до 2030 года будет поддержано не менее 1 тыс. ИТ-стартапов, создано примерно 2 тыс. решений и продуктов, а также подготовлено более 850 тыс. специалистов.

Выводы и рекомендации: Определение понятия цифрового суверенитета в контексте полномочий и деятельности государственных органов; анализ текущего уровня цифрового суверенитета в органах государственной власти, включающей оценку уровня доступа к технологиям, контроля над данными, кибербезопасности и законодательных механизмов; изучение инновационных процессов, которые могут быть реализованы в цифровом пространстве органов власти на основе использования новых технологий; оценка влияния цифрового суверенитета на возможности реализации инновационных процессов; разработка рекомендаций для улучшения цифрового суверенитета и стимулирования инноваций в цифровом пространстве органов государственной власти.

Цель данной статьи состоит в изучении взаимосвязи цифрового суверенитета и цифрового пространства с целью выявления его последствий и возможных направлений развития в данной области.

Объект исследования — цифровой суверенитет и цифровое пространство.

Предмет исследования — взаимосвязь цифрового суверенитета и цифрового пространства.

1. Методы и материалы

При написании автором использовались следующие методы: анализ научной литературы, законодательства и политических документов по цифровому суверенитету; анализ статистических данных о цифровом пространстве и политике государств в этой области. Методы анализа данных: качественный и количественный анализ полученных статистических данных, сравнительный анализ положительных и негативных аспектов цифрового суверенитета на цифровое пространство; формулирование выводов и рекомендаций на основе полученных результатов и анализа.

Для достижения поставленной цели в работе были поставлены следующие задачи:

1. Проведение анализа существующих концепций цифрового суверенитета и его влияния на цифровое пространство.
2. Исследование роли государства в формировании и использовании цифрового суверенитета.
3. Анализ степени цифрового суверенитета государства в цифровом пространстве и его способность контролировать свои цифровые данные.
4. Определение угроз и вызовов, связанных с цифровым суверенитетом для национальной безопасности и информационной сферы, а также формулирование рекомендаций по развитию политики в области цифрового суверенитета для обеспечения устойчивого и безопасного цифрового пространства.

В основу исследования легли научные труды Г.Р. Камаловой [1], А.В. Скидана, Ю.А. Чипиги, А.А. Исюка [2], И.О. Чистякова [3], Д.В. Кучеренко [4] и т. д.

2. Результаты и обсуждения

Становление и цифровая трансформация государственных информационных систем послужило основой для формирования не только цифрового пространства, но и цифрового суверенитета государства. Например, по результатам аудита государственных информационных систем (2019–2022 годы) проанализированы сведения в отношении 751 федеральных и 3 618 региональных информационных систем. Общая сумма расходов составила 460 миллиардов рублей [5].

Существенными признаками цифрового суверенитета государства является наличие собственных эффективных и высококонкурентных программных продуктов для решения широкого круга задач (национальные операционные системы, инструменты работы с Big Data, программные системы мониторинга, аналитики и прогнозирования, разработки в области искусственного интеллекта и т. д.). В рамках данной парадигмы на первый план выходят технологический потенциал и независимость государства от внешних поставщиков «высоких технологий» [6].

Цифровой суверенитет нами рассматривается как возможность государства контролировать свои цифровые данные, информацию, а также обеспечивать безопасность и защиту цифровых технологий и инфраструктуры. Это понятие включает в себя не только технические аспекты цифровых технологий, но также политические, экономические и социальные аспекты. Законодательство о цифровом суверенитете может включать в себя следующие аспекты: определение прав и обязанностей субъектов цифрового пространства, включая пользователей, компании и государственные органы; регулирование сбора, хранения, обработки и передачи персональных данных с учетом конфиденциальности и безопасности; защита киберпространства от кибератак и киберугроз, а также установление мер по предотвращению и пресечению киберпреступности; обеспечение независимости государства от иностранных цифровых платформ и технологий, привлечение внутренних ресурсов для развития собственного цифрового пространства; развитие и поддержка национальных цифровых инфраструктур, включая цифровые сервисы, интернет-инфраструктуру и цифровые платформы.

Цифровой суверенитет имеет важное значение как для государств, так и для общества в целом. Вот некоторые из ключевых аспектов его значения: цифровой суверенитет позволяет государству обеспечивать защиту информации, данных и критической инфраструктуры от киберугроз и кибератак; способствует развитию отечественной цифровой индустрии; включает защиту прав граждан на конфиденциальность данных, свободу выражения и доступ к информации; способствует развитию образования и науки на основе использования цифровых технологий и доступа к информации. Таким образом, цифровой суверенитет играет важную роль в обеспечении безопасности, экономического развития, защите прав граждан, независимости государств и развитии образования и науки. Он является ключевым элементом суверенитета государства и кибербезопасности.

Например, по результатам исследования отечественной компании Positive Technologies только лишь за 2022–2023 годы существенно увеличилось количество применяемых методов атаки на организации и частные лица на 10 процентных пунктов (рис. 1).

В целях проектирования модели взаимосвязи цифрового суверенитета и цифрового пространства важно исследовать предметную область и структурные элементы цифрового пространства. Отечественные ученые цифровое пространство рассматривают на гуманитарном и технологическом уровнях [7]. Цифровое пространство на технологическом уровне включает в себя цифровую инфраструктуру и цифровые ресурсы.

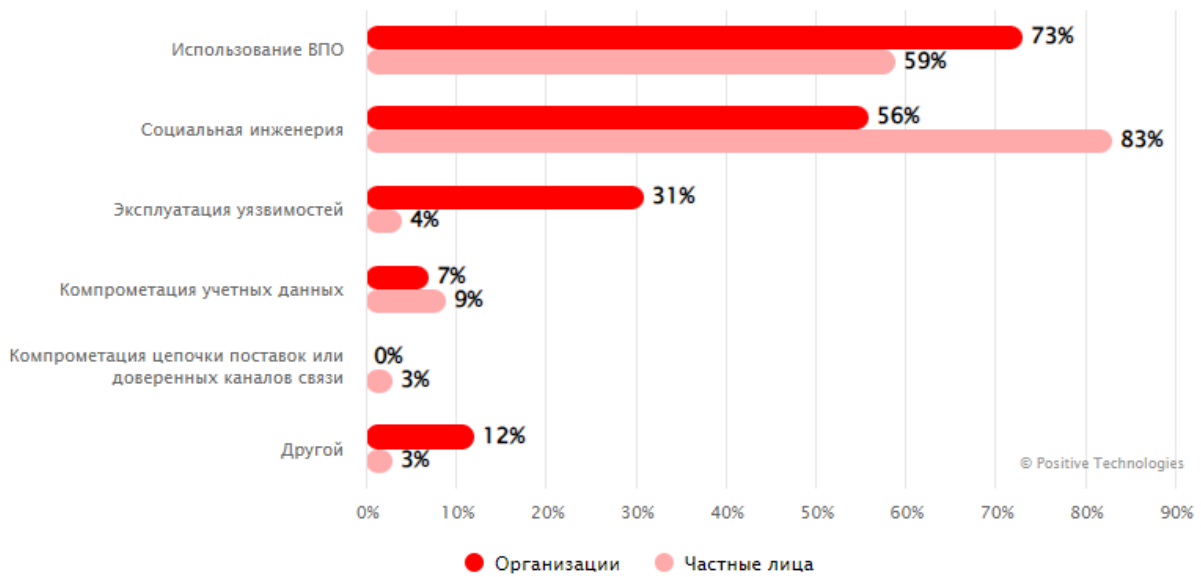


Рисунок 1. Методы атак (доля успешных атак)²

К цифровой инфраструктуре относятся: аппаратные средства, программное обеспечение, телекоммуникации, сети. К цифровым ресурсам — оцифрованные образы физических объектов [8]. Вопросам соотношения понятий «цифровое пространство» и цифровая среда посвящена монография, в которой цифровое пространство рассматривается как цифровая среда [9].

Исходя из вышеназванных научных подходов под цифровым пространством нами понимается пространство, которое интегрирует следующие цифровые типы среды: цифровые данные, цифровую информацию, цифровые информационные системы и сети, цифровые информационные ресурсы, цифровую информационную инфраструктуру, нормы регулирования, механизмы организации и управления (рис. 2).



Рисунок 2. Структурные элементы цифрового пространства (составлено автором)

Важнейшая роль в цифровом пространстве принадлежит цифровым данным, содержащим информацию в цифровой форме. К числу основных характеристик цифровых данных следует отнести их дискретность, прецизионность, хранение и передачу, обработку,

² Positive Technologies. Актуальные киберугрозы: IV квартал 2023 года — Режим доступа — <https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2023-q4/> (дата обращения: 08.06.2024).

воспроизводство, защиту и масштабируемость. Исходя из вышеперечисленных характеристик цифровые данные должны быть представлены в дискретной форме и иметь высокую степень прецизионности; сохранены на компьютерах, серверах или облачных хранилищах и переданы через интернет или локальные сети, а также защищены с помощью различных механизмов шифрования и контроля доступа.

Под цифровой информацией нами понимается информация, представленная в виде цифр, т. е. чисел, которые могут быть обработаны и переданы электронными устройствами. К числу общих элементов структуры цифровой информации относятся: единицы цифровой информации (бит, байт); различные блоки, которые могут иметь различные размеры в зависимости от конкретных требований и протоколов; метаданные, определяющие дополнительную информацию, которая описывает основные данные, такие как имя файла, размер, тип, дата создания. Они являются частью структуры цифровой информации.³

Сравнительный анализ цифрового пространства в Российской Федерации представлен на рисунке 3.



Рисунок 3. Сравнительный анализ цифрового пространства (составлено автором на основе [10])

Сравнительный анализ цифрового пространства позволяет сделать вывод о том, что в настоящее время Российская Федерация по всем перечисленным показателям незначительно отстает от стран ЭС. Например, по данным DataReportal⁴ состояние цифрового пространства в Российской Федерации в 2024 году характеризуется следующими показателями: в Российской Федерации насчитывалось 130,4 миллиона пользователей Интернета (проникновение интернета составляет 90,4 %); насчитывается 106,0 миллиона пользователей социальных сетей (73,5 % от общей численности населения); активировано 219,8 миллиона подключений к сотовой мобильной связи (152,5 % от общей численности населения); социальными сетями в России пользовались 91,50 миллиона пользователей в возрасте 18 лет и старше (81,3 % от общей базы пользователей Интернета в России); 54,8 % пользователей социальных сетей в России составляют женщины, в то время как 45,2 % составляют мужчины.⁵

³ Электронно-библиотечная система Лань. Введение в цифровые гуманитарные исследования: Учебно-методическое пособие — Режим доступа — <https://e.lanbook.com/book/283778?category=43749> (дата обращения: 08.06.2024).

⁴ Kepios. ALL THE NUMBERS YOU NEED — Режим доступа — <https://datareportal.com/> (дата обращения: 08.06.2024).

⁵ ResearchGate GmbH. Цифровая экономика: 2022 — Режим доступа — https://www.researchgate.net/publication/357968466_Cifrova_ekonomika_2022 (дата обращения: 08.06.2024).

В научных работах Короткова А.В.⁶, Карапаева О.В.⁷, Меняева А.А.⁸ проанализированы проблемы и недостатки современного состояния цифровой информации, к числу которых можно отнести: уязвимость к потере данных, если цифровая информация хранится на физическом носителе; необходимость регулярного обновления оборудования и программного обеспечения; проблемы с безопасностью цифровой информации, так как она может быть подвержена угрозам безопасности, таким как хакерские атаки, взломы и вирусы; потеря аутентичности поскольку цифровая информация может быть изменена или поддельна, что делает ее менее надежной, особенно в случае, когда невозможно проверить ее источник или целостность.

На наш взгляд, в целях оптимизации цифровой информации следует принять следующие меры:

1. Важно разработать эффективную систему хранения и организации цифровой информации. Это может включать использование структурированных папок и файлов, надлежащую маркировку и каталогизацию данных. Также рекомендуется резервировать данные и создавать регулярные копии информации для предотвращения потери данных при сбоях или ошибке.
2. Одним из способов оптимизации цифровой информации является сжатие данных. Существуют различные алгоритмы сжатия данных, которые позволяют уменьшить размер файлов без потери информации. Это может помочь увеличить пропускную способность сети и экономить дисковое пространство.
3. Для оптимизации цифровой информации важно улучшить скорость доступа к данным. Это может быть достигнуто с помощью оптимизации сетевой инфраструктуры, повышения производительности компьютерных систем, увеличения пропускной способности хранилищ данных и применения кэширования данных.
4. Цифровая информация должна быть защищена от угроз безопасности. Это может включать установку средств защиты данных, таких как антивирусное программное обеспечение и межсетевые экраны, регулярные обновления программного обеспечения, а также обучение пользователей правилам безопасности данных и паролей.
5. Для улучшения доступности и использования цифровой информации важно создать структурированную систему метаданных. Это поможет пользователям быстрее находить и анализировать нужные данные. Примеры метаданных включают название файла, дату создания, автора и теги.

⁶ Коротков, А.В. Преодоление цифрового неравенства как информационная стратегия современного общества: специальность 10.01.10 «Журналистика»: автореферат диссертации на соискание ученой степени кандидата филологических наук / Коротков Андрей Викентьевич. — Москва, 2003. — 26 с. — EDN NJPWMD.

⁷ Карапаев, О.В. Влияние цифровизации на процесс общественного воспроизводства: специальность 08.00.01 «Экономическая теория»: диссертация на соискание ученой степени кандидата экономических наук / Карапаев Олег Валерьевич, 2022. — 165 с. — EDN PSINPI.

⁸ Миняев, А.А. Методика оценки эффективности системы защиты территориально-распределенных информационных систем: специальность 05.13.19 «Методы и системы защиты информации, информационная безопасность»: автореферат диссертации на соискание ученой степени кандидата технических наук / Миняев Андрей Анатольевич. — Санкт-Петербург, 2021. — 22 с. — EDN RARSLT.

6. Автоматизация и оптимизация процессов обработки данных могут существенно повысить эффективность использования цифровой информации. Технологии, такие как искусственный интеллект и машинное обучение, могут использоваться для автоматизации задач обработки данных и анализа.
7. Важно обучать пользователей основам цифровой грамотности и эффективного использования цифровой информации. Это поможет им сократить время, затрачиваемое на поиск и обработку данных, а также повысит общую производительность и эффективность.
8. Процесс утилизации и переработки цифровой информации поможет минимизировать негативное влияние цифрового следа на окружающую среду. Разработка устойчивых методов хранения и утилизации данных, а также регулярная переработка устаревших или ненужных данных, помогут снизить потребление ресурсов и уменьшить количество электронных отходов.

Цифровые информационные системы широко используются в деятельности органов государственной власти в части оказания различных государственных и муниципальных услуг. Основные компоненты системы цифровой информации в государственном управлении России регулируются Федеральным законом от 27.07.2006 N 149-ФЗ (ред. от 12.12.2023) «Об информации, информационных технологиях и о защите информации». К числу таких компонентов системы относятся: государственные информационные системы (далее ГИС); муниципальные информационные системы; иные информационные системы.

Количество ГИС Федеральных министерств, служб, агентств, бюджетных учреждений представлен в таблице 1.

Таблица 1

Перечень и количество государственных информационных систем в федеральных министерствах, службах и агентствах

№ п/п	Наименование оператора ФГИС — заявителя	Кол-во
1	Федеральные министерства	123
2	Федеральные службы	106
3	Федеральные агентства	61
4	Органы государственной власти	14
5	Федеральные государственные унитарные предприятия	33
6	Всего	337

Источник: анализ авторов по количеству государственных информационных систем в федеральных министерствах, службах и агентствах

Общее количество государственных информационных систем составляет — 337, которые распределены следующим образом: федеральные министерства — 123 (значительное количество представлено в следующих министерствах: Минэкономразвития России — 31; Минкомсвязи России — 16; Минсельхоз России — 10. Федеральные службы — 106 (Федеральная служба по надзору в сфере транспорта — 20; Федеральная служба государственной регистрации, кадастра и картографии — 15; Федеральная служба по труду и занятости — 8). Федеральные агентства — 61 (Федеральное медико-биологическое агентство — 10; Федеральное агентство воздушного транспорта — 12; Федеральное агентство водных ресурсов — 11). Органы государственной власти — 14; федеральные государственные унитарные предприятия — 33.

В работах Камаловой Г.К., Кучеренко Д.В. проанализирована деятельность государственных информационных систем и были выявлены их недостатки:

1. Государственные информационные системы зачастую неэффективны и не в полной мере обеспечивают достаточный уровень продуктивности. Это может быть вызвано ограниченными ресурсами, сложными процедурами, бюрократией и недостаточной поддержкой со стороны правительства.
2. Важная информация, хранящаяся в государственных информационных системах, часто подвергается риску хакерских атак и внутренних угроз, таких как внутренние утечки данных или несанкционированный доступ к информации. Это может привести к серьезным последствиям, включая утечку конфиденциальной информации и нарушение прав граждан.
3. Многие государственные информационные системы работают изолированно друг от друга, что затрудняет обмен и интеграцию данных между различными ведомствами. В результате возникают дублирующиеся данные, информационные пробелы и сложности в обеспечении своевременного и точного доступа к информации.
4. Значительная часть государственных информационных систем характеризуется сложным интерфейсом и отсутствием интуитивно понятных функций. Это создает трудности для пользователей при работе с системой и требует дополнительного обучения и времени для освоения.
5. Государственные информационные системы зачастую не способны легко масштабироваться и адаптироваться к изменяющимся потребностям и требованиям. Это может ограничивать возможности улучшения и модернизации системы в будущем.
6. Разработка и поддержка государственных информационных систем может требовать значительных финансовых ресурсов. Нередко государственные проекты связаны с перерасходами бюджета, срывами сроков и низким уровнем качества.
7. Государственные информационные системы не всегда обеспечивают активное включение граждан и других заинтересованных сторон. Это может снижать прозрачность и уровень доверия к системе, а также уменьшать возможность обратной связи и улучшений.
8. Во многих случаях отсутствуют единые стандарты и подходы к разработке и управлению государственными информационными системами. Это может приводить к фрагментации и несовместимости систем, а также затруднять обмен данными и сотрудничество между различными органами государственной власти.

В федеральных органах государственной власти России существуют различные *сети цифровой информации*, которые используются для передачи данных и обеспечения коммуникации. К ним относятся:

1. Государственная телекоммуникационная сеть — комплекс коммуникационных сетей и систем, используемых для передачи данных и голосовой связи между органами государственной власти на федеральном, региональном и муниципальном уровнях.
2. Многие федеральные органы используют собственные высокоскоростные и локальные сети для внутренней коммуникации и обмена данными. Они обеспечивают связь между различными узлами сети (компьютеры, серверы, терминалы) и позволяют обеспечить безопасность и защиту данных.

3. Интранет, который представляет собой внутреннюю сеть, позволяющая организациям обмениваться информацией, ресурсами и сервисами внутри своих структурных подразделений. Он обеспечивает доступ к документам, базам данных, электронной почте, внутренним новостям и другой информации для сотрудников.
4. Системы электронного документооборота используются для обмена документами и информацией в электронной форме между организациями и сотрудниками внутри органов государственной власти.

Цифровые информационные ресурсы в федеральных органах государственной власти России могут включать: электронные базы данных; веб-порталы; электронные системы документооборота; электронные архивы; коммуникационные системы; информационно-аналитические системы; электронные сервисы. В трудах Скидана А.В., Чипиги Ю.А., Исюка А.А., Чистякова И.О. проведен анализ информационных ресурсов в деятельности органов государственной власти.

Цифровая информационная инфраструктура — это комплексный набор информационных технологий, ресурсов и процессов, необходимых для обеспечения передачи, хранения, обработки и управления данными в цифровой форме. Основные структурные элементы цифровой информационной инфраструктуры включают: *сетевую инфраструктуру* (Интернет, локальные сети, облачные вычисления, сервера и телекоммуникационное оборудование); *компьютерное оборудование* (компьютеры, ноутбуки, планшеты, мобильные устройства и другие устройства для обработки и хранения данных); *программное обеспечение* (операционные системы, прикладные программы, базы данных, аналитические инструменты и другие программы для обработки и управления данными); *хранилища данных* (цифровые хранилища, облачные хранилища, базы данных и другие механизмы для хранения информации); *информационную безопасность* (системы защиты данных, защита от кибератак, шифрование, аутентификация и другие меры, обеспечивающие конфиденциальность и сохранность данных); *управление информационными ресурсами* (процессы управления данными, мониторинг производительности информационных систем, планирование ресурсов цифровой инфраструктуры).

Некоторые из недостатков цифровой информационной инфраструктуры в органах государственной власти включают:

1. Органы государственной власти могут столкнуться с угрозами кибербезопасности, такими как хакерские атаки, вирусы и вредоносное ПО. Недостатки в защите данных могут привести к утечкам конфиденциальной информации и нарушению безопасности.
2. В разных органах государственной власти могут использоваться различные информационные системы и программное обеспечение, что затрудняет совместимость и обмен информацией между ними.
3. Не всегда в органах государственной власти есть достаточно опытные и квалифицированные специалисты по работе с цифровыми технологиями, что может привести к недостаточной подготовке кибербезопасности, неэффективному использованию существующих ресурсов и неспособности адаптироваться к быстро меняющимся технологиям.
4. Обработка и хранение большого объема данных требует эффективной системы управления информационными ресурсами, так как недостаточная организация данных и отсутствие четкой политики по управлению данными могут привести к потере информации или некорректному принятию решений.

5. С появлением новых технологий, таких как искусственный интеллект, интернет вещей и блокчейн, органы государственной власти сталкиваются с новыми угрозами и вызовами в области кибербезопасности и цифровой информационной инфраструктуры.
6. Не все регионы России имеют одинаковую доступность и инфраструктуру для использования цифровых технологий, данное обстоятельство может создавать неравенство в доступе граждан к государственным услугам и ограничивать эффективность внедрения цифровых систем.
7. Цифровые системы могут быть подвержены техническим сбоям и отказам, что может привести к проблемам в работе органов власти и недоступности услуг для граждан.
8. Использование цифровых технологий в органах власти требует особого внимания к вопросам конфиденциальности и защите персональных данных граждан. Нарушения конфиденциальности или утечки данных могут нанести ущерб доверию граждан к государству.

Социальные сети представляют собой платформы и веб-сайты, которые позволяют пользователям создавать профили, обмениваться информацией, коммуницировать друг с другом и взаимодействовать с различными контентом. В органах государственной власти России социальные сети играют важную роль как инструмент общения и взаимодействия с гражданами и предприятиями. Особенности социальных сетей в органах государственной власти России включают: органы государственной власти используют социальные сети для распространения информации о своей деятельности, проектах, программах и событиях. Это позволяет гражданам быть в курсе последних новостей и изменений; социальные сети предоставляют платформу для обратной связи и диалога между органами власти и гражданами. Граждане могут задавать вопросы, высказывать свои мнения и предлагать идеи, а органы государственной власти могут отвечать на них и учитывать их мнения; публикация информации на социальных сетях органов государственной власти России способствует прозрачности и открытости деятельности. Граждане имеют возможность получать доступ к информации о решениях, порядке и процедурах, а также о работе структур государственной власти; социальные сети позволяют гражданам активно участвовать в обсуждении и принятии решений. Они могут принимать участие в опросах, онлайн-консультациях и взаимодействовать с представителями органов власти; органы государственной власти России используют социальные сети для мониторинга и анализа общественного мнения. Это может помочь понять настроения и предпочтения граждан, а также принять более обоснованные решения.

В то же время использование социальных сетей в органах государственной власти России сопряжено с определенными рисками, такими как дезинформация, недостоверная информация, кибератаки и утечка конфиденциальных данных. Поэтому органы власти должны принимать меры безопасности для защиты информации и обеспечения надежности использования социальных сетей. В целом, использование социальных сетей в органах государственной власти России способствует улучшению коммуникации с гражданами, повышению прозрачности и эффективности работы, а также способствует активному участию граждан в принятии решений.

Рассмотренные нами структурные элементы цифрового пространства позволили сформировать базисные классификаторы цифрового пространства, а именно:

1. *Инфраструктурные классификаторы* — компоненты и сетевая структура цифрового пространства, такие как сети передачи данных, сервера, облачные хранилища, устройства и технологии связи.

2. *Информационные классификаторы*, описывающие данные, которые передаются и хранятся в цифровом пространстве, такие как тексты, изображения, аудио и видеофайлы, метаданные и другая информация.
3. *Пользовательские классификаторы*, рассматривающие участников цифрового пространства, их роли, поведение, цели и мотивации, а также взаимодействие между ними.
4. *Технологические классификаторы*, раскрывающие используемые технологии и инструменты в цифровом пространстве, такие как программное обеспечение, приложения, алгоритмы, протоколы и стандарты.
5. *Социальные классификаторы*, описывающие социальные взаимодействия и отношения в цифровом пространстве, такие как коммуникация, коллаборация, конфликты, сетевые сообщества, влияние и власть.
6. *Экономические классификаторы*, включающие экономические аспекты цифрового пространства, такие как модели бизнеса, монетизация контента, реклама, электронная коммерция и денежные транзакции.
7. *Правовые классификаторы*, регулирующие правовые аспекты цифрового пространства, такие как права и обязанности пользователей, авторские права, конфиденциальность данных, защита личной информации и право на доступ к информации.
8. *Управленческие классификаторы*, включающие набор инструментов, связанных с повышением эффективности управленческой деятельности.

В общем виде базисные классификаторы цифрового пространства представлены на рисунке 4.

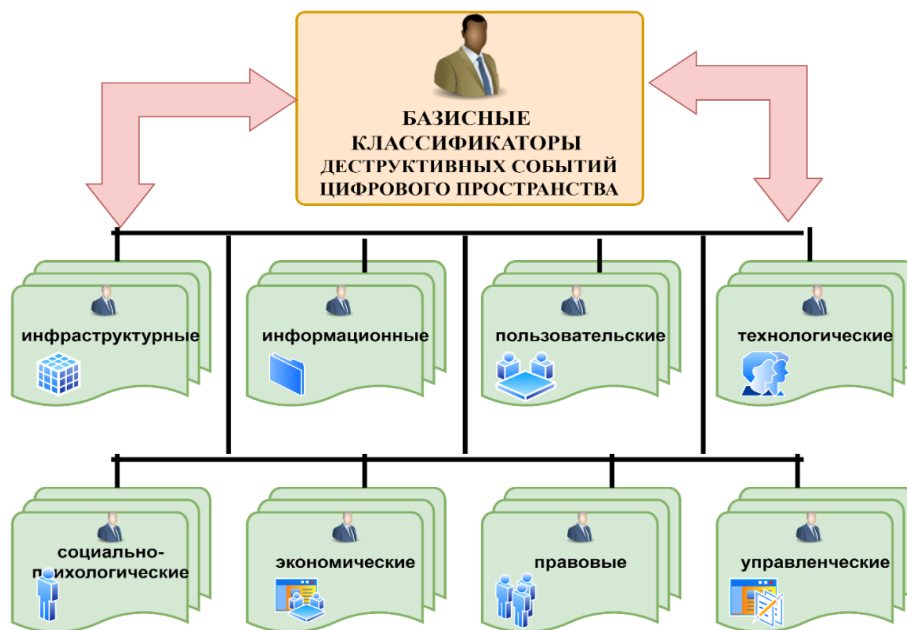


Рисунок 4. Базисные классификаторы цифрового пространства (составлено автором)

Инфраструктурные классификаторы цифрового пространства включает в себя следующие элементы: *Облачные сервисы*: хранилища данных, вычислительные ресурсы, облачные сервисы, которые позволяют компаниям создавать и разворачивать приложения и решения в облаке; *Сетевая инфраструктура*: сетевое оборудование, коммуникационные

каналы, протоколы и другие средства, необходимые для обеспечения связности и доступности систем и сервисов в цифровом пространстве; *Центры обработки данных (ЦОД)*: специализированные помещения, оборудованные вычислительным оборудованием, хранилищами данных, системами безопасности и другими средствами, обеспечивающими работу ИТ-инфраструктуры; *Виртуализация серверов*, хранилищ данных, сетевых ресурсов и другие технологии, позволяющие оптимизировать использование ресурсов и упростить управление инфраструктурой; *Мониторинг и управление ресурсами*: средства для мониторинга и управления вычислительными ресурсами, сетевыми устройствами, хранилищами данных и другими элементами инфраструктуры; *Безопасность*: средства для обеспечения безопасности информации, средств защиты от кибератак, аутентификации пользователей, шифрования данных и другие меры для обеспечения целостности и конфиденциальности информации; *Контейнеризация*: технологии контейнеризации, которые позволяют упаковать приложения и их зависимости в контейнеры для более эффективного развертывания и управления приложениями.

Информационные классификаторы цифрового пространства включает следующие структурные элементы: *Базы данных*: структурированные данные, которые хранятся и обрабатываются компьютерной программой для обеспечения доступа к информации; *Системы управления данными (СУБД)*: программное обеспечение, позволяющее организовывать и управлять базами данных, обеспечивая доступ к данным, их хранение, поиск, обновление и удаление; *Информационные ресурсы*: это набор данных, документов, отчетов, аналитических материалов и других информационных ресурсов, которые используются для принятия управленческих решений и выполнения бизнес-процессов; *Аналитические инструменты*: инструменты для анализа данных, создания отчетов, визуализации информации, прогнозирования трендов и показателей, а также другие средства для обработки данных и выявления закономерностей; *Интеграция данных*: методы и технологии для интеграции данных из различных источников, структурирования их, устранения дубликатов, обеспечения единой модели данных для всей организации; *Средства защиты информации*: обеспечивают защиту данных от несанкционированного доступа, искажения, утраты, а также обеспечивают конфиденциальность и целостность информации; *Системы управления контентом (СМС)*: обеспечивают управление и хранение контентом, включая тексты, изображения, видео, аудиофайлы, документы и другие мультимедийные материалы. Эти элементы информационного классификатора цифрового пространства обеспечивают организациям доступ к необходимой информации, обработку данных, анализ и использование информационных ресурсов для достижения поставленных целей и задач.

Содержание *пользовательских классификаторов цифрового пространства* включает следующие элементы: *Профиль пользователя* — информация о пользователе, его личные данные, настройки аккаунта и привязанные социальные сети; *Личный кабинет* — функционал для управления аккаунтом, подписками, платежами и настройками; *Новости и обновления* — раздел с последними новостями и обновлениями в цифровом пространстве, а также актуальной информацией о сервисе; *Каталог контента* — список доступного контента, такой как видео, статьи, аудиозаписи и прочее, с возможностью поиска и фильтрации; *Персонализированные рекомендации* — рекомендации контента на основе предпочтений и истории активности пользователя; *Онлайн-чат и обратная связь* — возможность общения с другими пользователями, а также обратная связь с администрацией сервиса; *События и мероприятия* — информация о предстоящих событиях, вебинарах, конференциях и других мероприятиях.

Содержание *технологических классификаторов цифрового пространства* может включать следующие элементы: интерфейс пользователя; алгоритмы обработки и анализа данных; базы данных; функциональные модули и компоненты; логика работы модуля; механизмы безопасности и защиты данных. Структурные элементы *социально-психологического*

классификатора цифрового пространства включают: *профили и аккаунты пользователей* — функциональность для взаимодействия и обмена информацией между участниками; *форумы, чаты, блоги* и другие инструменты для общения и обмена мнениями; группы и сообщества с общими интересами; *инструменты аналитики и статистики* для измерения социального воздействия; *системы управления* обратной связью и предложениями от участников; *модули для обучения и развития* социальных навыков и компетенций.

Структурные элементы *экономических классификаторов* цифрового пространства могут быть организованы следующим образом: веб-сайт, мобильное приложение, электронный магазин или платежная система; базы данных и хранилища информации для хранения и обработки данных о клиентах, заказах, товарах и услугах; отчетность и аналитические отчеты для оценки эффективности и планирования развития бизнеса; системы безопасности и защиты данных для обеспечения конфиденциальности и целостности информации; планирование для оптимизации использования ресурсов и улучшения операционной эффективности.

Структурные элементы *правовых классификаторов* цифрового пространства: *нормативные акты и законы*, регулирующие деятельность в цифровой среде; *политики и правила компаний* по обработке и защите данных пользователей; *лицензионные соглашения и договоры* об использовании цифровых ресурсов; *пользовательские соглашения* и правила использования онлайн-платформ; *механизмы обеспечения безопасности* и защиты прав субъектов в цифровой среде; *процедуры разрешения споров* и обращений от пользователей; контроль и надзор со стороны регулирующих органов по соблюдению законодательства в цифровом пространстве.

Управленческие классификаторы цифрового пространства включают: *инструменты для анализа и мониторинга данных* (панели управления, дэшборды, отчеты, инструменты для визуализации и анализа данных); *инструменты для управления процессами* (системы управления проектами, задачами, рабочим временем и другими бизнес-процессами); *инструменты для коммуникации и совместной работы* (чаты, видеоконференции, обмен документами и другие средства для совместной работы и общения с коллегами); *инструменты для управления ресурсами* (CRM-системы, учетные программы, системы управления ресурсами); *инструменты для анализа рынка и конкурентов* (мониторинг конкурентов, анализ трендов на рынке, прогнозирование спроса); *инструменты для управления персоналом* (системы управления персоналом, обучения и развития сотрудников, мотивации и удержания персонала).

На цифровое пространство существенное влияние оказывают деструктивные события, представляющие некоторые *инциденты или события, которые могут нанести ущерб информационной безопасности и цифровым ресурсам, таким как компьютерные системы, сети, электронные устройства, программное обеспечение и данные*. Эти события обычно вызываются злоумышленниками или киберпреступниками, которые используют различные методы и техники для нарушения, взлома или уничтожения данных, системы или инфраструктуры.

Целью злоумышленников может быть получение конфиденциальной информации, финансовая выгода, повреждение репутации организации или нарушение нормального функционирования системы с применением следующих деструктивных способов: запуск вирусов и вредоносного программного обеспечения; хакерские атаки и фишинг; DDoS-атаки и кибершпионаж; мошенничество и кражу данных; использование уязвимостей программного обеспечения и многое другое.

Несмотря на многочисленные преимущества цифрового развития, существуют и ключевые вызовы, которые могут возникнуть в сфере цифрового суверенитета и цифрового пространства в органах государственной власти.

Некоторые из них включают:

1. Угрозы кибербезопасности становятся все более сложными и разнообразными, что требует органам власти постоянного мониторинга и защиты цифровых данных от кибератак и киберпреступников.
2. Органы власти могут столкнуться с проблемой зависимости от иностранных технологий и поставщиков, что может негативно сказаться на цифровом суверенитете и безопасности данных.
3. Различные органы власти могут использовать разные цифровые системы и хранить данные в различных форматах, что затрудняет эффективное взаимодействие и обмен информацией между ними.
4. Низкий уровень цифровой грамотности у сотрудников и граждан может затруднить успешную реализацию цифровых проектов и обеспечение безопасности цифровых данных.
5. Быстрое развитие цифровых технологий требует постоянного обновления законодательства и регулирования в области цифрового пространства, чтобы обеспечить защиту данных, приватность граждан и эффективное управление информацией.

Для успешного преодоления этих вызовов органы власти должны активно работать над укреплением цифрового суверенитета, развитием безопасных цифровых систем и повышением уровня цифровой грамотности у своих сотрудников и общества в целом. Кроме того, важным фактором является законодательная база и правовые нормы в области цифрового суверенитета государства. Чтобы обеспечить цифровой суверенитет, необходимо иметь соответствующие законы и нормы, которые защищают данные и права пользователей в цифровом пространстве. Поэтому важно разрабатывать и внедрять такие законы, которые поддерживают цифровой суверенитет и обеспечивают безопасность и конфиденциальность данных.

Выводы

Для исследования взаимосвязи между цифровым суверенитетом и инновационными процессами в цифровом пространстве органов государственной власти можно провести следующие шаги:

1. Определение понятия цифрового суверенитета в контексте полномочий и деятельности государственных органов контролировать свои цифровые данные, информацию и коммуникации, обеспечивая при этом безопасность и конфиденциальность.
2. Анализ текущего уровня цифрового суверенитета в органах государственной власти, включающей оценку уровня доступа к технологиям, контроля над данными, кибербезопасности и законодательных механизмов.
3. Изучение инновационных процессов, которые могут быть реализованы в цифровом пространстве органов власти на основе использования новых технологий, улучшения качества обслуживания граждан и многое другое.
4. Оценка влияния цифрового суверенитета на возможности реализации инновационных процессов. Исследование может определить, насколько эффективно государственные органы могут использовать свои цифровые ресурсы и данные для внедрения инноваций.

5. Разработка рекомендаций для улучшения цифрового суверенитета и стимулирования инноваций в цифровом пространстве органов государственной власти. Эти рекомендации могут включать в себя предложения по улучшению кибербезопасности, внедрению новых технологий и обучению сотрудников.

Из проведенного исследования можно сделать следующие выводы:

1. Цифровой суверенитет играет значительную роль в развитии цифрового пространства в органах государственной власти. Он обеспечивает сохранность информации, защиту от киберугроз и обеспечивает независимость в области цифровых технологий.
2. Цифровой суверенитет способствует развитию цифровой экономики и повышению эффективности работы органов государственной власти за счет внедрения современных цифровых технологий.
3. Органы государственной власти должны активно работать над развитием цифровой культуры и поддержкой инноваций в цифровой сфере для улучшения качества предоставляемых государственных услуг.
4. Важно учитывать особенности цифрового суверенитета при разработке законодательства и стратегий по развитию цифрового пространства в органах государственной власти.

Исходя из этих выводов, можно сформулировать некоторые рекомендации для совершенствования стратегий цифрового развития и обеспечения цифрового суверенитета в органах государственной власти:

1. Разработка и утверждение специальной стратегии цифрового развития, которая бы включала в себя меры по укреплению цифрового суверенитета. В этой стратегии необходимо учитывать специфику информационной безопасности и защиты данных органов государственной власти.
2. Внедрение современных технологий защиты данных и информационной инфраструктуры для обеспечения цифрового суверенитета. Регулярное обновление систем защиты, мониторинг уязвимостей и обучение сотрудников вопросам кибербезопасности.
3. Поддержка цифровой культуры и обучение сотрудников органов государственной власти в области цифровых технологий. Обеспечение доступа к обучающим программам и курсам по цифровой грамотности.
4. Развитие сотрудничества с частным сектором и академическими учреждениями для обмена опытом и передачи передовых практик в области цифрового развития и обеспечения цифрового суверенитета.
5. Проведение регулярных аудитов и проверок цифровой инфраструктуры органов государственной власти с целью выявления слабых мест и устранения уязвимостей.

Эти рекомендации могут помочь органам государственной власти улучшить свою работу в области цифрового развития и обеспечения цифрового суверенитета.

ЛИТЕРАТУРА

1. Камалова, Г.Р. Государственные информационные системы России: анализ успешных практик / Г.Р. Камалова // Экономика и управление: научно-практический журнал. — 2022. — № 3(165). — С. 32–35. — DOI 10.34773/EU.2022.3.6. — EDN CQNBLL.
2. Скидан, А.В. Цифровизация как фактор повышения результативности государственного управления: проблемы и направления развития / А.В. Скидан, Ю.А. Чипига, А.А. Исюк // Государственное и муниципальное управление. Ученые записки. — 2021. — № 1. — С. 71–76. — DOI 10.22394/2079-1690-2021-1-1-71-76. — EDN BILLNE.
3. Чистяков, И.О. Актуальные проблемы применения цифровых технологий в деятельности органов государственной власти / И.О. Чистяков // Молодой ученый. — 2023. — № 18(465). — С. 384–387. — EDN DNNKRF.
4. Кучеренко, Д.В. Комплексная методика поддержки принятия решений при планировании работ по совершенствованию региональной инфраструктуры государственных информационных систем / Д.В. Кучеренко // Вестник Воронежского института ФСИН России. — 2021. — № 3. — С. 87–95. — EDN YQVBMV.
5. Иванов, А.В. Становление и институционализация государственных информационных систем / А.В. Иванов // Вектор научной мысли. — 2023. — № 3(3). — С. 103–108. — EDN XMAPZW.
6. Цифровой суверенитет современного государства: содержание и структурные компоненты (по материалам экспертного исследования) / В.А. Никонов, А.С. Воронов, В.А. Сажина [и др.] // Вестник Томского государственного университета. Философия. Социология. Политология. — 2021. — № 60. — С. 206–216. — DOI 10.17223/1998863X/60/18. — EDN PCWPLD.
7. Ячменева, В.М. Цифровое пространство как необходимое и достаточное условие цифровизации экономики / В.М. Ячменева, Е.Ф. Ячменев // Baikal Research Journal. — 2020. — Т. 11, № 3. — С. 2. — DOI 10.17150/2411-6262.2020.11(3).2. — EDN SNLTPY.
8. Сидорова, А.П. Понятие цифрового пространства и его характеристики. Возможности и угрозы использования цифрового пространства / А.П. Сидорова // Научный диалог: Молодой ученый: сборник научных трудов по материалам XXVIII международной научной конференции, Санкт-Петербург, 22 мая 2020 года / Международная Объединенная Академия Наук. — Санкт-Петербург: Международная Объединенная Академия Наук, 2020. — С. 48–55. — DOI 10.18411/spc-22-05-2020-11. — EDN PQCULK.
9. Информационная безопасность цифрового пространства / И.Л. Андреевский, И.Н. Васильева, И.Е. Галактионов [и др.]. — Санкт-Петербург: Санкт-Петербургский государственный экономический университет, 2019. — 155 с. — ISBN 978-5-7310-4465-3. — EDN VUCWDT.
10. Ураев, А.В. Современные проблемы информатизации и перспективы преодоления цифрового неравенства в России / А.В. Ураев // Молодой ученый. — 2023. — № 2(449). — С. 14–17. — EDN NMKAYD.

Avdiysky Vladimir Ivanovich

Financial University under the Government of the Russian Federation, Moscow, Russia
E-mail: VAvdiyskiy@fa.ru
ORCID: <https://orcid.org/0000-0002-6685-3589>

Ivanov Anatoly Viktorovich

Financial University under the Government of the Russian Federation, Moscow, Russia
E-mail: AIvanov@fa.ru
ORCID: <https://orcid.org/0000-0002-0316-1518>

Tsaregorodtsev Anatoly Valerievich

Financial University under the Government of the Russian Federation, Moscow, Russia
E-mail: Anvtsaregorodtsev@fa.ru
ORCID: <https://orcid.org/0000-0002-8447-3352>

Interrelation of digital sovereignty and digital space: new challenges and prospects

Abstract. The relevance of the article is due to the existing problems in the field of the relationship between digital sovereignty and digital space. These include: the lack of a unified methodology for measuring digital sovereignty and its impact on the digital space; the problem of balance between ensuring the digital sovereignty of the state and the free development of the digital space for innovation; ambiguity in understanding the concepts of digital sovereignty and digital space among various researchers and practitioners; issues of cybersecurity and data protection in the context of ensuring digital sovereignty and development of the digital space; the problem of globalization and the influence of transnational corporations on the digital space while states strive to ensure digital sovereignty. The study of these problems indicated their relevance, such as: the importance of studying the problems of digital sovereignty and digital space in the context of globalization and digitalization in this regard, ensuring digital sovereignty is becoming a key priority for states in the face of increasing digital threats and cyber attacks; the development of the digital space requires taking into account the features of digital sovereignty in order to ensure security, freedom and innovation in the Internet environment; The impact of digital sovereignty on the digital space has an impact on the economic and social development of society, requiring new strategies and policies in the field of digital transformation. Considering these aspects, an article on the study of the relationship between digital sovereignty and digital space represents a relevant and important direction of research. The novelty of the article lies in the detailed analysis of recent research and publications on the topic of digital sovereignty, which provides the basis for new conclusions and recommendations. Proposing new concepts and models that allow for a deeper understanding and analysis of the dynamics of digital transformation. Original conclusions and recommendations arising from the study of the influence of digital sovereignty on the development of the digital space, which may be useful for practitioners and researchers. Analyzing and presenting these aspects will help highlight the novelty of the article and the importance of its contribution to the academic and professional community. The purpose of the article is to study the relationship between digital sovereignty and digital space in order to identify its consequences and possible directions for development in this area. Research objectives: analysis of existing concepts of digital sovereignty and its impact on the digital space; study of the role of the state in the formation and use of digital sovereignty; analysis of the degree of digital sovereignty of the state in the digital space and its ability to control its digital data; identifying threats and challenges related to digital sovereignty for national security and the information sphere, as well as formulating recommendations for the development of policies in the field of digital sovereignty to ensure a sustainable and secure digital space. Research methods: analysis of scientific literature, legislation and policy documents on digital sovereignty; analysis of statistical data on the digital space and state

policies in this area. Data analysis methods: qualitative and quantitative analysis of the obtained statistical data, comparative analysis of the positive and negative aspects of digital sovereignty on the digital space; formulating conclusions and recommendations based on the results obtained and analysis. Conclusions and recommendations: definition of the concept of digital sovereignty in the context of the powers and activities of government bodies; analysis of the current level of digital sovereignty in public authorities, including an assessment of the level of access to technology, data control, cybersecurity and legislative mechanisms; studying innovative processes that can be implemented in the digital space of government authorities based on the use of new technologies; assessing the impact of digital sovereignty on the ability to implement innovative processes; developing recommendations to improve digital sovereignty and stimulate innovation in the digital space of public authorities. The novelty of the article lies in a detailed analysis of recent research and publications on the topic of digital sovereignty, which provides the basis for new conclusions and recommendations. Offering new concepts and models that allow deeper understanding and analysis of the dynamics of digital transformation. Original conclusions and recommendations arising from the study of the impact of digital sovereignty on the development of the digital space, which may be useful for practitioners and researchers. The analysis and presentation of these aspects will help to emphasize the novelty of the article and the importance of its contribution to the academic and professional community.

Keywords: digital sovereignty; digital space; relationship between digital sovereignty and digital space; information data; information systems; information infrastructure; social networks; cyber threats; cyber crimes; cyber security