

МЕТОДИКА ОЦЕНКИ УРОВНЯ ЦИФРОВОЙ АВТОНОМИИ ИНФОРМАЦИОННОГО ПРОДУКТА

METHODOLOGY FOR ASSESSING INFORMATION PRODUCT DIGITAL AUTONOMY LEVEL

**A. Tsaregorodtsev
I. Mukhin
S. Volkov**

Summary. The digitalization of society has led to the spread of state sovereignty in the field of information and communications technologies. This has resulted in the emergence of the concept of digital state sovereignty. However, in critical areas of society, states depend on digital services and ICT components, which they cannot control. This could lead to potential negative consequences such as restricted or denied access to information, a decrease in information security, and possible remote shutdowns of software functions. Therefore, it is important for states to develop their own information products that have a high level of digital independence in terms of digital sovereignty. This article proposes a methodology for assessing information product digital autonomy level, which allows us to understand the level of sovereignty of an information product necessary for making further decisions related to the product.

Keywords: digital sovereignty, digitalization of society, information security, information product, import substitution.

Царегородцев Анатолий Валерьевич

*Доктор технических наук, профессор, директор, ФГАОУ
ВО Российский университет дружбы народов, г. Москва
tsaregorodtsev_av@pfur.ru*

Мухин Илья Николаевич

*Специалист, старший преподаватель, ФГАОУ ВО
Российский университет дружбы народов, г. Москва
mukhin_in@pfur.ru*

Волков Сергей Дмитриевич

*Заместитель директора, ФГАОУ ВО Российский
университет дружбы народов, г. Москва
volkov_sd@pfur.ru*

Аннотация. С цифровизацией общества государственный суверенитет все больше распространяется и на сферу информационно-коммуникационных технологий, что привело к появлению понятия цифрового суверенитета государства. В важнейших сферах жизни общества государство так или иначе зависит от цифровых услуг, ИКТ и их компонентов, разработка, производство и эксплуатация которых находятся вне его собственного контроля. Это приводит к потенциальным негативным последствиям, связанным с ограничением или полным отказом в доступе к информационным ресурсам и данным, существенному снижению уровня информационной безопасности ИКТ, возможному удаленному отключению программных функций. Именно поэтому государственно важной задачей является разработка собственных информационных продуктов, обладающих высоким уровнем цифровой автономии с точки зрения цифрового суверенитета. В данной статье предлагается методика оценки уровня цифровой автономии информационного продукта, позволяющая понять уровень его суверенизации, необходимый для принятия дальнейших решений, связанных с продуктом.

Ключевые слова: цифровой суверенитет, цифровизация общества, информационная безопасность, информационный продукт, импортозамещение.

Цифровой суверенитет в настоящее время является предметом дискуссий на всех политических уровнях — от национальных площадок до уровня ООН. Этот термин так популярен, поскольку представляет собой, своего рода, ландшафт на поверхность которого проецируются разнообразные стратегические инициативы и политические требования различных государств. Говорить об устоявшемся сегодня уровне понимания масштабов ландшафта цифрового суверенитета сложно, потому целесообразно рассматривать его в качестве открытой динамичной структуры, состоящей из различных компонент суверенизации, которая может изменяться в зависимости от решаемой государством задачи. Ландшафт цифрового суверенитета может быть представлен, в том числе, следующими компонентами, представленными на рисунке 1, хотя едва ли можно претендовать на полноту данной модели.

Тот факт, что зависимость от источников сырья, рынков, решений иностранных правительств и отсутствие проработанных механизмов международного регулирования может негативно сказаться на выполнении государственных задач продемонстрировала, не в последнюю очередь, жёсткая конкуренция в процессе разработки вакцины и международная конкуренция за рынки сбыта медицинских товаров в период пандемии COVID-19. В этой связи цифровые технологии заслуживают особого внимания, поскольку интегрированы в сложные сети взаимозависимостей между государствами и выполняют системообразующие интегральные функции, обеспечивая государства способностью принимать решения и воплощать их в жизнь. Целью целенаправленных действий по обеспечению цифрового суверенитета государства является независимый, самостоятельный и безопасный доступ к цифровым техноло-

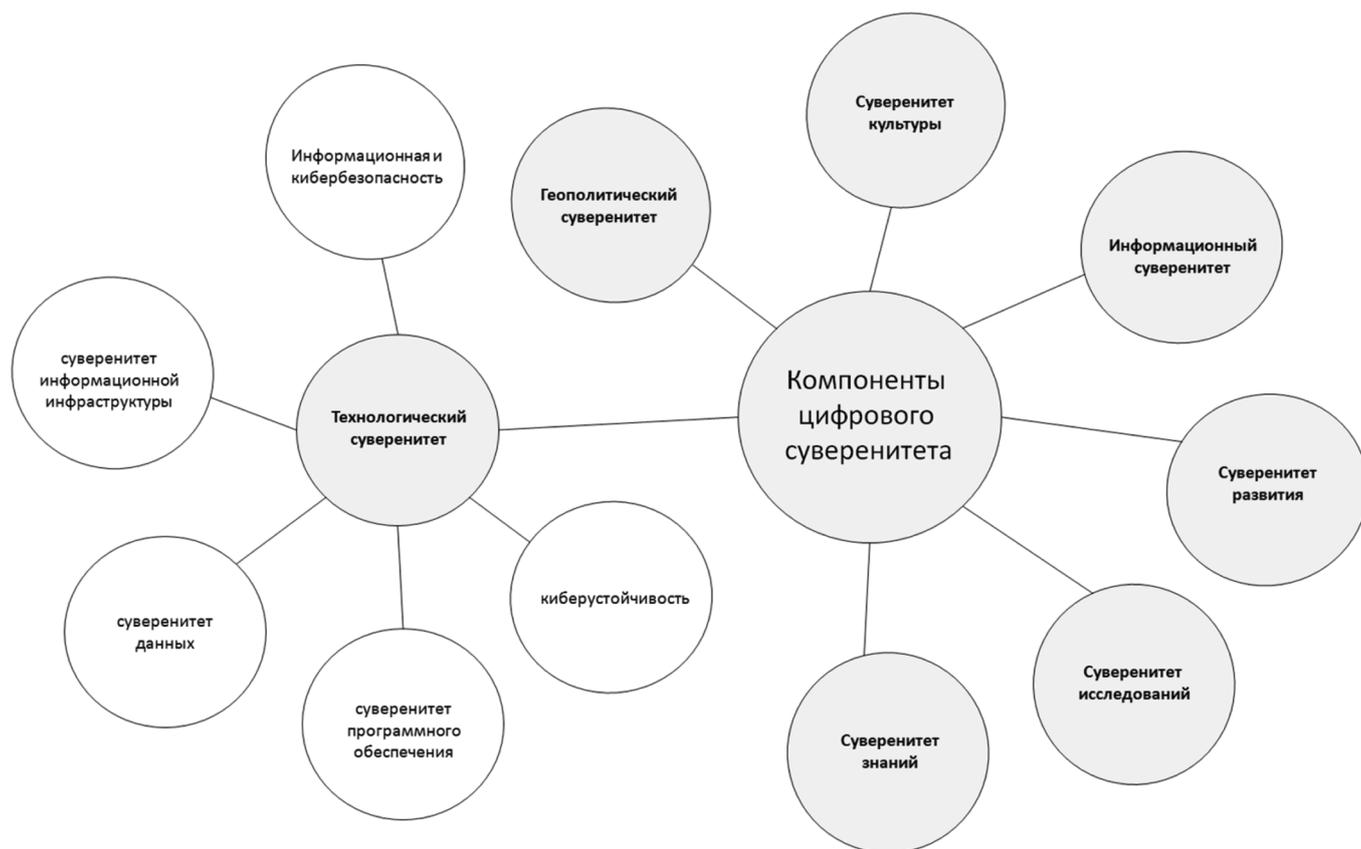


Рис. 1. Компоненты цифрового суверенитета

гиям, чтобы государство могло надежно предоставлять, прежде всего, общественные услуги, и снимать любые ограничения свободы в принятии решений на международной арене из-за отсутствия доступа к цифровым технологиям или недостаточного контроля над ними.

Государственные меры по сдерживанию COVID-19 показывают, что это далеко не интеллектуальные игры: некоторые производители операционных систем для мобильных устройств, вопреки намерениям ряда европейских стран, отказались открывать свои интерфейсы для развёртывания архитектуры и подключения к единой базе данных предупреждения о коронавирусе. Таким образом, эти государства не могли разрешить противоречие в вопросах взаимодействия с частными технологическими компаниями, а именно, защиты интеллектуальной собственности, персональных данных с необходимостью введения экстренных мер раннего предупреждения и защиты от коронавирусной инфекции.

С цифровизацией общества государственный суверенитет все больше распространяется и на ИКТ. Поэтому цифровой суверенитет не следует отбрасывать как модный цифровой политический термин, но следует понимать, как постоянную государственную задачу по созданию и расширению возможностей государства за счет

осознанного стратегического управления уровнем технологической зависимости.

В важнейших сферах жизни общества государство так или иначе зависит от цифровых услуг, ИКТ и их компонентов, разработка, производство и эксплуатация которых в значительной степени находятся вне его собственного контроля. Такие зависимости, в частности, прослеживаются для проприетарных программных продуктов во всех отраслях экономики. Технологическая зависимость приводит к потенциальным негативным последствиям, связанным с ограничением или полным отказом в доступе к информационным ресурсам и данным, существенному снижению уровня информационной безопасности ИКТ, возможному удаленному отключению программных функций. Утрата технологического суверенитета создаёт основания для формулирования новых угроз национальной безопасности:

- технологическая зависимость в рамках цифровой трансформации может привести к потере международной конкурентоспособности национальных отраслей экономики;
- технологическая зависимость существенно осложняет юридическую защиту крупных национальных технологических компаний на международной арене.

Позиционирование системно-определяющей функции современных ИКТ связано с политическим осознанием системной значимости ИКТ практически для всех сфер деятельности государства. Реализация целей достижения высокого уровня конкурентоспособности экономики государства напрямую зависят от динамики развития цифровой индустрии. Вместе с тем, неустойчивость международных отношений, связанная с объективными факторами отсутствия чётко определённых зон ответственности государств в ИКТ среде, отсутствия технического регулирования, общепризнанных международных правовых норм, отсутствия единого понимания термина «инцидент» в киберпространстве способствует формированию такой среды, в которой международные организации, международные соглашения и даже межправительственные союзы теряют свою обязательную силу. Увеличивается уровень политизированности международных торговых отношений, включая цифровые услуги и информационные продукты. Логика рыночных отношений трансформируется, цифровые структуры все чаще признаются в качестве инструментов ценностной политики и международного влияния. Технологическая основа цифровой трансформации глобальных рынков характеризуется сложными системами взаимодействия на основе программного обеспечения в составе сложных ИКТ-систем. Примером может служить технология 5G, которая не является прозрачной для операторов сотовой связи и частично находятся вне их контроля. Таким образом можно сформулировать ключевые предпосылки формирования сфер государственного контроля в отношении цифрового суверенитета:

- необходимость управлять сложными ИКТ;
- глубокое осознание системно-определяющей функции ИКТ;
- анализ новых вызовов цифровой геополитики;
- ослабление международного порядка, связанное с отсутствием единых общепризнанных международных правовых норм.

Цифровые приложения тесно вплетены в единую сеть технологических зависимостей, отдельные компоненты этой сети обеспечены международным разделением труда и сотрудничеством. Эта деятельность обеспечивается большим количеством технических и организационных зависимостей, в основе которых лежат комбинации компонентов ИКТ — технологических пакетов. В общем виде технологический пакет может состоять из набора компонент — сетей, оборудования, программного обеспечения, данных и платформ. Компоненты, используемые для предоставления цифровых услуг, могут различаться на разных этапах процесса их предоставления потребителю, обеспечивая целостный процесс их предоставления. Для предоставления услуги используются различные программные компоненты, операционные системы, серверные операционные системы или специализированное программное обеспечение, а так-

же различные сети для передачи данных или различное оборудование, такое как ПК, маршрутизаторы, смартфоны и т. п. Технологический пакет, обеспечивающий предоставление государственной услуги, включает в себя все технические компоненты на каждом отдельном этапе процесса предоставления услуг. Любые организационные изменения процесса предоставления услуг могут привести к изменениям в технологическом пакете.

Сегментация технологического пакета является, в некотором роде, абстракцией, поскольку в реальных системах эти сегменты практически невозможно отличить друг от друга. Интернет функционирует в пространстве многих технологических зависимостей, но при ближайшем рассмотрении, отдельные его компоненты можно классифицировать в качестве платформ, объединяющих сегменты сетей, которые, в свою очередь, состоят из своих собственных технологических пакетов, представленной собственной инфраструктурой. Современные цифровые технологии основаны на сложной системе иерархии ИКТ, что обуславливает необходимость использования в качестве механизма управления уровнем суверенитета в цифровой сфере контрольные процедуры, но не полное избегание зависимостей.

Информационные продукты и цифровые услуги являются результатом длинных цепочек создания ценности, отдельные этапы которых — от замысла и исследования продукта до вывода его в промышленную эксплуатацию, имеют свои специфические требования к обеспечению цифрового суверенитета государства.

Достаточно ли иметь национальную базу данных собственной разработки, которая является компонентом стратегически важной государственной услуги населению, в случае, когда другие компоненты технологического пакета обеспечиваются внешним поставщиком? Является ли стратегически важным снижение уровня зависимости и усиление контроля со стороны государства для внешних поставщиков программного обеспечения, которое не участвует в осуществлении деятельности ГИС? Насколько необходимо снизить зависимость от внешних исследовательских институтов, чтобы обеспечить национальный патент на инновационную разработку? В тех случаях, когда общие зависимости могут проявляться в предоставлении и использовании цифровых приложений или когда могут возникнуть различные требования с точки зрения цифрового суверенитета, следует описывать компоненты проявлений цифрового суверенитета, которые следуют из общей технологической цепочки создания ценности для обеспечения процесса предоставления цифровой услуги. Исходя из этого, можно предложить набор измерений цифрового суверенитета, в границах которого распространяться система принятия решений, действий или стратегическое целеполагание в цифровой среде (рисунок 2).

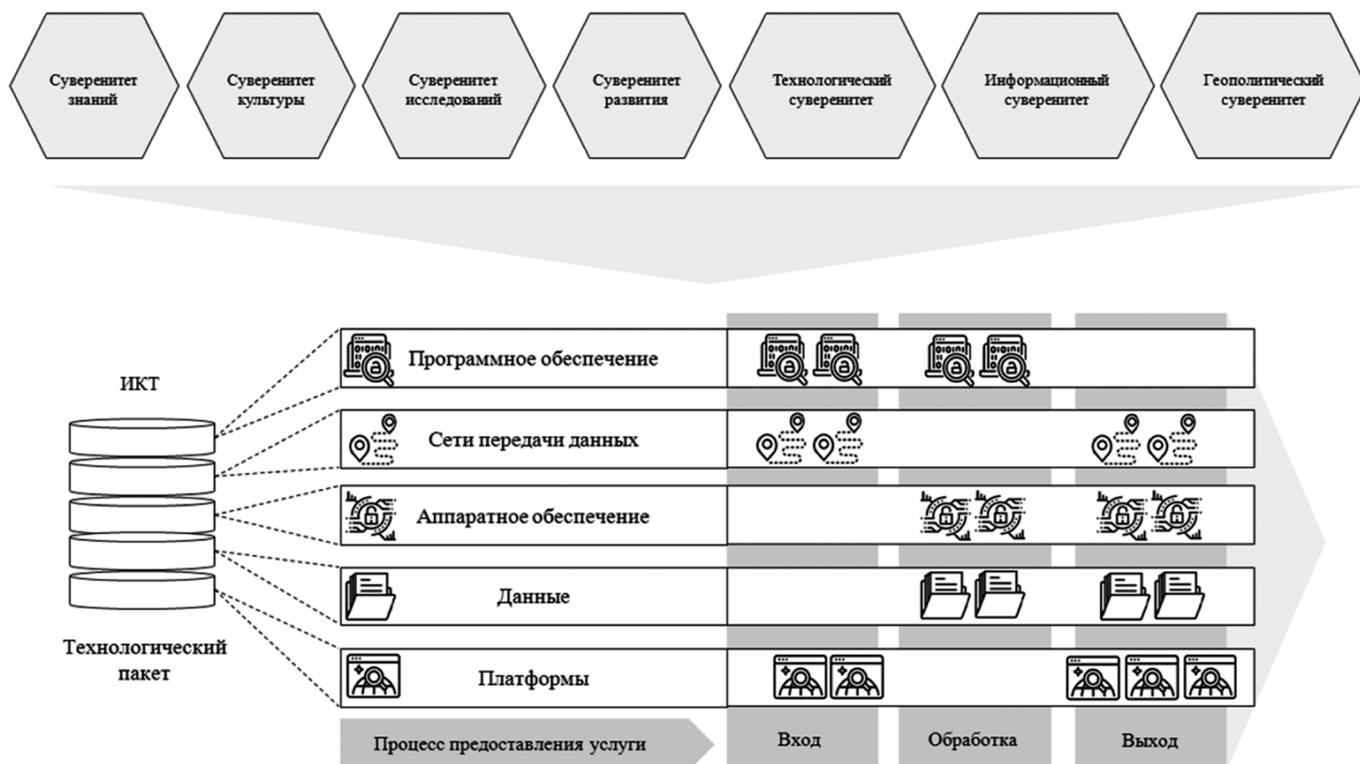


Рис. 2. Уровни обеспечения цифрового суверенитета

В данной статье в качестве набора измерений цифрового суверенитета представлены и рассматриваются следующие компоненты:

- суверенитет знаний;
- культурный суверенитет;
- суверенитет научно-исследовательской деятельности;
- суверенитет развития;
- технологический суверенитет;
- информационный суверенитет;
- геополитический суверенитет.

Суверенитет знаний утверждает право государства иметь доступ к глобальным информационным ресурсам, изучать свойства компонент международной цифровой инфраструктуры, получать экспертные заключения от иностранных специалистов, беспрепятственно обмениваться информацией и накапливать знания в процессе обучения и повышения квалификации граждан.

Культурный суверенитет утверждает право государства руководствоваться ценностями и нормами поведения, которые выработаны в ходе исторического развития народа, страны. Стратегическая цель государства в контексте культурного суверенитета формулируется как недопущение использования сферы культуры для нанесения ущерба национальному государственно-политическому суверенитету и территориальной целостности страны.

Суверенитет научно-исследовательской деятельности утверждает право государства на свободу выбора проводить научные изыскания, продвигать результаты национальных научных исследований в среде мирового научного сообщества, иметь доступ к международным научным ресурсам (алгоритмам, вычислительным мощностям и т. д.), иметь возможность сотрудничества и беспрепятственного обмена результатами научно-исследовательской деятельности в масштабах мирового научного сообщества.

Суверенитет развития утверждает право государства на свободу в выборе концепций, дизайна, способов реализации продуктов и сервисов в сфере высоких технологий, доступ к ресурсам для разработки и испытаний прототипов, доступ к необходимым знаниям в специализированных областях, имеющих отношение к продуктам и сервисам, адаптацию продуктов и сервисов внешних поставщиков к собственным требованиям, наличие доступа к инструментам разработки, программным библиотекам и экспертам.

Технологический суверенитет утверждает право государства на наличие политической точки зрения, согласно которой информационная и коммуникационная инфраструктура и технологии соответствуют законам, потребностям и интересам страны, в которой находятся потребители продуктов и услуг.

Информационный суверенитет утверждает право государства самостоятельно формировать информаци-

онную политику, распоряжаться информационными потоками, обеспечивать информационную безопасность независимо от внешнего влияния. Информационный суверенитет включает в себя любые компоненты, связанные с информационной сферой государства.

Геополитический суверенитет утверждает право государства на суверенную целостность и независимость в вопросах формирования внешней и внутренней политики, международных отношений, политических, военно-стратегических, экологических, экономических аспектах деятельности государства.

Рассмотрение различных аспектов суверенитета и сопоставление их с компонентами технологического пакета создает набор возможных зависимостей и факторов риска, которые необходимо учитывать при стратегическом управлении цифровыми сервисами. Прежде всего, рассматривается каждый технический компонент технологического пакета цепочки услуг. В отношении каждого из компонент цифрового суверенитета рассматриваются уровень значимости его влияния на компоненты технологического пакета (рисунок 3). Подобный взгляд на измерения уровня суверенитета приводит к выводу об уровне суверенитета или автономии данного компонента в отношении внешнего участия и позволяет оценить риск цифровой автономии с точки зрения отдельных технических компонентов информационного продукта в целом. Данные оценки должны быть взвешены в отношении уровня критичности технического компонента для всей цепочки услуг. Результатом анализа станет уровень цифровой автономии услуги, как части информационного продукта в целом, что позволит, в том числе, оценить объём импортозамещения для безопасного использования данной услуги и информационного

продукта. Допустим, что все программные компоненты, используемые в цепочке предоставления услуги в рамках информационного продукта, разрабатываются внутренним (локальным) поставщиком, изначально это характеризует высокую степень цифровой автономии услуги. Если предположить, что отдельные экземпляры программного обеспечения зависят от поставщика, юридически размещённого вне национального правового поля (внешний поставщик), то общая цифровая автономия снижается, увеличивая риск суверенности цифрового продукта, в структуру которого входит эта услуга.

Уровень цифровой автономии оценивается с точки зрения интересов государства. Чем выше стратегическая значимость услуги, тем выше уровень цифровой автономии, что необходимо учитывать уже на стадии замысла и создании услуги. Важность отдельных технических компонентов для создания государственной услуги может быть использована для определения их приоритета в плане создания возможности безраздельного управления услугой. Добиться большего контроля со стороны государства, для приоритетных технических компонентов возможно, используя механизм оценки влияния компонентов цифрового суверенитета на технологический пакет для каждого технического компонента на стадиях жизненного цикла услуги. Баланс между критичностью компонентов, принимающего участие в предоставлении услуг, с одной стороны, и экономической эффект, качество предоставления услуги, с другой, даёт возможность провести взвешенную оценку при выборе локального и внешнего поставщика услуг. Подход, основанный на анализе риска, позволяет разработать адекватные механизмы контроля.

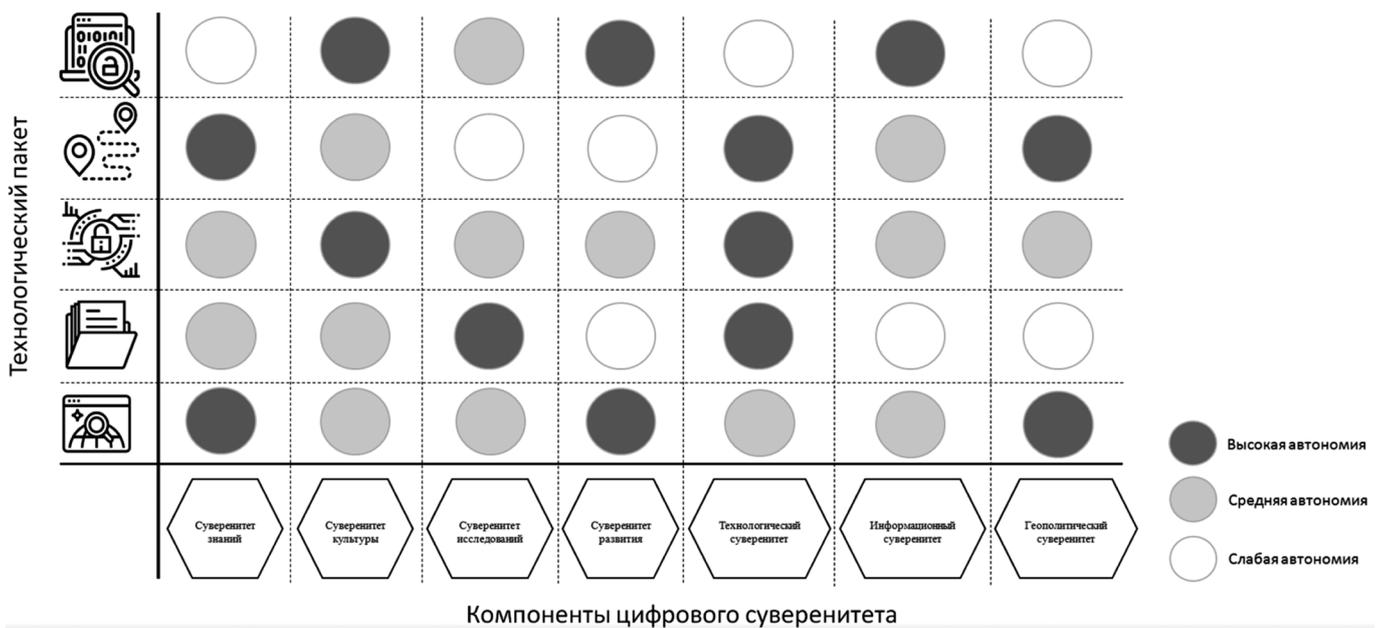


Рис. 3. Матрица для оценки степени цифровой автономии

В рамках данной статьи разработан алгоритм (рисунк 4) оценки уровня цифровой автономии продукта, в состав которого входит набор цифровых услуг и компонентов технологического пакета ИКТ. Развитием подхода к оценке уровня цифровой автономии продукта должна стать методика оценки рисков цифровой автономии продукта, которая позволит всесторонне оценить внешние и внутренние зависимости компонентов продукта (цифровые услуги и сервисы) и компонентов технологического пакета ИКТ от факторов риска цифровой автономии. Перспективным видится создание единой автоматизированной системы и базы данных компонент цифрового суверенитета. Учитывая большой объём данных в масштабах государства и динамику модификации таких данных, для разработки интерфейса взаимодействия с АС целесообразно использовать технологии обработки больших данных, включая инструменты обучения искусственного интеллекта.

Рассмотрим методику определения уровня цифровой автономии продукта.

На первом шаге проводится анализ функций компонентов информационного продукта и оценка уровня их стратегической значимости. Критерии стратегической значимости в терминах обеспечения цифрового суве-

ренитета должны формироваться исходя из ключевых целей и задач, в рамках которых разрабатываются и реализуются компоненты продукта — цифровые услуги и сервисы, массовости использования продукта населением государства, значимости для обеспечения институтов государственной власти, народного хозяйства, науки и образования, обеспечения безопасности и обороноспособности государства и пр. Источниками формирования критериев, в том числе, должны служить:

- нормативные акты в сфере управления экономикой;
- нормативные акты в сфере социальной политики;
- нормативные акты в сфере обеспечения законности, прав и свобод граждан;
- нормативные акты в сфере обеспечения обороны страны, государственной безопасности, реализации внешней политики государства.

Результатам первого шага должны стать разработанные критерии оценки уровня стратегической значимости данного информационного продукта.

На втором шаге проводится анализ состава и оценка уровня стратегической значимости компонентов технологического пакета ИКТ информационного продукта. Наряду с принципами, заложенными в основу оценки

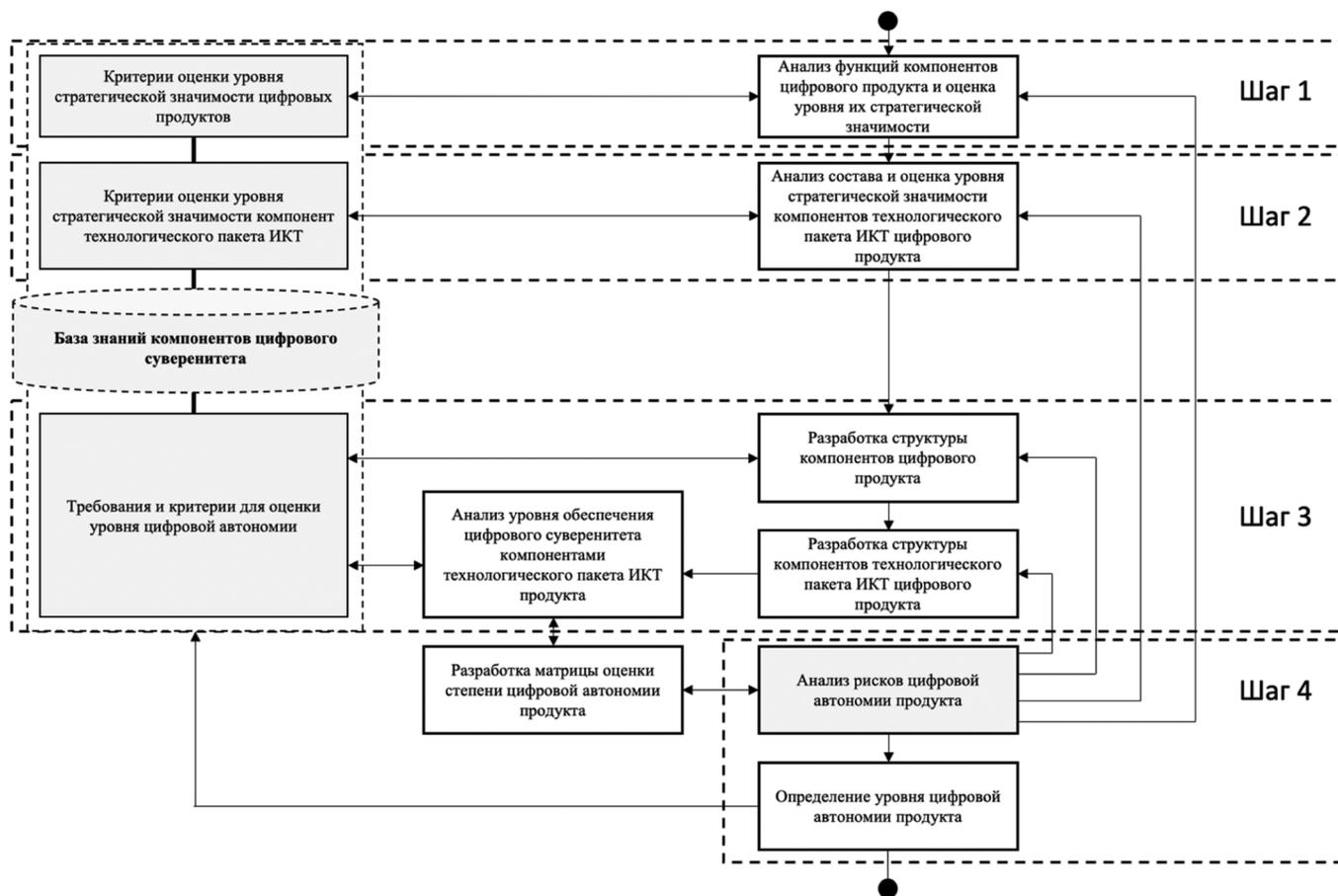


Рис. 4. Алгоритм оценки уровня цифровой автономии информационного продукта

стратегической значимости цифровых услуг, обеспечивающие процесс ИКТ должны, также, оцениваться на предмет их принадлежности к объектам критической информационной инфраструктуры (КИИ), учёта релевантных отраслевых норм и стандартов, требований к безопасности, живучести, киберустойчивости, инновационности компонент их уникальности, технологическим особенностям применения (например, совместимость, взаимозаменяемость компонент) и пр.

Результатам второго шага должны стать разработанные критерии оценки уровня стратегической значимости компонентов технологического пакета ИКТ, обеспечивающих деятельность информационного продукта и его компонентов.

На третьем шаге проводится разработка структуры компонентов информационного продукта и анализ уровня обеспечения цифрового суверенитета компонентами технологического пакета ИКТ продукта.

Результатам третьего шага должна стать составленная матрица для оценки степени цифровой автономии компонентов информационного продукта.

На четвёртом шаге проводится анализ матрицы для оценки степени цифровой автономии и определяется уровень цифровой автономии продукта. Под уровнем цифровой автономии информационного продукта (L) следует понимать способность продукта обеспечить надлежащее качество цифровых услуг, в том числе, за счёт частичного или полного использования заимствованных компонентов технологического пакета ИКТ, но при условии безусловной компенсации этого заимствованного объёма в случае отказа внешнего поставщика от сотрудничества:

$$L = \frac{(C - I)}{(C + I)} \times 100\% \quad (1)$$

где C — компонента собственной разработки как признак суверенного лидерства, I — компонента заимствования как форма использования зарубежных достижений.

Числитель показателя определяет долю отечественного производителя в информационном продукте и свидетельствует об уровне собственных (национальных) технологий в его реализации. Положительная величина доли участия отечественного производителя — свидетельство высокой конкурентоспособности информационного продукта, при условии наличия такой конкуренции на внешнем рынке, при его отсутствии — показатель собственной цифровой автономии продукта. Знаменатель показателя характеризует уровень заимствованных технологий, долю интеграции продукта во внешнеэкономической деятельности или, в терминах цифровой суверенности, характеризует уровень интеллектуальной

изоляции или внешней зависимости информационного продукта.

Значение показателя представляется в процентном виде в пределах $[-100\%, 100\%]$. Отрицательное значение показателя свидетельствует о преобладании заимствованных компонент, положительное — о преобладании компонент собственного производства. По мере продвижения от полного заимствования к его абсолютному отсутствию, информационный продукт проходит критическую точку $L = 0$, которую будем называть точкой достижения цифровой автономии.

В качестве примера рассмотрим динамику суверенизации информационного продукта, представляющего собой цифровую услугу массового использования, состоящую из набора $N = 1000$ ключевых обеспечивающих компонент ИКТ. Пусть известно количество компонент ИКТ собственной и заимствованной разработки на горизонте 2020–2023 годов. Используя (1), найдём L в указанном временном периоде эксплуатации и занесём результат в таблице 1.

Таблица 1. Пример оценки уровня суверенизации цифровой услуги

	2020	2021	2022	2023
Компонента собственной разработки	368	456	567	617
Компонента заимствования	632	544	433	383
L	-26,4 %	-8,8 %	13,4 %	23,4 %

Динамика L позволяет сделать вывод о том, что начиная с 2020 года развитие данной услуги происходит по пути замещения компонент ИКТ внешних производителей. В период с 2021 по 2022 годы цифровая услуга прошла точку достижения цифровой автономии, а в 2023 уровень цифровой автономии составил 23,4 % от общего количества используемых компонент ИКТ.

Проводимый на данном шаге анализ рисков цифровой автономии имеет преимущество в использовании прогнозных моделей, которые позволят рассмотреть возможные сценарии соотношений заимствованных технологий к технологиям собственного производства, что позволит уже на этапе дизайна цифровой услуги исследовать различные фактора риска и принять стратегически верное решение в контексте цифрового суверенитета.

Результатам четвёртого шага должны стать оценка уровня цифровой автономии продукта, выведенная по результатам проведения анализа рисков цифровой автономии услуги.

Заключение

Подводя итог, следует обратить внимание на то, что киберпространство — это, прежде всего, среда ком-

муникации и взаимодействия, где взаимозависимости не всегда являются источником угроз цифровому суверенитету государства. Скорее, речь идет об осознанном выборе степеней зависимости. Основная цель цифровой автономии — снижение риска, достигается за счет проведения детального анализа зависимостей компонентов ИКТ и компонентов цифрового суверенитета. Зависимости могут быть незначительными, ограничи-

ваться институциональными механизмами, сознательно выбираться в рамках стратегического партнерства, быть неизбежными или критическими, что требует анализа и оценки рисков суверенитету государства. В данной статье авторы представили разработанную методику оценки уровня цифровой автономии информационного продукта.

ЛИТЕРАТУРА

1. Бухарин В.В. Компоненты цифрового суверенитета Российской Федерации как техническая основа информационной безопасности // Вестник МГИМО Университета. 2016. № 6 (51). С. 76–91. <https://vestnik.mgimo.ru/jour/article/view/640/625#>
2. Ефремов А.А. Обеспечение государственного суверенитета Российской Федерации в информационном пространстве в документах стратегического планирования // Академический юридический журнал. 2017. №. 2. С. 11–20.
3. Шестопал С.С., Мамычев А.Ю. Суверенитет в глобальном цифровом измерении: современные тренды // Балтийский гуманитарный журнал. 2020. Т. 9. № 1 (30). С. 398–403. <http://portfolio.vvsu.ru/files/CBA3B2C2-2B2B-41DC-BC5D-9A4FD08BDA1C.pdf>
4. Ефремов А.А. Проблемы реализации государственного суверенитета в информационной сфере // Вестник УрФУ. Безопасность в информационной сфере. 2016. № 2 (20). С. 54–60. <http://www.info-secur.ru/index.php/ojs/article/view/136/126>

© Царегородцев Анатолий Валерьевич (tsaregorodtsev_av@pfur.ru); Мухин Илья Николаевич (mukhin_in@pfur.ru);

Волков Сергей Дмитриевич (volkov_sd@pfur.ru)

Журнал «Современная наука: актуальные проблемы теории и практики»