

10. Отчет о результатах деятельности Правительства Республики Башкортостан в 2019 году [Электронный ресурс]. URL: www.pravitelstvorb.ru/upload/iblock/ea/ea24b5dff9b2452adcffb455c9d1171.pdf
11. Республика Башкортостан 2017-2019 гг. Статистический сборник. Официальное издание / Территориальный орган Федеральной службы государственной статистики по Республике Башкортостан. Уфа: Башкортостанстат. 2020. 62 с.
12. Республика Башкортостан в цифрах. Статистический сборник. Официальное издание / Территориальный орган Федеральной службы государственной статистики по Республике Башкортостан (Башкортостанстат). Уфа. 2018. 156 с.
13. Рынок добычи и переработки нефти в России: жизнь после ОПЕК+ [Электронный ресурс]. URL: www.delprof.ru/press-center/open-analytics/rynok-dobychi-i-pererabotki-nefti-v-rossii-zhizn-posle-opek/
14. Среднегодовая численность и структура занятых в экономике по видам экономической деятельности (2010–2016 гг.) [Электронный ресурс]. URL: www.bashstat.gks.ru/storage/mediabank/QoE5UQCU/Среднегодовая_численность_занятых_в_экономике_2010-2016_гг.pdf
15. Среднегодовая численность и структура занятых в экономике по видам экономической деятельности (2017–2019 гг.) [Электронный ресурс]. URL: www.bashstat.gks.ru/storage/mediabank/0ER1uVKE/Среднегодовая_численность_занятых_в_экономике_2017-2019_гг.pdf
16. Среднесписочная численность работников организаций по видам экономической деятельности [Электронный ресурс]. URL: www.clck.ru/Tb69w
17. Среднесписочная численность работников организаций по видам экономической деятельности [Электронный ресурс]. URL: www.clck.ru/U2SWS
18. Отгружено товаров собственного производства, выполнено работ и услуг собственными силами (без НДС, акцизов и аналогичных обязательных платежей) по «хозяйственным» видам деятельности по 2016 г. [Электронный ресурс]. URL: www.fedstat.ru/indicator/31279
19. Zulkarnay I. Why Russia has again been sliding from Federalism to Unitarianism // Вопросы государственного и муниципального управления. 2018. № 5. С. 116–132.

Социально-экономическая оценка цифровой устойчивости регионов Российской Федерации

Socio-economic Evaluation for Digital Sustainability of Regions of the Russian Federation (DOI: 10.34773/EU.2021.4.17)

**Д. ЯХЯЕВ, А. ГРИГОРИЩИН,
Л. СИЛУАНОВА, Т. НАУМУШКИНА**

Яхьяев Дилмурад Батырджанович, старший преподаватель кафедры государственного и муниципального управления Высшей школы экономики, управления и права Северного (Арктического) федерального университета имени М.В. Ломоносова. E-mail: d.yahyaev@narfu.ru

Григорищин Алексей Викторович, ассистент кафедры государственного и муниципального управления Высшей школы экономики, управления и права Северного (Арктического) федерального университета имени М.В. Ломоносова. E-mail: a.grigorischin@narfu.ru

Силуанова Людмила Сергеевна, канд. экон. наук, доцент кафедры менеджмента Высшей школы экономики, управления и права Северного (Арктического) федерального университета имени М.В. Ломоносова. E-mail: l.siluanova@narfu.ru

Наумушкина Татьяна Алексеевна, студентка 3 курса Высшей школы экономики, управления и права Северного (Арктического) федерального университета имени М.В. Ломоносова. E-mail: n.tannya@mail.ru

Статья посвящена оценке цифровой устойчивости регионов Российской Федерации. В ходе выполнения исследований и изучения существующих подходов были определены два элемента, формирующих

цифровую устойчивость: уровень цифрового развития и уровень цифровой безопасности. Оба элемента стали основой авторской методике оценки цифровой устойчивости, представленной в данной статье. Проведенный анализ, согласно методике, выявил три группы регионов: лидирующие, отстающие и сбалансированные. Также были разработаны рекомендации органам государственной власти для развития цифровой безопасности.

Ключевые слова: цифровизация, цифровая безопасность, цифровая устойчивость, цифровая экономика.

The article is devoted to the evaluation of digital sustainability of the regions of the Russian Federation. In the course of research and study of existing approaches, two elements were identified that form digital sustainability, firstly, the level of digital development, and secondly, the level of digital safety. Both elements became the basis of the author's methodology for evaluating digital sustainability presented in this article. The analysis performed according to the methodology revealed three groups of regions: leading, lagging and balanced. Also, recommendations were developed to public authorities for the development of digital safety.

Key words: digitalization, digital safety, digital sustainability, digital economy.

Основные положения

1. Проведенная оценка цифровой устойчивости говорит о прямой связи между уровнем цифрового развития и уровнем цифровой безопасности регионов.
2. В период с 2017 г. по 2019 г. наблюдается положительная тенденция, о которой говорит переход большей части регионов из сектора отстающих в сектор сбалансированных.
3. Основными причинами дифференциации регионов РФ по уровню цифровой безопасности являются: неразвитость цифровой инфраструктуры и несоразмерное финансирование регионов, направленное на развитие цифровой экономики.

Введение

Цифровые технологии становятся частью повседневной экономической и политической жизни субъектов Российской Федерации, двигателем развития общества в целом. Доступность компьютерной техники, цифровые технологии и информация становятся неотъемлемой частью современного мира, приводя к увеличению числа случаев неправомерного вмешательства, отсюда возникает соответствующая потребность в развитии механизмов обеспечения безопасности, защиты информации от угроз и несанкционированного доступа, защиты коммуникационных каналов. Таким образом, можно сказать, что глобальный процесс цифровизации приводит к острой необходимости обеспечения цифровой безопасности регионов Российской Федерации.

По результатам изучения отечественных и зарубежных источников было выделено несколько подходов к понятию цифровой безопасности. Например, российский предприниматель в сфере информационных технологий, искусственного интеллекта и разработки программного обеспечения Игорь Ашманов разделяет данное понятие на две части – в одну он включает непосредственно кибербезопасность, которая связана с безопасным функционированием программного обеспечения, устройств и каналов связи, а ко второй относит информационную безопасность, связанную с воздействием на сознание или же безопасное функционирование умов. С похожей точкой зрения, но в более узком значении данное определение рассматривают Примак Т.К. и Серова О.А., в своей научной работе под названием «Цифровая безопасность: правовое регулирование, соотношение с кибербезопасностью». Они не включают вторую часть данного понятия, которую выделяет Игорь Ашманов, и рассматривают понятие кибербезопасности как составную часть информационной безопасности; в таком случае мы можем говорить о том, что оба автора понимают данное определение одинаково [4]. Анализ дополнительных источников позволил выявить, что чаще всего данный термин используется в качестве синонима для таких вещей, как информационная безопасность, кибербезопасность, цифровой (информационный) суверенитет. Несмотря на различие существующих формулировок, соответствующие источники вкладывают в определения одинаковый или частично схожий смысл – это некие механизмы защиты, обеспечивающие целостность, сохранность и конфиденциальность информации, находящейся в цифровом виде [1].

Подводя итог обзору литературы, отметим, что в рамках данной работы цифровая или информационная безопасность будет пониматься как комплекс мер, методов и механизмов, направленных на защиту цифровой информации и определённых аспектов цифровизации.

Однако отсутствие единого подхода к понятию цифровой безопасности не является серьёзной проблемой, это лишь следствие основной, главной проблемы – неравномерности и дифференциации степени развития цифровизации регионов РФ.

Методы

В процессе исследования использовалась совокупность научных методов, в основу которых положены анализ статистических данных, сравнительный и временной анализ. Теоретической базой является комплекс отечественных и зарубежных источников, посвященных цифровизации и цифровой безопасности регионов Российской Федерации [3; 7].

В рамках данной работы была разработана методология оценки уровня развития цифровизации и цифровой безопасности регионов, индексы с соответствующими названиями были рассчитаны по следующим формулам: для начала использовался минимаксный метод, с помощью выявленных минимальных и максимальных значений в исследуемый период (2017–2019 гг.) по отобраным авторами показателям были рассчитаны коэффициенты, характеризующие степень развития субъектов по данному показателю [6].

Каждый коэффициент рассчитывался по следующей формуле, однако их стоит разделить, поскольку эти коэффициенты относятся к разным индексам, поэтому для начала, формула расчета коэффициентов для индекса цифрового развития показана ниже:

$$I_n = \frac{X - X_{min}}{X_{max} - X_{min}}$$

где I_n – значение рассчитанного коэффициента, демонстрирующего уровень развития субъекта по конкретному показателю из группы показателей, относящихся к развитию цифровизации; X – статистическое значение показателя; X_{min} – минимальное статистическое значение среди субъектов Российской Федерации; X_{max} – максимальное статистическое значение среди субъектов Российской Федерации.

Далее представлена формула расчета коэффициентов для демонстрации уровня цифровой безопасности регионов:

$$Q_n = \frac{X - X_{min}}{X_{max} - X_{min}}$$

где Q_n – значение рассчитанного коэффициента, демонстрирующего уровень развития субъекта по конкретному показателю из группы показателей, относящихся к развитию цифровой безопасности; X – статистическое значение показателя; X_{min} – минимальное статистическое значение среди субъектов Российской Федерации; X_{max} – максимальное статистическое значение среди субъектов Российской Федерации.

$$K_{DL} = \frac{\sum I_1, \dots, I_{22}}{n}$$

где K_{DL} – значение индекса уровня цифрового развития регионов Российской Федерации, отражающее долю организаций, использующих информационно-коммуникационные технологии, уровень оснащения организаций, доступность интернета в них, долю организаций, имеющих веб-сайты, а также уровень оснащения домашних хозяйств персональными компьютерами, наличие доступа к сети Интернет, численность активных абонентов фиксированного широкополосного (в том числе мобильного) доступа к сети Интернет, протяженность каналов, образованных цифровыми системами передачи и долю населения, осуществляющего заказ товаров и услуг (в том числе государственных и муниципальных) через интернет.

Индекс уровня цифрового развития регионов рассчитывается за 2017, 2018 и 2019 годы, таким образом, предоставляя нам возможность проследить тенденцию непосредственного развития. Аналогично индексу цифровизации рассчитывается индекс уровня цифровой безопасности:

$$K_{DS} = \frac{\sum Q_1, \dots, Q_4}{p}$$

где K_{DS} – значение индекса уровня цифровой безопасности регионов Российской Федерации, отражающее уровень цифровизации местной телефонной сети, уровень оснащённость организаций специальными программными средствами, локальными вычислительными средствами и средствами защиты информации.

При написании научно-исследовательской работы был проведен анализ на основе статистических данных. При выборе показателей использовались официальные статистические сборники Федеральной службы государственной статистики (РОССТАТ) и Единой межведомственной информационно-статистической системы (ЕМИСС). В качестве показателей по оценке уровня цифрового развития были выбраны показатели, представленные в таблице 1.

Таблица 1

Система показателей оценки уровня цифрового развития регионов РФ

№ п/п	Наименование показателя
1	Организации, использовавшие персональные компьютеры
2	Организации, использовавшие серверы
3	Организации, использовавшие сеть Интернет
4	Организации, использовавшие широкополосный доступ к сети Интернет
5	Организации, имевшие веб-сайт
6	Число персональных компьютеров на 100 работников, всего
7	Число персональных компьютеров на 100 работников с доступом к сети Интернет
8	Организации, использовавшие системы электронного документооборота
9	Организации, использовавшие электронный обмен данными между своими и внешними информационными системами, по форматам обмена
10	Удельный вес домашних хозяйств, имевших персональный компьютер
11	Удельный вес домашних хозяйств, имевших доступ к сети Интернет
12	Удельный вес домашних хозяйств, имевших широкополосный доступ к сети Интернет
13	Население, использовавшее сеть Интернет
14	Население, использовавшее сеть Интернет, в том числе каждый день или почти каждый день
15	Численность активных абонентов фиксированного широкополосного доступа к сети Интернет
16	Численность активных абонентов мобильного широкополосного доступа к сети Интернет
17	Протяженность каналов, образованных цифровыми системами передачи
18	Доля населения, использовавшего сеть Интернет для получения государственных и муниципальных услуг в общей численности населения, получившего государственные и муниципальные услуги
19	Доля населения, использовавшего сеть Интернет для заказа товаров и (или) услуг в общей численности населения
19	Уровень цифровизации местной телефонной сети – всего
20	Доля образовательных учреждений, реализующих образовательные программы с использованием дистанционных образовательных технологий для реализации основных образовательных программ, в общем числе самостоятельных образовательных учреждений среднего профессионального образования
21	Доля образовательных учреждений, реализующих образовательные программы с использованием дистанционных образовательных технологий для реализации основных образовательных программ, в общем числе самостоятельных образовательных учреждений высшего профессионального образования

Также в качестве показателей для расчета индекса цифровой безопасности и соответствующего ей уровню развития были выбраны показатели, представленные в таблице 2.

Таблица 2

Система показателей оценки уровня цифровой безопасности регионов РФ

№ п/п	Наименование показателя
1	Объем инвестиций в основной капитал, направленных на приобретение информационного, компьютерного и телекоммуникационного (ИКТ) оборудования (без субъектов малого предпринимательства и объема инвестиций, не наблюдаемых прямыми статистическими методами)
2	Доля организаций, использовавших средства защиты информации, передаваемой по глобальным сетям – всего
3	Доля организаций, использовавших локальные вычислительные сети, в общем числе обследованных организаций
4	Использование специальных программных средств в организациях

Результаты и обсуждение

По результатам исследования, проведенного на основании описанного ранее в работе метода, были получены значения индексов, демонстрирующие уровень цифрового развития и уровень развития цифровой безопасности. Изучая научные статьи, мы столкнулись с тем, что ранее упомянутые понятия часть авторов определяют как цифровую устойчивость. В связи с чем авторским коллективом было принято решение сформулировать определение понятия «Цифровая устойчивость регионов» [2].

Цифровая устойчивость – это совокупность используемых цифровых технологий, обеспечивающих стабильность и конкурентоспособность регионов в области цифрового развития, а также способность предотвратить угрозы.

Для дальнейшего анализа регионы разделены на три сектора.

Первый сектор – это *сектор лидирующих регионов*. В данный сектор на протяжении всех трёх изучаемых лет попадают такие города Российской Федерации, как Москва и Санкт-Петербург. В 2019 году добавились регионы: Мурманская область, Ямало-Ненецкий автономный округ, Тульская область, Камчатский край, Магаданская область, Сахалинская область, Чукотский автономный округ и Оренбургская область. Таким образом, число субъектов увеличилось с двух в 2017 году до 10 в 2019 году.

Присутствие данных субъектов в группе лидирующих регионов говорит об их высокой цифровой устойчивости, высокой цифровой культуре населения и бизнеса, а также о наивысшем уровне использования организациями специальных программных средств, средств дополнительной защиты и локальных вычислительных сетей (ЛВС). Также стоит отметить значительные государственные и частные инвестиции в элементы цифровой среды и ИКТ, непосредственно формирующие уровень цифровизации и цифровой безопасности регионов.

Сектор сбалансированных регионов является наиболее наполненным в течение всего рассматриваемого периода. Это связано с тем, что многие регионы попали в данный сектор, имея среднее значение по обоим индексам. Стоит отметить, что достаточное количество сбалансированных регионов имеют потенциал для перехода в сектор регионов-лидеров.

Сектор отстающих регионов имеет также свою положительную динамику. На 2017 год в эту зону входили 5 субъектов – Республика Дагестан, Чеченская Республика, город Севастополь, Республика Бурятия и Кабардино-Балкарская Республика. В 2018 году в данном секторе остались только 3 региона – Республика Дагестан, Чеченская Республика и Республика Бурятия, но в 2019 году Бурятия уже смогла перейти в сектор сбалансированных регионов, максимально приблизившись к регионам-лидерам за счет увеличения показателей, непосредственно

связанных с уровнем цифровизации организаций. Отстающими регионами, согласно данному анализу, являются Республика Дагестан и Чеченская Республика.

Заключение

Таким образом, мы можем говорить о том, что объединяющей проблемой отстающих регионов является отсутствие развитой цифровой инфраструктуры [5]. Существенное влияние на проблему слабой развитости цифровой инфраструктуры оказывает ещё одна дополнительная проблема – слабая кадровая обеспеченность в связи с ростом образовательной миграции.

Также одной из проблем, на наш взгляд, является несоразмерное распределение финансовых ресурсов из федерального бюджета между бюджетами субъектов РФ. Предлагаемое нами решение данной проблемы состоит в следующем – при распределении федеральных субсидий органам власти необходимо принимать во внимание позицию субъектов по значениям индексов уровня развития цифровизации и уровня цифровой безопасности.

Литература

1. Бухарин В.В. Компоненты цифрового суверенитета Российской Федерации как техническая основа информационной безопасности // Вестник МГИМО. 2016. № 6. С. 77–78.
2. Королева Н.Ш., Топунова И.Р. Информационная безопасность как условие развития цифровой экономики // Modern Economy Success. 2019. № 3. С. 110–116.
3. Кузнецов Ю.А., Маркова С.Е. Некоторые аспекты количественной оценки уровня цифрового неравенства регионов Российской Федерации // Экономический анализ: теория и практика. 2014. № 32.
4. Примак Т.К., Серова О.А. Цифровая безопасность: правовое регулирование, соотношение с кибербезопасностью // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. 2019. № 2. С. 57–60.
5. Полябин С.В., Коваленко Л.В. Цифровая инфраструктура // Сб. науч. трудов «Энергия молодых». Кузбасский государственный технический университет им. Т.Ф. Горбачева. 2012. С. 169–170.
6. Степанова В.В., Уханова А.В., Григоришин А.В., Яхяев Д.Б. Оценка цифровых экосистем регионов России // Экономические и социальные перемены: факты, тенденции, прогноз. 2019. Т. 12. № 2. С. 73–90.
7. Яхяев Д.Б., Григоришин А.В. Вызовы и перспективы развития цифровой экономики в Российской Федерации // Арктические исследования: от экстенсивного освоения к комплексному развитию: материалы I Междунар. молодежной науч.-практ. конф. (26–28 апреля 2018 г.): в 2 т. / Сев. (Арктич.) федер. ун-т; ФИЦКИА РАН. Т. 1. Архангельск: САФУ, 2018. С. 44–47.