π-Economy. 2023, Том 16, № 3. С. 63–79.
π-Economy. 2023, Vol. 16, No. 3. Pp. 63–79.

Экономическая безопасность
Economic safety

Научная статья
УДК 332.142
DOI: https://doi.org/10.18721/JE.16304

ЗАЩИЩЁННОСТЬ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА КАК ФАКТОР ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ РЕГИОНА: ИНСТРУМЕНТАРИЙ ОЦЕНКИ

М.М. Балог[1] ✉ , **А.В. Бабкин**[1,2]

[1] Псковский государственный университет,
г. Псков, Российская Федерация;

[2] Санкт-Петербургский политехнический университет Петра Великого,
Санкт-Петербург, Российская Федерация

✉ seb5658@yandex.ru

Аннотация. Неоднозначное влияние современных информационно-коммуникационных технологий на экономическую и социальную среду актуализирует внимание к информационным аспектам экономической безопасности. Цель работы заключается в разработке и апробации методики оценки защищённости информационного пространства как фактора экономической безопасности региона. В рамках настоящего исследования были использованы такие методы как сравнительный анализ, типологизация, системный метод, методы статистического анализа, индексный и рейтинговый методы, корреляционный анализ. Анализ и систематизация определений понятия информационная безопасность и исследовательских подходов к измерению данного явления, а также разработка методологии и методики оценки защищённости информационного пространства регионов и апробация данного инструментария позволили сделать ряд выводов. Во-первых, защищенность информационного пространства определена в качестве одного из значимых факторов экономической безопасности региона. Комплексный подход в трактовке понятия информационной безопасности выявлен в качестве универсального методологического инструмента, сочетающего в себе как технические, так и социально обусловленные (культурно-исторические, политико-правовые, финансовые и др.) аспекты данной проблематики. Разработанная индексно-рейтинговая методика оценки защищённости информационного пространства позволяет оценить вероятность реализации угроз экономической безопасности, имеющих информационный характер посредством изучения состояния цифровой инфраструктуры, информационной открытости организаций и учреждений, защищенности пользователей от киберугроз, цифровой и финансовой грамотности населения. Во-вторых, между большинством компонентов информационной безопасности не прослеживается заметная взаимосвязь (средний уровень связанности обнаружен только между цифровой инфраструктурой и информационной открытостью организаций и учреждений). Данная ситуация свидетельствует, что обеспечение информационной безопасности в разрезе цифровизации различных сфер жизнедеятельности осуществляется стихийно и требует большей координации. В-третьих, межрегиональные диспропорции в развитии цифровых и предметных (финансовых) компетенций населения, необходимых для обеспечения информационной безопасности выше, чем аналогичные диспропорции в рамках прочих компонентов информационной защищенности (цифровая инфраструктура, наличие у организаций и учреждений Интернет-сайтов и применение пользователями антивирусного ПО). Также модули цифровых и финансовых компетенций показали наихудшие результаты с точки зрения количества регионов, имеющих в соответствующих аспектах не удовлетворительный уровень информационной безопасности. Подводя итоги исследования следует отметить необходимость использования системного подхода в реализации политики управления информационной безопасностью на региональном уровне. Пропорциональное развитие всех компонентов информационной безопасности повысит эффективность использования выделяемых для этого ресурсов и обеспечит высокое качество защищенности информационного пространства. Дальнейшие исследования

в рамках данной проблематики будут направлены на уточнение показателей диагностики информационной безопасности и методов их нормирования.

Ключевые слова: информационная безопасность, экономическая безопасность, регион, цифровая инфраструктура, информационная открытость, киберугрозы, цифровая грамотность, финансовая грамотность

Благодарности: грант Псковского государственного университета по мероприятию «Проведение фундаментальных научных исследований и поисковых научных исследований малыми научными группами под руководством ведущего ученого», Заявка № science2022_2-8561-6522

Для цитирования: Балог М.М., Бабкин А.В. (2023) Защищённость информационного пространства как фактор экономической безопасности региона: инструментарий оценки. π-Economy, 16 (3), 63–79. DOI: https://doi.org/10.18721/JE.16304

Research article
DOI: https://doi.org/10.18721/JE.16304

INFORMATION SPACE SECURITY AS A REGIONAL ECONOMIC SECURITY FACTOR: ASSESSMENT TOOL

M.M. Balog[1] ✉, A.V. Babkin[1,2]

[1] Pskov State University, Pskov, Russian Federation;

[2] Peter the Great St. Petersburg Polytechnic University, St. Petersburg, Russian Federation

✉ seb5658@yandex.ru

Abstract. The ambiguous impact of modern information and communication technologies on the economic and social environment actualizes attention to the information aspects of economic security. The purpose of the work is to develop and test a methodology for assessing the security of the information space as a factor in the economic security of the region. Within the framework of this study, such methods as comparative analysis, typology, system method, methods of statistical analysis, index and rating methods, correlation analysis were used. Analysis and systematization of the definitions of the information security concept and research approaches to measuring this phenomenon, as well as the development of a methodology for assessing the security of the information space of regions and testing of this toolkit, led to a number of conclusions. Firstly, the security of the information space is defined as one of the significant factors in the economic security of the region. An integrated approach to the interpretation of the concept of information security is identified as a universal methodological tool that combines both technical and socially determined (cultural, historical, political, legal, financial, etc.) aspects of this issue. The developed index-rating methodology for assessing the security of the information space makes it possible to assess the likelihood of economic security threats that are informational in nature by studying the state of the digital infrastructure, the information openness of organizations and institutions, the protection of users from cyber threats, digital and financial literacy of the population. Secondly, there is no noticeable relationship between most information security components (the average level of connectivity was found only between the digital infrastructure and the information openness of organizations and institutions). This situation indicates that ensuring information security in the context of digitalization of various spheres of life is carried out spontaneously and requires greater coordination. Thirdly, inter-regional disparities in the development of digital and subject (financial) competencies of the population necessary to ensure information security are higher than similar disproportions in other components of information security (digital infrastructure, the availability of websites in organizations and institutions, and the use of anti-virus software by users). In addition, the modules of digital and financial competencies showed the worst results in terms of the number of regions that have an unsatisfactory level of information security in the relevant aspects. Summing up the results of the study, there is a noticeable need for systematic approach in the implementation of information security management policy at the regional level. The proportional development of all

components of information security will increase the efficiency of the use of resources allocated for this and ensure the high quality of information space security. Further research within the framework of this issue will be aimed at clarifying the indicators of information security diagnostics and methods for their regulation.

Keywords: information security, economic security, region, digital infrastructure, information openness, cyber threats, digital literacy, financial literacy

Acknowledgements: Pskov State University grant for "Conducting fundamental scientific research and exploratory scientific research by small scientific groups under the guidance of a leading scientist", Application No. science2022_2-8561-6522

Citation: Balog M.M., Babkin A.V. (2023) Information space security as a regional economic security factor: assessment tool. π-Economy, 16 (3), 63–79. DOI: https://doi.org/10.18721/JE.16304

Введение

Актуальность исследования

Обострение угроз в экономической и социальной сферах в результате санкционного давления на российскую экономику со стороны недружественных государств актуализирует интерес к процессу обеспечения экономической безопасности. Важным вопросом при этом является определение приоритетов экономической безопасности, в связи с чем в рамках данной работы предлагается обратить внимание на её информационную составляющую. Вопросы защищённости информационного пространства человека и общества имеют высокую значимость среди основных направлений государственного управления, что подтверждается вниманием к информационной безопасности в документах стратегического планирования. Стратегия национальной безопасности России в качестве одного из национальных интересов содержит развитие безопасного информационного пространства и защиту общества от деструктивного информационно-психологического воздействия. Доктрина информационной безопасности России ориентирована на защиту жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, связанных с применением информационных технологий в политических и военных целях. Согласно Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы в формировании современного информационного пространства влиятельную роль играет безопасность, проявляющаяся в социокультурных, нормативно-правовых, образовательных, информационно-консультативных и технико-технологических аспектах.

Процесс развития информационно-коммуникационных технологий, современный этап которого представлен цифровизацией, существенным образом трансформирует различные стороны общественной жизни. Создание, хранение, распространение и использование информации в цифровом виде порождает новые возможности и угрозы для общества [3]. С одной стороны, цифровые инструменты повышают конкурентоспособность предприятий, улучшают качество государственного управления, выводят на новый уровень качество жизни людей и способствуют формированию высокоэффективного человеческого капитала [20, 21]. С другой стороны, цифровизация порождает новые вызовы и угрозы экономической безопасности, такие как зависимость от импорта цифровых технологий, неравенство регионов и социальных групп в цифровых и предметных компетенциях, хищение данных составляющих служебную, коммерческую и банковскую тайну, разнообразные по целям и способам осуществления кибератаки, нарушение конфиденциальности персональных данных, мошенничество при помощи вредоносного программного обеспечения или методов социальной инженерии, распространение заведомо недостоверной (фейковой) информации и многие другие [19, 22, 24]. Без преувеличения, оцифрованная информация подобно атомной энергии способна выступить мощным фактором общественного прогресса или же стать причиной краха того или иного общества.

Столь мощный и неоднозначный потенциал цифровых технологий требует переосмысления приоритетности вызовов и угроз экономической безопасности. В результате этого представляется оправданным изучение экономической безопасности на основе защищённости информационного пространства в контексте цифровизации.

Цель работы заключается в разработке и апробации методики оценки защищённости информационного пространства как фактора экономической безопасности региона. Для достижения поставленной цели в исследовании реализуются следующие задачи: анализ и систематизация теоретических подходов трактовки понятия информационной безопасности и оценки уровня защищенности информационного пространства; формирование методологии и методики оценки защищенности информационного пространства; апробация разработанного подхода на регионах Российской Федерации и выявление проблем в обеспечении информационной безопасности; определение взаимосвязи между основными компонентами информационного пространства региона в условиях цифровизации.

Объектом в рамках настоящего исследования является регион, рассматриваемый с позиции защищенности информационного пространства. Предметом исследования выступает экономическая безопасность региона.

Литературный обзор

В силу того, что информационная безопасность является многомерным понятием и рассматривается представителями разных наук, в литературе представлено несколько теоретических подходов к изучению данного явления. В качестве основных исследовательских подходов можно определить технический, социологический и комплексный. В рамках технического подхода под информационной безопасностью понимается безопасность информации и поддерживающей инфраструктуры от влияния деструктивных факторов, способных нанести ущерб поддерживающей инфраструктуре, а также пользователям и владельцам информации[1]. Информационная безопасность также определяется как совокупность методов предотвращения от несанкционированного доступа, взлома, раскрытия, утечки, изменения или удаления данных в информационном пространстве [18]. Несколько более широкая трактовка информационной безопасности в рамках технического подхода предполагает, что это базисное технологическое качество системы, определяющее: 1) возможность противостоять негативному влиянию информационных угроз, 2) уровень угроз, которые формируются в процессе обеспечения информационной безопасности как для различных элементов самой системы, так и для внешней среды [8]. Информационная безопасность на уровне предприятия как правило исследуется именно посредством технического подхода, поскольку он способен охватить наиболее актуальные вызовы и угрозы для конкретной организации в этой области знания. Однако на уровне личности, общества, региона и государства требуются и другие теоретико-методологические решения, учитывающие значительное многообразие факторов, влияющих на данные объекты.

Согласно социологическому подходу информационная безопасность – это состояние социума, при котором обеспечена защита личности, общества и государства от воздействия информационных потоков осуществляемых в интересах деструктивных сил и направленных на деформацию общественного и индивидуального сознания, следствием чего выступает девиантное поведение, усиление социально-политических, экономических и духовных противоречий, психологической напряженности в обществе [11]. Под информационной безопасностью в социологическом контексте понимается также состояние субъектов общества позволяющее им эффективно функционировать на основе 1) объективного отсутствия информационных рисков и угроз, 2) субъективного восприятия ситуации в сфере информационного пространства как таковой [13]. Кроме того,

[1] Галатенко В.А. (2020) Основы информационной безопасности: учебное пособие. 3-е изд. Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа.

информационная безопасность предполагает возможность распространять и получать надежную информацию по любым вопросам, а также защиту от предвзятой и искаженной информации [12].

Таким образом, если представители технического подхода сосредоточены на вопросах обеспечения целостности, доступности и конфиденциальности информации, то исследователи, придерживающиеся социологического подхода, держат в центре внимания тот или иной информационный контент. Соответственно, в рамках проведения специализированных исследований, сосредоточенных на какой-то одной сфере общественной жизни, в зависимости от вида изучаемой информации можно обозначить существование политического, правового, экономического, психологического, социально-гуманитарного, культурно-исторического и других теоретических подходов к информационной безопасности.

При этом нужно отметить, что угрозы информационной безопасности могут исходить не только от имеющих деструктивное содержание информационных потоков. Опасность могут представлять и другие факторы, например, неразвитость информационно-коммуникационной инфраструктуры или недостаточный уровень знаний населения в той или иной предметной области. Кроме того, в ряде случаев угрозы носят комплексный характер, так мошенничество может совершаться как методами социальной инженерии, так и использованием вредоносного программного обеспечения или уязвимостей в программном обеспечении клиентов финансовых организаций. Разумеется, нельзя забывать и про одновременность существования значительного количества актуальных для общества и государства угроз информационной безопасности. В связи вышесказанным представляет интерес комплексный подход к защищенности информационного пространства. Данный подход содержится в Доктрине информационной безопасности России, где информационная безопасность трактуется как состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются суверенитет, устойчивое социально-экономическое развитие и обороноспособность государства, законные права и свободы человека, достойное качество жизни населения. Согласно Доктрине, рассматриваемые угрозы носят как информационно-технический, так и информационно-психологический характер. В силу широты охвата исследовательской проблематики данное определение информационной безопасности получило распространение в научном сообществе [2, 4, 7]. Привлекательность комплексного подхода в том, что он позволяет акцентировать внимание на культурно-исторических, политико-правовых и финансово-экономических аспектах информационной безопасности, не упуская из виду техническую составляющую данного процесса.

В научной и методической литературе достаточно широко представлены публикации, по оценке уровня информационной безопасности объектов разного уровня управления, при этом большинство из них сосредотачивают внимание на уровне организации. Отмечается, что в основе оценивания рисков информационно-управляющих систем организаций лежат количественные методы обработки статистических данных которые затем могут быть расширены качественными методами в виде экспертных оценок или построения дерева принятия решений [10]. Для оценки информационной безопасности предприятий может быть использована система индикаторов с предельно допустимыми значениями или модель зрелости организационных, кадровых и программно-технических процессов. Ещё одним инструментом является применение коэффициентов, определяющих качество информации (полноты, точности, непротиворечивости) использующейся для принятия управленческих решений [14]. Процедура анализа информационной безопасности предприятия также может включать такие экспертные методы как SWOT-анализ, розу и спираль рисков, оценку риска стадии проекта и метод Дельфи [1].

Рассматривая организации в отраслевом разрезе отметим существование утвержденных методик измерения информационной безопасности, которые носят рекомендательный или обязательный характер. В частности, оценка информационной безопасности организаций банковской системы регламентирована соответствующим стандартом Банка России, содержащим показате-

ли информационной безопасности и способы их оценивания [16]. Федеральная служба по техническому и экспортному контролю также разработала подобную методику, которая обязательна для государственных и муниципальных информационных систем, информационных систем персональных данных и прочих значимых объектов [9].

Среди представленных методов оценки защищенности информационного пространства на региональном уровне преобладают количественные методы, основанные на обработке статистических данных. Анализ научной литературы позволил систематизировать указанные методы следующим образом: анализ динамики первичных показателей, индексный и индексно-рейтинговый методы, а также стоимостной метод.

Самым простым методом оценки информационной безопасности на территориальном уровне является отслеживание динамики показателей использования отдельных информационно-коммуникационных технологий [2]. Познавательная ценность данного подхода является достаточно ограниченной, поскольку он не предполагает возможности обработки данных большого количества показателей.

Индексный метод предполагает расчет интегрального индекса (коэффициента) на основе первичных статистических показателей. В качестве примера можно привести исследование, в котором предлагается учитывать информационные факторы при расчёте коэффициента жизнестойкости общества. Отмечается, что что все группы факторов, включая информационные, могут как повышать, так и снижать жизнестойкость [6].

Индексно-рейтинговый метод является логическим продолжением предыдущего подхода и предполагает распределение объектов исследования на основе значения их индексов в некоторой последовательности (возрастания или убывания), либо группировку указанных объектов. Так оценка информационной безопасности регионов выполняется на основе расчета интегральных показателей, в результате чего регионы распределяются по классам защищенности [17]. Схожим исследовательским подходом является измерение состояния информационного пространства региона в контексте оценки его экономической безопасности. Здесь на основе выбранных показателей экономической безопасности (включая информационные) рассчитываются подиндексы групп показателей, которые затем агрегируются в индекс экономической безопасности региона, содержащий информационную составляющую. На основе данного индекса регионы ранжируются в соответствии с текущим уровнем опасности [15].

Стоимостной метод предполагает возможность экономического измерения состояния информационной безопасности. Согласно данному подходу оценка информационной безопасности регионов основывается на определении соотношения уровня угроз и уровня защищенности регионального информационного пространства с применением коэффициента, обеспечивающего приведение результата к стоимостным показателям. Альтернативным вариантом в рамках данного подхода является измерение величины ущерба, связанного с фактической реализации угроз информационной безопасности региона [5].

Методы и материалы

В рамках настоящего исследования были использованы такие методы как сравнительный анализ, типологизация, системный метод, методы статистического анализа, индексный и рейтинговый методы, корреляционный анализ. Методами статистического анализа были обработаны массивы данных по информационной безопасности 82 регионов России за 2021 год (Ненецкий, Ямало-Ненецкий и Ханты-Мансийский автономные округа рассматривались составе Архангельской и Тюменской областей). Выбор данного временного отрезка продиктован наличием сформировавшейся постковидной цифровой среды и отсутствием воздействие атипичных угроз информационной безопасности 2022–2023 годов. Применение индексного и рейтингового методов позволило рассчитать индексы оценивающие информационную безопасность и выполнить груп-

пировку регионов на основе соответствия фактических значений индексов нормативным. Для оценки степени взаимосвязи между развитием цифровой инфраструктуры, информационной открытости организаций и учредений, защищённости от киберугроз, цифровой и финансовой грамотности населения использован корреляционный анализ.

Источником статистических данных для модулей цифровая инфраструктура, информационная открытость организаций и учреждений, защищенность пользователей от киберугроз и цифровая грамотность выступил Росстат. Данные для модуля финансовая грамотность получены из информационного ресурса моифинансы.рф Минфина России и Росстата.

Результаты и обсуждение

В научной литературе информационная безопасность определяется в качестве одной из составных частей экономической безопасности [25]. При этом отмечается, что использование современных информационно-коммуникационных технологий помимо ряда положительных эффектов также способствует развитию деструктивных явлений в экономике и трансформации угроз экономической безопасности [15]. Реализация угроз в области информационной безопасности способна дестабилизировать экономическую ситуацию в регионе и значительно снизить потенциал его развития [5]. Таким образом, защищенность информационного пространства признаётся исследователями одним из значимых факторов экономической безопасности региона.

Разработанная методика оценки защищенности информационного пространства представляет собой индексно-рейтинговую оценку данного явления и состоит из трех основных этапов.

Первый этап предполагает нормирование каждого из выбранных статистических показателей посредством индекса информационной безопасности, для нахождение которого используются пороговые значения рассматриваемых показателей по формуле:

$$I_{ij} = \frac{Y_{ij}}{\text{ПОРОГЗНАЧ } Y_{ij}},$$

где I_{ij} – индекс информационной безопасности j-го показателя, который характеризует i-ый регион; Y_{ij} – фактическое значение j-го показателя для i-го региона.

В качестве пороговых значений применялись средние значения национальной экономики. В модуле финансовая грамотность средние значения были рассчитаны автором, во всех остальных модулях использованы значения из данных Росстата. Сгруппированные в пять модулей показатели защищенности информационного пространства представлены в табл. 1. Значимость указанных модулей для реализации цели настоящего исследования определяется тем, что они содержательно отражают основные аспекты информационной безопасности в условиях цифровизации:

- модуль цифровой инфраструктуры оценивает базовую техническую возможность обеспечения информационной безопасности домохозяйствами, организациями и органами власти при помощи цифровых технологий;
- модуль информационной открытости определяет доступность полной, достоверной и актуальной информации от организаций и учреждений для всех заинтересованных сторон;
- модуль защищенности от киберугроз отражает уровень защищенности пользователей от актуальных угроз информационной безопасности в цифровой среде, таких как вирусные атаки, несанкционированный доступ к информации, спам, перенаправление на фальшивые сайты;
- модуль цифровой грамотности показывает фактическое состояние цифровых компетенций населения, достаточный уровень которых является необходимым условием обеспечения информационной безопасности в условиях цифровизации;

• модуль финансовой грамотности отражает защищенность населения от имеющих информационную природу финансовых угроз, таких как мошенничество, отсутствие финансового планирования, нерациональные инвестиционные решения, панические покупки и др.

В случае, если рассчитанный индекс показателя больше или равен единице (≥ 1) можно говорить о соблюдении информационной безопасности по данному конкретному показателю. Отклонение индекса в сторону меньшую единице (< 1) диагностирует ситуацию нарушения защищённости информационного пространства.

Таблица 1. Показатели защищённости информационного пространства
Table 1. Information space security indicators

№	Модули/показатели
	Цифровая инфраструктура
1	Доля домохозяйств с широкополосным доступом к сети Интернет,%
2	Доля организаций, использующих доступ к сети Интернет со скоростью не менее 2 Мбит/с, %
3	Доля органов государственной власти и органов местного самоуправления, имеющих скорость передачи данных через Интернет не менее 2 Мбит/сек, %
	Информационная открытость организаций и учреждений
4	Доля организаций, имевших веб-сайт, %
5	Доля учреждений здравоохранения, имевших веб-сайт, %
6	Доля учреждений культуры, имевших веб-сайт, %
	Защищенность пользователей от киберугроз
7	Доля пользователей сети Интернет, не сталкивавшихся с проблемами информационной безопасности (вирусные атаки, несанкционированный доступ к информационным ресурсам, спам и др.), %
8	Доля пользователей сети Интернет, применяющих средства защиты информации, %
9	Доля организаций, использующих средства защиты информации, передаваемой по глобальным сетям, %
	Цифровая грамотность населения
10	Доля населения, активно использующего сеть Интернет, %
11	Доля населения, использующего сеть Интернет для получения государственных и муниципальных услуг, %
12	Доля населения, использующего сеть Интернет для заказа товаров и (или) услуг, %
	Финансовая грамотность населения
13	Доля школьников, принявших участие в мероприятиях по финансовой грамотности, %
14	Доля студентов СПО, принявших участие в мероприятиях по финансовой грамотности, %
15	Количество реализованных проектов по инициативному бюджетированию на 10 000 человек, ед.

Второй этап настоящего исследования заключался в нахождении субиндексов информационной безопасности для каждого модуля из табл. 1. Субиндекс определялся через нахождения среднего значения индексов отдельных показателей, входящих в модуль.

На третьем этапе был составлен рейтинг защищенности информационного пространства регионов России посредством суммирования субиндексов рассчитанных на предыдущем этапе работы.

Качество цифровой инфраструктуры является базовым условием оперативного осуществления комплекса необходимых действий с информацией посредством использования цифровых технологий. В свою очередь слабое развитие широкополосного доступа в сеть Интернет будет является физическим барьером для получения стейкхолдерами региона выгод и возможностей, которые предлагает цифровая среда. Результаты проведенной оценки уровня развития цифровой инфраструктуры на региональном уровне представлены в табл. 2. Наилучшее значение субиндекса в рамках данного модуля составляет 1,14 и принадлежит Тамбовской области. Наихудший ре-

зультат демонстрирует Чукотский автономный округ со значением 0,71. Отношение минимального и максимального значения развития цифровой инфраструктуры составляет 1,6 раза. Критерию обеспечения информационной безопасности соответствуют в расссматриваемом модуле 42 региона России.

Информационная открытость организаций и учреждений позволяет жителям регионов оперативно получать необходимую информацию обращаясь к интернет-сайтам данных структур. Это минимизирует такие угрозы в области информационной безопасности как мошенничество, распространение фейковой информации, отсутствие/нехватка необходимых данных. Оценка уровня информационной открытости организаций и учреждений регионов отражена в табл. 3. Лидером по данному критерию является Чеченская Республика со значением субиндекса 1,31, аутсайдером – Республика Калмыкия со значением 0,75. Дифференциация минимума и максимума в рамках модуля Информационная открытость организаций и учреждений составляет 1,7 раза. В 44 субъектах Федерации информационная открытость организаций различных видов экономической деятельности, а также учреждений здравоохранения и культуры находится в нормативном состоянии.

Таблица 2. Ранжирование регионов по уровню развития цифровой инфраструктуры
Table 2. Ranking of regions by level of digital infrastructure development

≥ 1,00	Тамбовская область, Чеченская Республика, Оренбургская область, Пермский край, г. Москва, Омская область, г. Санкт-Петербург, Мурманская область, Республика Адыгея, Сахалинская область, Магаданская область, Ставропольский край, Республика Алтай, Свердловская область, Кабардино-Балкарская Республика, Кемеровская область, Нижегородская область, Белгородская область, Владимирская область, Липецкая область, Челябинская область, Воронежская область, Тюменская область, Калининградская область, Московская область, Приморский край, Хабаровский край, Камчатский край, Республика Карелия, Республика Калмыкия, Томская область, Республика Северная Осетия – Алания, г. Севастополь, Республика Коми, Ярославская область, Новосибирская область, Удмуртская Республика, Ленинградская область, Курская область, Вологодская область, Астраханская область, Краснодарский край
≥ 0,75	Амурская область, Брянская область, Карачаево-Черкесская Республика, Республика Хакасия, Рязанская область, Ивановская область, Псковская область, Смоленская область, Тульская область, Калужская область, Алтайский край, Чувашская Республика – Чувашия, Архангельская область, Новгородская область, Республика Крым, Орловская область, Волгоградская область, Иркутская область, Ростовская область, Республика Татарстан, Тверская область, Самарская область, Ульяновская область, Республика Тыва, Республика Ингушетия, Красноярский край, Республика Башкортостан, Пензенская область, Республика Марий Эл, Саратовская область, Кировская область, Республика Саха (Якутия), Республика Мордовия, Республика Бурятия, Забайкальский край, Костромская область, Курганская область, Еврейская автономная область, Республика Дагестан
≥ 0,50	Чукотский автономный округ

Таблица 3. Ранжирование регионов по уровню информационной открытости организаций и учреждений
Table 3. Ranking of regions by the level of information openness of organizations and institutions

≥ 1,25	Чеченская Республика, Белгородская область
≥ 1,00	Магаданская область, Сахалинская область, Тамбовская область, Кемеровская область, Томская область, Чувашская Республика, Брянская область, Свердловская область, Нижегородская область, Ленинградская область, Чукотский авт.округ, Оренбургская область, Республика Коми, Ставропольский край, Московская область, г.Санкт-Петербург, Новгородская область, Хабаровский край, Тульская область, Тюменская область, Камчатский край, Республика Ингушетия, Калининградская область, Владимирская область, Республика Марий Эл, Республика Крым, Смоленская область, Омская область, Удмуртская Республика, Челябинская область, Рязанская область, Пермский край, Калужская область, Амурская область, Краснодарский край, Республика Карелия, Алтайский край, Мурманская область, Архангельская область, Республика Башкортостан, Ивановская область, Курганская область

Окончание таблицы 3

≥ 0,75	Ярославская область, Вологодская область, Республика Саха (Якутия), Пензенская область, г. Москва, Красноярский край, Ростовская область, Республика Адыгея, Новосибирская область, Республика Алтай, Забайкальский край, Псковская область, Тверская область, Астраханская область, Приморский край, Волгоградская область, Кабардино-Балкарская Республика, Самарская область, Кировская область, Саратовская область, Иркутская область, Республика Бурятия, г. Севастополь, Воронежская область, Карачаево-Черкесская Республика, Орловская область, Республика Татарстан, Республика Хакасия, Костромская область, Республика Мордовия, Курская область, Липецкая область, Республика Северная Осетия – Алания, Еврейская авт. область, Ульяновская область, Республика Дагестан, Республика Тыва, Республика Калмыкия

Защищенность от киберугроз напрямую зависит от уровня вредоносной активности, направленной злоумышленниками на пользователей, а также от поведения самих пользователей, в том числе применения современных антивирусных средств защиты информации. Последствия внедрения вредоносных программ в компьютер могут варьироваться от несущественного увеличения исходящего трафика до утраты критически важной информации пользователей или полной потери работоспособности компьютера. Диагностика защищенности пользователей от киберугроз в российских регионах выполнена в табл. 4. Наиболее безопасная среда в контексте рассматриваемых угроз определена в Кировской области со значением субиндекса 1,24. Наименьший уровень безопасности в соответствующей сфере диагностирован на уровне 0,7 в Чеченской Республике. Дифференциация между лидером и аутсайдером составляет 1,8 раза. Согласно полученным данным, в 53 регионах защищенность пользователей от киберугроз соответствует критериям обеспечения информационной безопасности.

Таблица 4. Ранжирование регионов по уровню защищенности пользователей от киберугроз
Table 4. Ranking regions by level of user protection against cyber threats

≥ 1,00	Кировская область, Чукотский автономный округ, Оренбургская область, Ярославская область, Тамбовская область, Республика Адыгея, Псковская область, Республика Крым, Республика Татарстан, Курская область, Кабардино-Балкарская Республика, Амурская область, Архангельская область, Удмуртская Республика, Брянская область, Омская область, Республика Коми, Саратовская область, Карачаево-Черкесская Республика, Республика Карелия, Астраханская область, Новосибирская область, Орловская область, Челябинская область, Тверская область, Хабаровский край, Алтайский край, Новгородская область, Сахалинская область, Кемеровская область, Свердловская область, Владимирская область, Костромская область, Калужская область, Белгородская область, Чувашская Республика – Чувашия, Забайкальский край, Волгоградская область, Республика Ингушетия, Ленинградская область, Смоленская область, Вологодская область, Ульяновская область, Пермский край, Нижегородская область, Воронежская область, Мурманская область, Республика Башкортостан, Иркутская область, Республика Марий Эл, Еврейская автономная область, Ростовская область, Тюменская область
≥ 0,75	Курганская область, Ставропольский край, Республика Мордовия, Ивановская область, г. Санкт-Петербург, Самарская область, Тульская область, Приморский край, Калининградская область, Красноярский край, Камчатский край, г. Севастополь, Магаданская область, Томская область, Республика Алтай, Московская область, Рязанская область, Республика Хакасия, Краснодарский край, Республика Калмыкия, Пензенская область, Республика Тыва, Республика Бурятия, г. Москва, Республика Саха (Якутия), Липецкая область, Республика Северная Осетия – Алания, Республика Дагестан
≥ 0,50	Чеченская Республика

Динамичное развитие информационно-коммуникационных технологий и их значительное влияние на все сферы жизни общества делает уровень цифровой грамотности существенным фактором обеспечения информационной безопасности региона. Оценка компетенций населения в области использования цифровых ресурсов отражена в табл. 5. Со значением субиндекса 1,35 лидером здесь является г. Москва, аутсайдером определен имеющий значение 0,63 Забайкальский край. Дифференциация между минимальным и максимальным значениями в рассматриваемой сфере составляет 2,1 раза. Согласно результатам проведенного анализа, только в 27 регионах Рос-

сии обеспечение информационной безопасности в разрезе цифровой грамотности соответсвует нормативному значению.

Финансовая грамотность и информационная безопасность тесно взаимосвязаны в вопросах получения актуальной финансово-экономической информации, операциях дистанционного банковского обслуживания, инвестициях при помощи цифровых платформ, взаимодействия с налоговыми органами, а также противодействия мошенничеству и фейкам. Цифровизация способствует росту благосостояния, достаточный уровень которого является необходимым условием для приобретения пользователями современных и дорогостоящих цифровых решений. Результаты оценки финансовой грамотности населения российских регионов представлены в табл. 6, согласно которой дифференциация между максимальным и минимальным значениями в рамках данного модуля составила 4,9 раза. Региональным лидером финансовой грамотности стала Республика Татарстан со значением соответствующего субиндекса 2,2. Последнее место занимает Волгоградская область со значением 0,45. В целом в 30 регионах Российской Федерации уровень финансовой грамотности соответствует нормативному значению.

Таблица 5. Ранжирование регионов по уровню цифровой грамотности населения
Table 5. Ranking of regions by the level of digital literacy of the population

≥ 1,25	г. Москва, Московская область
≥ 1,00	Мурманская область, Владимирская область, Тульская область, Астраханская область, Тюменская область, г. Санкт-Петербург, Оренбургская область, Республика Татарстан, Чеченская Республика, Республика Бурятия, Ростовская область, Краснодарский край, Республика Тыва, Воронежская область, Курская область, Саратовская область, Челябинская область, Волгоградская область, Ивановская область, Республика Карелия, Вологодская область, Омская область, г. Севастополь, Пензенская область, Нижегородская область
≥ 0,75	Кировская область, Камчатский край, Республика Саха (Якутия), Республика Башкортостан, Белгородская область, Тамбовская область, Томская область, Удмуртская Республика, Архангельская область, Республика Коми, Ярославская область, Брянская область, Пермский край, Республика Калмыкия, Калининградская область, Карачаево-Черкесская Республика, Липецкая область, Смоленская область, Чукотский автономный округ, Иркутская область, Свердловская область, Чувашская Республика – Чувашия, Сахалинская область, Хабаровский край, Курганская область, Новосибирская область, Костромская область, Псковская область, Республика Алтай, Самарская область, Приморский край, Кемеровская область, Республика Ингушетия, Ленинградская область, Ставропольский край, Новгородская область, Республика Дагестан, Алтайский край, Красноярский край, Амурская область, Кабардино-Балкарская Республика, Республика Крым, Магаданская область, Ульяновская область, Республика Хакасия, Республика Адыгея, Калужская область, Республика Марий Эл, Еврейская автономная область, Орловская область
≥ 0,50	Тверская область, Республика Мордовия, Рязанская область, Республика Северная Осетия – Алания, Забайкальский край

Среди первичных показателей наибольший разрыв между регионами наблюдается по количеству проектов инициативного бюджетирования на 10 000 человек населения и составляет порядка 1310 раз. Максимальное значение данного показателя принадлежит Вологодской области, минимальное – Астраханской области. Кроме того, в рассматриваемый период полностью отсутствовала практика инициативного бюджетирования в Еврейской автономной области, Республиках Северная Осетия – Алания, и Хакасия, а также Кабардино-Балкарской и Карачаево-Черкесской Республиках.

Рейтинг защищенности информационного пространства регионов России, представленный в табл. 7 определен посредством суммирования субиндексов рассчитанных для каждого модуля. При его расчёте субиндекс модуля финансовой грамотности учитывался с коэффициентом 0,33, т.к. финансовые компетенции являются частью предметных компетенций, куда также входят политико-правовые и культурно-исторические компетенции, рассмотрение которых не входило в задачи настоящего исследования. Прочие субиндексы учитывались с коэффициен-

том 1. Лидирующая позиция рейтинга принадлежит Тамбовской области, далее находятся г. Москва и Республика Татарстан. Последнее место рейтинга защищенности информационного пространства занимает Республика Северная Осетия – Алания. Дифференциация между максимальным и минимальным значениями рейтинга составляет 1,4 раза. Касаемо промежуточных результатов нашла подтверждение гипотеза что наибольшие межрегиональные различия будут представлены в границах модулей финансовой грамотности (в 4,9 раза) и цифровой грамотности (в 2,1 раза). Также данные модули показали наихудшие результаты с точки зрения количества регионов, имеющих в соответствующих аспектах не удовлетворительный уровень информационной безопасности.

Таблица 6. Ранжирование регионов по уровню финансовой грамотности населения
Table 6. Ranking of regions by the level of financial literacy of the population

≥ 2,00	Республика Татарстан, Республика Бурятия, Вологодская область, Новгородская область
≥ 1,50	Чувашская Республика – Чувашия, Тамбовская область, г. Москва, Костромская область
≥ 1,25	Республика Коми, Республика Ингушетия, Орловская область, Чукотский автономный округ, Республика Карелия, Белгородская область, Алтайский край
≥ 1,00	Амурская область, Ульяновская область, Республика Саха (Якутия), Калининградская область, Республика Башкортостан, Архангельская область, Московская область, Хабаровский край, Владимирская область, Республика Хакасия, Воронежская область, Ярославская область, Иркутская область, Республика Дагестан
≥ 0,75	Курская область, Сахалинская область, Ленинградская область, Псковская область, Калужская область, Удмуртская Республика, Брянская область, Республика Калмыкия, Рязанская область, Камчатский край, Тверская область, Курганская область, Самарская область, Кемеровская область, Республика Алтай, Кировская область, Магаданская область, Мурманская область, Тюменская область, Тульская область, Ставропольский край, Саратовская область, Забайкальский край, Липецкая область, г. Санкт-Петербург, Ивановская область, Челябинская область, Нижегородская область, Оренбургская область, Новосибирская область
≥ 0,50	Омская область, Краснодарский край, Пермский край, Кабардино-Балкарская Республика, Республика Адыгея, Республика Марий Эл, г. Севастополь, Ростовская область, Приморский край, Республика Крым, Чеченская Республика, Смоленская область, Свердловская область, Томская область, Республика Мордовия, Красноярский край, Карачаево-Черкесская Республика, Республика Тыва, Пензенская область, Еврейская автономная область, Республика Северная Осетия – Алания
≥ 0,25	Астраханская область, Волгоградская область

Таблица 7. Рейтинг защищенности информационного пространства регионов
Table 7. Rating of the information space security of the regions

№ в рейтинге / регион	Балл	№ в рейтинге / регион	Балл
1. Тамбовская область	5,051	42. Томская область	4,304
2. г. Москва	4,840	43. Пермский край	4,287
3. Республика Татарстан (Татарстан)	4,771	44. Алтайский край	4,276
4. Белгородская область	4,758	45. Ивановская область	4,260
5. Оренбургская область	4,732	46. Псковская область	4,245
6. Вологодская область	4,729	47. Ставропольский край	4,238
7. Московская область	4,698	48. Краснодарский край	4,222
8. Чувашская Республика – Чувашия	4,694	49. Саратовская область	4,222
9. Владимирская область	4,662	50. Ростовская область	4,200
10. Республика Коми	4,633	51. Костромская область	4,177
11. Новгородская область	4,587	52. Республика Адыгея (Адыгея)	4,168
12. Мурманская область	4,586	53. Смоленская область	4,164

Окончание таблицы 7

13. Республика Карелия	4,552	54. Новосибирская область	4,154
14. Сахалинская область	4,533	55. Республика Саха (Якутия)	4,139
15. г. Санкт-Петербург	4,510	56. Республика Алтай	4,125
16. Тюменская область	4,506	57. Иркутская область	4,123
17. Республика Бурятия	4,471	58. Республика Крым	4,122
18. Омская область	4,464	59. Кабардино-Балкарская Республика	4,115
19. Брянская область	4,459	60. Орловская область	4,112
20. Тульская область	4,454	61. г. Севастополь	4,109
21. Нижегородская область	4,447	62. Волгоградская область	4,107
22. Ярославская область	4,446	63. Калужская область	4,107
23. Чеченская Республика	4,415	64. Карачаево-Черкесская Республика	4,072
24. Челябинская область	4,412	65. Курганская область	4,045
25. Кемеровская область	4,408	66. Приморский край	4,012
26. Архангельская область	4,396	67. Тверская область	3,992
27. Удмуртская Республика	4,393	68. Самарская область	3,986
28. Чукотский автономный округ	4,392	69. Пензенская область	3,986
29. Хабаровский край	4,390	70. Рязанская область	3,950
30. Курская область	4,378	71. Липецкая область	3,946
31. Калининградская область	4,373	72. Республика Марий Эл	3,936
32. Воронежская область	4,366	73. Ульяновская область	3,928
33. Свердловская область	4,345	74. Республика Хакасия	3,917
34. Кировская область	4,337	75. Республика Калмыкия	3,908
35. Камчатский край	4,329	76. Красноярский край	3,858
36. Ленинградская область	4,318	77. Республика Тыва	3,841
37. Астраханская область	4,316	78. Забайкальский край	3,786
38. Амурская область	4,314	79. Республика Мордовия	3,686
39. Республика Ингушетия	4,309	80. Еврейская автономная область	3,630
40. Магаданская область	4,308	81. Республика Дагестан	3,621
41. Республика Башкортостан	4,305	82. Республика Северная Осетия – Алания	3,582

Таблица 8. Матрица парных коэффициентов корреляции
Table 8. Matrix of pairwise correlation coefficients

	Цифровая инфраструктура	**Информационная открытость**	**Защищённость от киберугроз**	**Цифровая грамотность**	**Финансовая грамотность**
Цифровая инфраструктура	1				
Информационная открытость	0,456493	1			
Защищённость от киберугроз	0,02833	0,156822	1		
Цифровая грамотность	0,280831	0,141934	–0,05717	1	
Финансовая грамотность	–0,09065	0,127154	0,201859	0,028874	1

Далее следует определить, насколько сбалансированно развиты различные составляющие информационной безопасности регионов страны. Предположим наличие диспропорций между развитием цифровой инфраструктуры, информационной открытости организаций и учреждений, защищённости от киберугроз, цифровой и финансовой грамотности, что будет свидетельствовать

о слабой управляемости процессом обеспечения информационной безопасности. Для определения степени взаимосвязи компонентов информационной безопасности использована матрица парных коэффициентов корреляции, отраженная в табл. 8.

В качестве выборки для расчета коэффициентов использованы рейтинги регионов страны в 5 модулях, составленные на основе ранжирования их субиндексов. Между цифровой инфраструктурой и информационной открытостью организаций и учреждений здравоохраннеия и культуры обнаружен средний уровень взаимосвязи. Согласно t-критерию Стьюдента линейный коэффициент корреляции является статистически значимым для данных модулей. Между всеми остальными рассмотренными модулями наблюдается низкий уровень взаимосвязи. Это подтверждает гипотезу о том, что обеспечение информационной безопасности в разрезе цифровизации различных сфер жизнедеятельности осуществляется стихийно и требует большей координации.

Заключение

Анализ и систематизация определений понятия информационная безопасность и исследовательских подходов к измерению данного явления, а также разработка методологии и методики оценки защищённости информационного пространства регионов и апробация данного инструментария позволили сделать следующие результаты:

1. Защищенность информационного пространства определена в качестве одного из значимых факторов экономической безопасности региона. Комплексный подход в трактовке понятия информационной безопасности выявлен в качестве универсального методологического инструмента, сочетающего в себе как технические, так и социально обусловленные (культурно-исторические, политико-правовые, финансовые и др.) аспекты данной проблематики. Разработанная индексно-рейтинговая методика оценки защищённости информационного пространства позволяет оценить вероятность реализации угроз экономической безопасности, имеющих информационный характер посредством изучения состояния цифровой инфраструктуры, информационной открытости организаций и учреждений, защищенности пользователей от киберугроз, цифровой и финансовой грамотности населения.

2. Между большинством компонентов информационной безопасности не прослеживается заметная взаимосвязь (средний уровень связанности обнаружен только между цифровой инфраструктурой и информационной открытостью организаций и учреждений). Данная ситуация свидетельствует, что обеспечение информационной безопасности в разрезе цифровизации различных сфер жизнедеятельности осуществляется стихийно и требует большей координации.

3. Межрегиональные диспропорции в развитии цифровых и предметных (финансовых) компетенций населения, необходимых для обеспечения информационной безопасности выше, чем аналогичные диспропорции в рамках прочих компонентов информационной защищенности (цифровая инфраструктура, наличие у организаций и учреждений Интернет-сайтов и применение пользователями антивирусного ПО). Также модули цифровых и финансовых компетенций показали наихудшие результаты с точки зрения количества регионов, имеющих в соответствующих аспектах не удовлетворительный уровень информационной безопасности.

Подводя итоги исследования следует отметить необходимость использования системного подхода в реализации политики управления информационной безопасностью на региональном уровне. Пропорциональное развитие всех компонентов информационной безопасности повысит эффективность использования выделяемых для этого ресурсов и обеспечит высокое качество защищенности информационного пространства.

Направления дальнейших исследований

Дальнейшие исследования в рамках данной проблематики будут направлены на уточение показателей диагностики информационной безопасности и методов их нормирования.

СПИСОК ИСТОЧНИКОВ

1. Александров А.В., Велигура А.В., Соколова Я.В. (2016) Методика комплексной оценки состояния информационной безопасности предприятия. *Экономический вектор*, 2 (5), 104–112.

2. Ахметьянова А.И., Кузнецова А.Р. (2016) Проблемы обеспечения информационной безопасности в России и ее регионах. *Фундаментальные исследования*, 8, 82–86.

3. Балог М.М., Демидова С.Е., Троян В.В. (2021) Влияние цифровизации экономики на рынок труда. *ЭТАП: экономическая теория, анализ, практика*, 5, 60–74.

4. Бойченко О.В., Иванюта Д.В. (2021) Модели информационной безопасности. *Экономика строительства и природопользования*, 3 (80), 33–39.

5. Брумштейн Ю.М., Подгорный А.Н. (2011) Информационная безопасность региона: анализ содержания термина, моделей оценки и некоторых вопросов управления. *Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика*, 1, 24–30.

6. Казанцев С.В. (2020) Жизнестойкость общества: показатели и оценка динамики. *Экономическая безопасность*, 3 (4), 457–468.

7. Кайгородцев А.А., Кайгородцева Т.Ф. (2020) Проблемы обеспечения информационной безопасности России в условиях цифровизации. *Society and Security Insights*, 3 (3), 79–89.

8. Малюк А.А., Милославская Н.Г. (2014) На пути к созданию теории защиты информации. *Вестник РГГУ. Серия: Документоведение и архивоведение. Информатика. Защита информации и информационная безопасность*, 11 (133), 35–66.

9. *Методика оценки угроз безопасности информации* (2021) [online] Available at: https://docs.cntd.ru/document/607699443 [Accessed 20.05.2023]. (in Russian)

10. Миков Д.А., Булдакова Т.И., Сюзев В.В., Смирнова Е.В., Бауман Ю.И. (2019) Модели оценки защищённости данных в информационно-управляющих системах реального времени. Проблемы современной науки и образования, 11-1 (144), 15–20.

11. Митрохина Е.Ю. (2014) *Информационная безопасность личности* (*социологический аспект*), монография, Москва: Российская таможенная академия.

12. Николаев А.А. (2007) Государственно-идеологическая компонента информационной безопасности. *Власть*, 4, 38–40.

13. Радионов М.В. (2015) Информационное общество и проблемы информационной безопасности: социологические проблемы исследования. *Гуманитарные, социально-экономические и общественные науки*, 6 (1), 186–190.

14. Рудакова Т.А., Бондаренко А.С. (2019) Инструментарий оценки информационной составляющей экономической безопасности предприятия. *Лизинг*, 6, 47–55.

15. Светлаков А.Г., Глотина И.М. (2018) Влияние информационного пространства на экономическую безопасность региона. *Экономика региона*, 14 (2), 474–484.

16. *Стандарт Банка России СТО БР ИББС-1.2-2014*. (2014) [online] Available at: https://cbr.ru/statichtml/file/59420/st-12-14.pdf [Accessed 25.05.2023]. (rus)

17. Шевко Н.Р., Хадиуллина Г.Н. (2019) Формирование системы показателей информационной безопасности российских регионов в условиях растущей неопределенности внешней среды. *Вестник Уфимского юридического института МВД России*, № 2 (84), 79–85.

18. Юнусова Д.А., Дахададаева А.А. (2022) Информационная безопасность региона. *Индустриальная экономика*, 5 (3), 458–463.

19. Balog M., Demidova S. (2021) Human Capital Development in the Context of the Fourth Industrial Revolution. *IOP Conference Series Earth and Environmental Science*, 666. DOI: https://doi.org/10.1088/1755-1315/666/6/062120

20. Tamegawa K., Ukai Y., Chida R. (2014) Macroeconomic Contribution of the Cloud Computing System to the Japanese Economy. *The Review of Socionetwork Strategies*, 9, 85–74. DOI: https://doi.org/10.1007/s12626-014-0047-7

21. Nicoletti G., von Rueden C., Andrews D. (2020) Digital technology diffusion: A matter of capabilities, incentives or both? *European economic review*, 128. DOI: https://doi.org/10.1016/j.euroecorev.2020.103513

22. Yip M., Shadbolt N., Tiropanis Th., et al. (2012) The digital underground economy: a social network approach to understanding cybercrime. *Digital Futures 2012: The Third Annual Digital Economy All Hands Conference, Aberdeen, United Kingdom*.

23. Ribaux O., Souvignet T.R. (2020) «Hello are you available?» Dealing with online frauds and the role of forensic science. *Forensic Science International: Digital Investigation*, 33. DOI: https://doi.org/10.1016/j.fsidi.2020.300978

24. Rymarczyk J. (2020) Technologies, Opportunities and Challenges of the Industrial Revolution 4.0: Theoretical Considerations. *Entrepreneurial Business and Economics Review*, 8 (1), 185–198. DOI:10.15678/EBER.2020.080110

25. Николаев М.А., Демидова С.Е., Балог М.М. (2018). *Методология управления экономической безопасностью на региональном уровне. Часть I: коллективная монография*. Псков: Псковский государственный университет.

REFERENCES

1. Aleksandrov A.V., Veligura A.V., Sokolova Ya.V. (2016) Metodika kompleksnoi otsenki sostoyaniya informatsionnoi bezopasnosti predpriyatiya. *Ekonomicheskii vektor*, 2 (5), 104–112.

2. Akhmet'yanova A.I., Kuznetsova A.R. (2016) Problemy obespecheniya informatsionnoi bezopasnosti v Rossii i ee regionakh. *Fundamental'nye issledovaniya*, 8, 82–86.

3. Balog M.M., Demidova S.E., Troyan V.V. (2021) Vliyanie tsifrovizatsii ekonomiki na rynok truda. *ETAP: ekonomicheskaya teoriya, analiz, praktika*, 5, 60–74.

4. Boichenko O.V., Ivanyuta D.V. (2021) Modeli informatsionnoi bezopasnosti. *Ekonomika stroitel'stva i prirodopol'zovaniya*, 3 (80), 33–39.

5. Brumshtein Yu.M., Podgornyi A.N. (2011) Informatsionnaya bezopasnost' regiona: analiz soderzhaniya termina, modelei otsenki i nekotorykh voprosov upravleniya. *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriya: Upravlenie, vychislitel'naya tekhnika i informatika*, 1, 24–30.

6. Kazantsev S.V. (2020) Zhiznestoikost' obshchestva: pokazateli i otsenka dinamiki. *Ekonomicheskaya bezopasnost'*, 3 (4), 457–468.

7. Kaigorodtsev A.A., Kaigorodtseva T.F. (2020) Problemy obespecheniya informatsionnoi bezopasnosti Rossii v usloviyakh tsifrovizatsii. *Society and Security Insights*, 3 (3), 79–89.

8. Malyuk A.A., Miloslavskaya N.G. (2014) Na puti k sozdaniyu teorii zashchity informatsii. *Vestnik RGGU. Seriya: Dokumentovedenie i arkhivovedenie. Informatika. Zashchita informatsii i informatsionnaya bezopasnost'*, 11 (133), 35–66.

9. *Metodika otsenki ugroz bezopasnosti informatsii* (2021) [online] Available at: https://docs.cntd.ru/document/607699443 [Accessed 20.05.2023]. (rus)

10. Mikov D.A., Buldakova T.I., Syuzev V.V., Smirnova E.V., Bauman Yu.I. (2019) Modeli otsenki zashchishchennosti dannykh v informatsionno-upravlyayushchikh sistemakh real'nogo vremeni. *Problemy sovremennoi nauki i obrazovaniya*, 11-1 (144), 15–20.

11. Mitrokhina E.Yu. (2014) *Informatsionnaya bezopasnost' lichnosti* (*sotsiologicheskii aspekt*)*, monografiya*, Moskva: Rossiiskaya tamozhennaya akademiya.

12. Nikolaev A.A. (2007) Gosudarstvenno-ideologicheskaya komponenta informatsionnoi bezopasnosti. *Vlast'*, 4, 38–40.

13. Radionov M.V. (2015) Informatsionnoe obshchestvo i problemy informatsionnoi bezopasnosti: sotsiologicheskie problemy issledovaniya. *Gumanitarnye, sotsial'no-ekonomicheskie i obshchestvennye nauki*, 6 (1), 186–190.

14. Rudakova T.A., Bondarenko A.S. (2019) Instrumentarii otsenki informatsionnoi sostavlyayushchei ekonomicheskoi bezopasnosti predpriyatiya. *Lizing*, 6, 47–55.

15. Svetlakov A.G., Glotina I.M. (2018) Vliyanie informatsionnogo prostranstva na ekonomicheskuyu bezopasnost' regiona. *Ekonomika regiona*, 14 (2), 474–484.

16. *Standart Banka Rossii STO BR IBBS-1.2-2014.* (2014) [online] Available at: https://cbr.ru/statichtml/file/59420/st-12-14.pdf [Accessed 25.05.2023]. (rus)

17. Shevko N.R., Khadiullina G.N. (2019) Formirovanie sistemy pokazatelei informatsionnoi bezopasnosti rossiiskikh regionov v usloviyakh rastushchei neopredelennosti vneshnei sredy. *Vestnik Ufimskogo yuridicheskogo instituta MVD Rossii*, № 2 (84), 79–85.

18. Yunusova D.A., Dakhadadaeva A.A. (2022) Informatsionnaya bezopasnost' regiona. *Industrial'naya ekonomika*, 5 (3), 458–463.

19. Balog M., Demidova S. (2021) Human Capital Development in the Context of the Fourth Industrial Revolution. *IOP Conference Series Earth and Environmental Science*, 666. DOI: https://doi.org/10.1088/1755-1315/666/6/062120

20. Tamegawa K., Ukai Y., Chida R. (2014) Macroeconomic Contribution of the Cloud Computing System to the Japanese Economy. *The Review of Socionetwork Strategies*, 9, 85–74. DOI: https://doi.org/10.1007/s12626-014-0047-7

21. Nicoletti G., von Rueden C., Andrews D. (2020) Digital technology diffusion: A matter of capabilities, incentives or both? *European economic review*, 128. DOI: https://doi.org/10.1016/j.euroecorev.2020.103513

22. Yip M., Shadbolt N., Tiropanis Th., et al. (2012) The digital underground economy: a social network approach to understanding cybercrime. Digital Futures 2012: *The Third Annual Digital Economy All Hands Conference*, Aberdeen, United Kingdom.

23. Ribaux O., Souvignet T.R. (2020) «Hello are you available?» Dealing with online frauds and the role of forensic science. *Forensic Science International: Digital Investigation*, 33. DOI: https://doi.org/10.1016/j.fsidi.2020.300978

24. Rymarczyk J. (2020) Technologies, Opportunities and Challenges of the Industrial Revolution 4.0: Theoretical Considerations. *Entrepreneurial Business and Economics Review*, 8 (1), 185–198. DOI:10.15678/EBER.2020.080110

25. Nikolaev M.A., Demidova S.E., Balog M.M. (2018). *Metodologiya upravleniya ekonomicheskoi bezopasnost'yu na regional'nom urovne. Chast' I: kollektivnaya monografiya*. Pskov: Pskovskii gosudarstvennyi universitet.

СВЕДЕНИЯ ОБ АВТОРАХ / INFORMATION ABOUT AUTHORS

БАЛОГ Михаил Михайлович
E-mail: seb5658@yandex.ru
Mikhail M. BALOG
E-mail: seb5658@yandex.ru
ORCID: https://orcid.org/0000-0001-8785-2780

БАБКИН Александр Васильевич
E-mail: al-vas@mail.ru
Aleksandr V. BABKIN
E-mail: al-vas@mail.ru

Поступила: 28.05.2023; Одобрена: 19.06.2023; Принята: 19.06.2023.
Submitted: 28.05.2023; Approved: 19.06.2023; Accepted: 19.06.2023.