РЕГИОНАЛЬНАЯ И ОТРАСЛЕВАЯ ЭКОНОМИКА

Балтийский экономический журнал. 2023. № 1(41). С. 4–16.
Baltic Economic Journal. 2023;(1(41)):4–16.

РЕГИОНАЛЬНАЯ И ОТРАСЛЕВАЯ ЭКОНОМИКА

Научная статья
УДК 338.22.021.4
https:// doi.org/10.46845/2073-3364-2023-0-1-4-16

Информационные технологии как объекты экономической безопасности

Сергей Михайлович Ежелый
ФГБОУ ВО "Калининградский государственный технический университет", Калининград, Россия
sergey.ezheliy@klgtu.ru

Аннотация. В статье рассматриваются вопросы экономической безопасности в связи с проблемой зависимости применяемых в России информационных технологий от иностранных производителей. Используется подход постановки информационных технологий в качестве объектов экономической безопасности информационной инфраструктуры, которая охватывает все экономические системы и государственное управление. На основе методологии выбора конкурентоспособных решений предложены прикладные решения для обеспечения защищенности национальных интересов.

Ключевые слова: экономическая безопасность, информационные технологии, информационная инфраструктура, методика

Для цитирования: Ежелый С. М. Информационные технологии как объекты экономической безопасности // Балтийский экономический журнал. 2023. № 1(4). С. 4-16. https:// doi.org/10.46845/2073-3364-2023-0-1-4-16

REGIONAL AND SECTORAL ECONOMY

Original article

Information technologies as objects of economic security

Sergey M. Ezheliy
Kaliningrad State Technical University, Kaliningrad, Russia
sergey.ezheliy@klgtu.ru

Abstract. The article discusses the issues of economic security in connection with the problem of dependence of information technologies used in Russia from foreign manufacturers. The approach of setting information technologies as objects of economic security of the information infrastructure, which covers all economic systems and public administration, is used. Based on the methodology of choosing competitively capable solutions, applied solutions are proposed to ensure the protection of national interests.

***Keywords**: economic security, information technology, information infrastructure, methodology*

***For citation**:* Ezheliy S. M. Information technologies as objects of economic security // Baltic Economic Journal. 2023;(1(41)): 4-16. https:// doi.org/10.46845/2073-3364-2023-0-1-4-16

Произошедшие в период 2020-2022 гг. события показали, что практически вся совокупность экономических систем стран, относимых к развитым (далее − "западным"), выведена из динамического равновесия. Для них экономическое развитие на ближайшую перспективу в возрастающей степени детерминируется изменением концептуальных взглядов в сторону глобально неофеодальных политических, идеологических, религиозно-культурных концептов в ущерб традиционным национальным экономическим рыночным воззрениям на выгодность и безопасность. В "западных" экономических системах прогнозируются такие процессы, как:

– нарастающее экономическое доминирование со стороны США с управляемым сокращением экономического суверенитета остальных стран;

– перераспределение потенциала реальной экономики "западных" экономических систем в пользу США за счет сокращения потенциала остальных;

– неравномерность увеличения стоимости ресурсов, нарастающая аритмия части бизнес-процессов, сокращение добавочной стоимости конечных продуктов для части "западных" экономик;

– сокращение экономической базы для обеспечения общественных благ, следствием которого будет эластичное сжатие финансирования социальных систем некоторых западных стран;

– создание иерархически сложной новой структуры американоцентричной группы экономических систем, нацеленных на активизацию внешней экономической экспансии и ужесточение конкурентной борьбы с внешними игроками.

Вышеназванные процессы становятся дополнительными внешними факторами, оказывающими негативное влияние на российскую экономику, находящуюся с 2022 г. в состоянии выживания ввиду наращивания "западных" антироссийских санкций и иных ограничений, направленных на ее подавление.

Проблемой исследования ставится совокупность прогнозируемых кризисных явлений в российской экономике, связанных с зависимостью информационно-телекоммуникационного комплекса России от зарубежных информационных и цифровых технологий, средств и систем обработки информации.

Востребованность тематики определяется усилиями по сохранению устойчивости экономики под возрастающим давлением санкций, достижению стратегических целей развития независимого информационного общества и цифровой экономики страны.

В рамках тематики исследования по вопросам сопряжения применения цифровых технологий и экономической безопасности промышленности проводили российские ученые-экономисты И. Л. Авдеева, С. Г. Грачев, О. В. Гудкова, О. А. Доничев, А. Б. Козлов, А. В. Полянин. В данной работе

информационные и цифровые технологии исследуются как предметы экономической безопасности в инфраструктурной сети, общей практически для всех экономических систем. Инфраструктурная сеть в случае ее условного вычленения рассматривается как информационно-технологический комплекс (далее - ИТК), который имеет те же черты, что и традиционно изучаемые оборонно-промышленный, агропромышленный и другие российские многоотраслевые комплексы.

Для проведения данного исследования применялись методы наблюдения, описания, сравнения, анализа, синтеза, экспертных оценок, математического моделирования.

ИТК в максимальной степени связан отношениями со всеми без исключения системами всех уровней, включая государственное управление, входя в них в качестве инфраструктурной сети. Общая схема ИТК [1] представлена на рисунке 1.

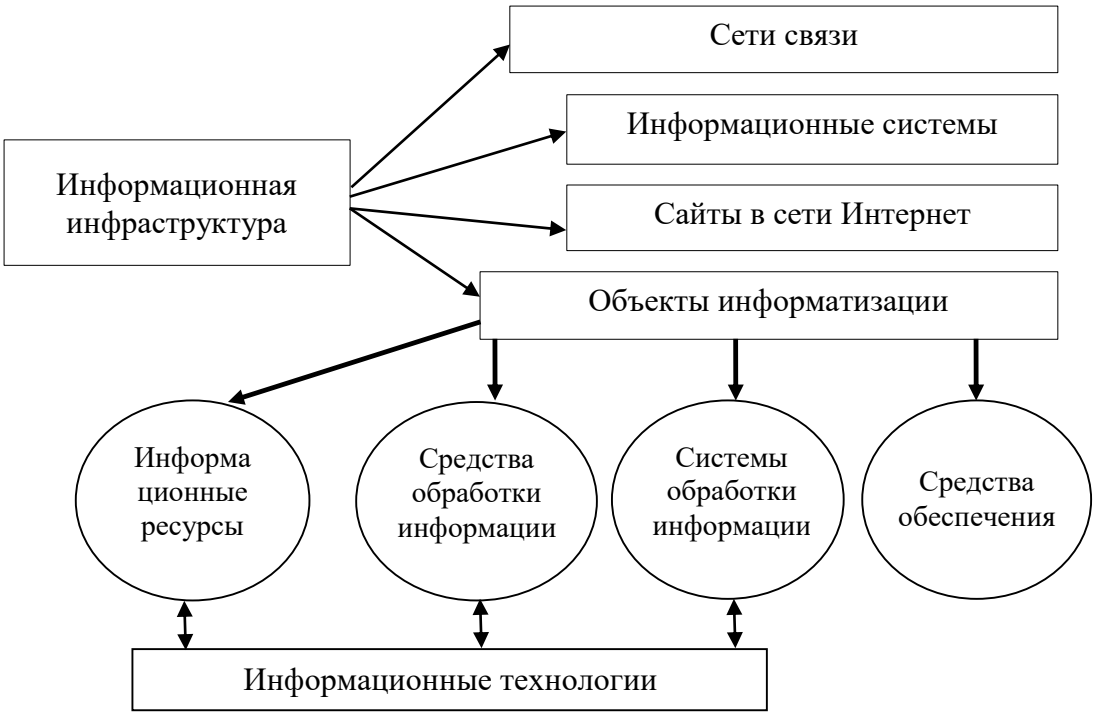

Рисунок 1 – Информационная инфраструктура
Figure 1 – Information infrastructure

Обязательным условием для нормального функционирования инфраструктуры является использование информационных ресурсов, средств и систем обработки информации в соответствии с заданной информационной технологией (далее – ИТ, ИТ-решения).

Технологии обработки информации в текущее время представляют собой сложный набор интеллектуальных и технических решений, включающий традиционные, аналоговые и цифровые решения.

Процессы, методы обработки информации, включающие ее поиск, сбор, хранение, обработку, предоставление, распространение, а также способы

осуществления таких процессов и методов, − суть информационные технологии [2].

Исследование экономических систем, управления ими и их взаимоотношений с точки зрения экономической безопасности даст высоковероятные прогностические выводы и предложит оптимальные прикладные решения только в случае учета влияния на них информационных технологий, а также изучения ИТ в качестве предмета. ИТ-решения воздействуют через информационные ресурсы, средства и системы обработки на объекты информатизации (реальные субъекты и объекты экономики национального, регионального, отраслевого и местного уровня), а через них – на всю информационную инфраструктуру страны.

Современные информационные технологии являются цифровыми и основаны на представлении сигналов дискретными полосами аналоговых уровней, а не в виде непрерывного спектра. Все уровни в пределах полосы представляют собой одинаковое состояние сигнала [3]. Естественно, что сами технические средства, а равно и их компоненты − аппаратный, программный и иные составляющие − стали отдельными родами товаров.

С точки зрения экономической безопасности существенными обстоятельствами и угрозами внешнего характера являются:

– значительная зависимость нашей страны от импортных поставок технологического и технического оборудования и аппаратных средств;

– зависимость от иностранных производителей автоматических средств управления технологическими процессами;

– зависимость от иностранных производителей систем управления базами данных и корпоративных информационных систем;

– отсутствие стратегии по снижению зависимости от иностранных государств по широкой номенклатуре товаров и услуг.

Правительства технологически развитых стран, включая США, часто используют технологии в качестве рычага, с помощью которого можно влиять на политику и действия других стран [4]. Зависимость от иностранных поставщиков важнейших военных компонентов и технологий и связанные с ними риски привлекли внимание и беспокойство США в 2010-х годах.

В этой связи представляется особо важным проанализировать практику работы действующих российских систем информационной и экономической безопасности, выработать предложения по совершенствованию системы.

Исследование состояния защищенности жизненно важных интересов включает в себя изучение всех аспектов протекания экономических процессов и динамики взаимоотношений, включая правовой, технико-технологический, организационно-административный и другие.

В нашей стране в целом сформирована система экономической безопасности, включающая сегмент информационной безопасности; приняты действенные стратегические политические документы, а также нормативные правовые акты, которые работают в текущих условиях, включая:

– Стратегию национальной безопасности Российской Федерации [5];

– Доктрину информационной безопасности Российской Федерации [1];

– Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы [7];

– Национальную программу "Цифровая экономика Российской Федерации" [9].

Анализ состояния защищенности интересов России по элементам, которые объединены информационными технологиями (см. рисунок 1), показывает наличие ряда системных угроз.

Специалисты в ИТ-решениях в открытых публикациях [10] говорят о ряде специализированных методов риск-менеджмента в информационной безопасности и кибербезопасности, базирующихся на стандартах, в частности, ГОСТ Р ИСО/МЭК 27001-2021 "Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования". Он идентичен международному стандарту ИСО/МЭК 27001:2013 (ISO/IEC 27001:2013). В России такие основополагающие документы приняты и используются с рядом особенностей. Как показал опрос экспертов в ИТ-сфере и изучение текстов стандартов, введенные в действие документы информационной и кибербезопасности почти во всех случаях являются аутентичным переводом на русский язык иностранных стандартов.

Федеральный орган власти Росстандарт продолжает участвовать в деятельности международных неправительственных организаций, которые разрабатывают международные стандарты и априори считаются непререкаемыми авторитетами. К таким организациям относятся:

1. ИСО (ISO) – Международная организация по стандартизации, расположена в Швеции. Стандарты в области информационной и кибербезопасности разрабатывает технический комитет "ISO/IEC JTC 1 Information Technology". Его особенностью является то, что секретариат комитета − Американский национальный институт стандартов (ANSI), председателем комитета до конца 2023 г. остается директор по стандартам корпорации INTEL Ф. Уэннблом (Ph. Wennblom).

2. Международная электротехническая комиссия (МЭК), расположена в Швейцарии. Является организацией, разрабатывающей стандарты в области информационной и кибербезопасности.

В настоящее время между ИСО и МЭК установлен полный консенсус по выработке стандартов. Действует объединенный технический комитет ИСО и МЭК (JTC 1) по информационным технологиям [13].

Также специалистами по информационной безопасности часто используются разработки в виде т. н. фреймворков, наименования которых начинаются аббревиатурой NIST. Данные документы опубликованы Национальным институтом стандартов и технологий Министерства торговли США (NIST – National Institute of Standards and Technology).

Очевиден факт доминирования интересов американских компаний в развитии формально международной кооперации в ИТ-сфере. В этой связи показательны результаты сравнения ситуации с разработкой национальных стандартов в сфере информационной безопасности и кибербезопасности "западных" и "восточных" экономических систем. Наибольшего развития ИТ-сфера получила в Китае и Индии. При этом, если индийские стандарты целиком

соответствуют международным стандартам ИСО и МЭК, то китайские документы, хотя и частично, связаны с международными, но в основном представляют собой самостоятельные наработки [11, 12].

Исходя из национальных интересов и понимания технического суверенитета России, необходима постепенная суверенизация стандартов и нормативных правовых актов на долгосрочной основе в виде совокупности программных мероприятий. Их реализация невозможна без научно-исследовательских и опытно-конструкторских работ, в том числе проводимых в конфиденциальном порядке.

Анализ состояния защищенности интересов России по средствам обработки информации (программному обеспечению) показывает, что нашим интересам и целям отвечает состояние, когда рынок, субъекты и объекты комплекса будут насыщены программами российского изготовления, т. е. выполненными аккредитованными российскими ИТ-компаниями с персоналом, являющимся резидентами Российской Федерации. Здесь необходимо учитывать сложившиеся условия и специфику трудовой деятельности разработчиков программ, мировую структуру соответствующих предприятий−разработчиков программ и распределения кадров [6], инвестиционные потоки в этой сфере, которые в интегрированном виде показывают динамику роста персонала (таблица 1). В состав персонала включены технические писатели, администраторы, инженеры по аппаратному обеспечению, программисты САПР, дата-сайнтисты, математики и пр. [14, 15].

Таблица 1 − Распределение работников информационно-телекоммуникационного комплекса, млн. чел.

Table 1 − Distribution of employees of the information and telecommunications complex, mln. people

Год	Общее количество персонала в ИТ-сфере		
	в целом в мире	в США	в России
2019 факт	26,4	4,2	1,4
2023 прогноз	27,7	4,3	1,7
2024 прогноз	28,7	4,4	2

Рынок труда ИТ-специалистов нестабилен практически во всех странах, наблюдаются резонансные и кризисные явления, перемежающиеся резким ростом кадрового дефицита и виртуальным или реальным перемещением кадров в страны, создающие наиболее благоприятные условия для работы. Эти явления связаны с изменениями стратегий крупнейших игроков, которые, как правило, являются резидентами США.

По предположению специализирующейся в ИТ-сфере консалтинговой компании "GARTNER" (США), в 2022 и 2023 гг. мировые расходы только на программное обеспечение поднимутся на 9,6 % (около 810 млрд. долл.) и 11,8 % (около 900 млрд. дол.) соответственно. Кроме того, ожидается рост продаж ИТ-услуг.

Поскольку любая российская ИТ-компания может привлечь на основе аутсорсинга, аутстафинга или в виде фрилансера специалиста из любой страны,

важным представляется понимание критериев "российское программное обеспечение" и "российская система обработки информации".

Для перехода к критериям необходимо оценить вероятности (риски) наступления ущерба в связи с применением иностранного компонента в программном обеспечении или системе обработки информации. Программное обеспечение и систему обработки будем называть "комплекс". Вероятность наступления экономического ущерба (события ζ) будем обозначать как $P(\zeta)$. Вероятность нахождения в комплексе некоего иностранного компонента (события ξ) будем обозначать как $P(\xi)$. Нам необходимо рассмотреть, какой ущерб может быть нанесен при использовании иностранного программного обеспечения, вероятность события применения иностранного компонента и связанного с ним ущерба $P(\xi \mid \zeta)$. В этом случае риск рассчитывается по формуле Байеса:

$$P(\xi \mid \zeta) = P(\zeta \mid \xi) \times P(\xi) / P(\zeta). \quad (1)$$

Если исходить из предположения, что иностранный компонент содержит заложенную ошибку, которая неизбежно повлечет значительный ущерб, то его нахождение в составе программного обеспечения нежелательно. Следовательно, для уменьшения риска долю иностранного компонента необходимо уменьшить до минимума. Целесообразно создавать в комплексе дублирующие параллельные пути решения задачи, стоящей перед программным обеспечением, т. е. наращивать долю российского компонента.

Уместно подчеркнуть, что вопросы четкого определения субъектов и объектов критической информационной инфраструктуры (КИИ) актуализированы в последние годы. Однако следует признать, что практически все объекты насыщены иностранным программным обеспечением (таблица 2).

Таблица 2 − Критерий и пороговые значения доли российского программного обеспечения, %

Table 2 − Criteria and thresholds for the share of Russian software, %

Показатель	Период		
	конец 2022 г.	конец 2023 г.	конец 2024 г.
Доля использования российского и евразийского ПО на значимых объектах КИИ по отрасли	не менее 10	не менее 40	не менее 100

Информация отражена в "Методических рекомендациях по формированию отраслевых планов мероприятий по обеспечению готовности заказчиков к преимущественному использованию российского программного обеспечения".

Планировавшиеся методики оценки показателей использования российского программного обеспечения и программного кода, их текущие и целевые значения фактически разработаны только в 2022 г. и трансформированы в вышеупомянутые "Методические рекомендации по формированию отраслевых планов …". В условиях 2020−2023 гг. основное направление работы − замещение на объектах критической информационной инфраструктуры иностранного программного обеспечения российским или евразийским.

Актуальные сведения о количестве действующих российских компаний, которые участвуют в разработке, наладке и реализации программного обеспечения [16], отражены в таблице 3.

Таблица 3 − Распределение действующих предприятий в отраслях (на 30.01.2023 г.)
Table 3 − Distribution of operating enterprises in industries (as of 30.01.2023)

№ п/п	Наименование вида деятельности, код по ОКВЭД-2	Количество компаний	
		всего	с выручкой свыше 2 млрд. руб.
1	Разработка компьютерного программного обеспечения, консультационные услуги в данной области и другие сопутствующие услуги	50037	211
	в т. ч. непосредственная разработка компьютерного программного обеспечения	31263	130
2	Деятельность в области информационных технологий	17078	50
3	Торговля оптовая информационным и коммуникационным оборудованием	10147	95

В целях защиты интересов страны был создан Реестр программного обеспечения, в который включаются ИТ-решения аккредитованных организаций. Кроме того, в нашей стране предприняты попытки интегрировать ИТ-компании, работающие в Евразийском экономическом союзе. В Реестр российского программного обеспечения по состоянию на 30.01.2023 г. включено 16077 единиц программного обеспечения от 5431 правообладателя. В Реестр евразийского программного обеспечения включено 67 единиц программного обеспечения от 23 правообладателей. Сопоставление данных таблицы 3 и отчетов по Реестрам свидетельствует о потенциале российской ИТ-сферы, который необходимо использовать в интересах страны и общества.

В условиях введения в отношении Российской Федерации санкций в ИТ-сфере угрозы блокирования работы ИТ-решений многократно возросли. В этой связи, как подчеркивают эксперты в области информационной безопасности, необходимо планомерно снижать зависимость от иностранного программного обеспечения, не допуская маятниковой ситуации с переходом зависимости в информационных технологиях от "западных" к "восточным" экономическим системам, которые рассматривают Россию только как рынок сбыта своих высокотехнологичных решений.

Самым существенным условием должна стать минимизация сроков исполнения задач, ставящихся политическим руководством страны перед федеральными и региональными органами власти, персональная ответственность должностных лиц.

Анализ состояния защищенности интересов России по системам обработки информации и средствам обеспечения сопряжен с исследованием состояния индустрии и промышленности, которые входят в информационно-телекоммуникационный комплекс в качестве инфраструктурной сети. Действующие в настоящее время хозяйствующие субъекты способны

изготовлять законченные производством объекты только с использованием импортного технологического и контрольно-измерительного оборудования. В этой связи реальные условия функционирования ИТ-предприятий вынудили ввести термин "минимально допустимый уровень локализации". Правительством РФ заданы параметры – такие уровни локализации, в соответствии со значениями которых телекоммуникационному оборудованию, изготовленному на территории РФ, может быть присвоен статус телекоммуникационного оборудования российского происхождения.

Применяемые технологические операции изображены на рисунке 2.

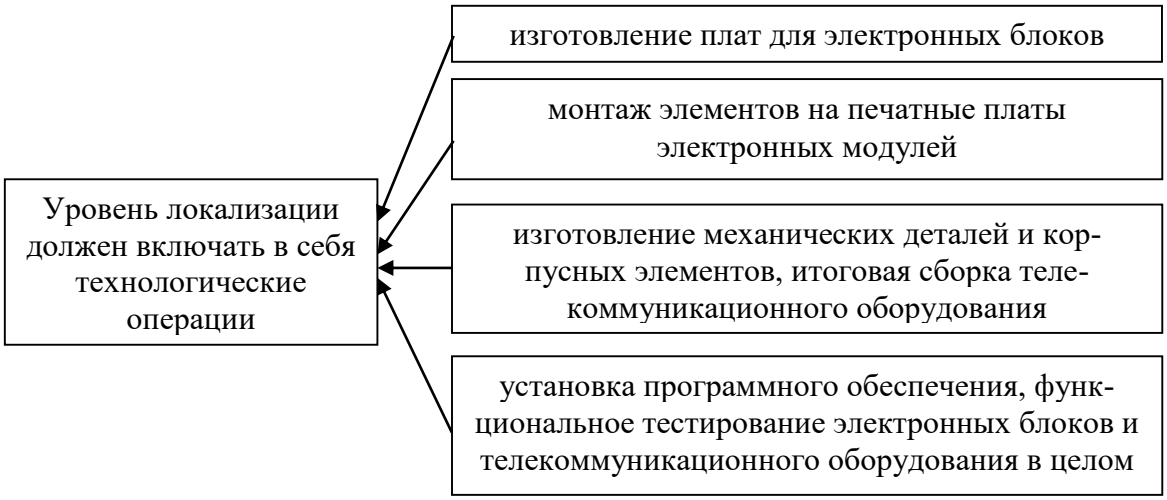

Рисунок 2 - Полнота использования на территории России технологических операций
Figure 2 - Completeness of the use of technological operations in Russia

Расчет значения уровня локализации УР осуществляется по формуле [8]:

$$У_Р = (\sum_{i=1}^{4} Т_i \cdot М_i) \cdot \left(1 + 2\frac{S_{is}}{S_\Sigma} + \frac{S_o}{S_\Sigma}\right), \quad (2)$$

где $Т_i$ − расчетный удельный вес технологической операции в структуре трудоемкости изготовления каждого вида телекоммуникационного оборудования.

Всего имеется 4 операции (рисунок 2); $М_i < 1$ − доля фактически изготовленного телекоммуникационного оборудования по каждой технологической операции. Ее расчет осуществляется по документам, регламентированным ГОСТ 3.1102-2011; S_{is} – стоимость интегральных схем российского производства; S_o − стоимость пассивных и дискретных элементов российского производства; S_Σ − суммарная стоимость сырья, материалов и комплектующих, используемых в телекоммуникационном оборудовании.

Для разных наименований и групп оборудования пороговые значения $У_Р$ – от 60 до 85 % [8].

Достижение порогового значения критерия определяется мнением межведомственного экспертного совета, который был создан при Минпромторге РФ в 2012 г., однако информация о том, кто именно считается экспертом, а также о его работе носит закрытый характер. Определенным опасным фактором,

который может исказить реальное положение дел по признанию оборудования российским, является отсутствие возможности тайного голосования экспертов.

Интересам страны отвечает стратегия индустриализации отрасли производства компьютеров, электронных и оптических изделий. Согласно "Общероссийскому классификатору видов экономической деятельности" (ОКВЭД-2), данная отрасль относится к классу 26, а также к группам 28.99.2, 33.13, 62.02.2, связанным с ИТ. В России сложилась диспропорция доходов между сегментом изготовления аппаратной части и сегментом разработки программного обеспечения. Угрозы системной зависимости от иностранных систем обработки информации могут быть купированы только системной деятельностью по разработке российских операционных систем [17].

Для возврата суверенной управляемости в ИТК России на основе методологии выбора конкурентоспособных решений в научно-технической деятельности крайне необходимыми для национальной экономической системы в целом и технически реализуемыми потребностями являются:

– восстановление промышленности полупроводников, производства элементной базы полупроводников;

– обеспечение постоянных и ритмичных поставок сырья редкоземельных элементов и другого сырья и полуфабрикатов.

Решения должны иметь стратегический характер, охватывать все хозяйственные комплексы и на первом этапе предусматривать некоторое сокращение рынка импортной бытовой компьютерной и другой электронной техники, протекционизм для отечественного производства и соответствующих товаров.

Автор полагает важным в перспективе 3−5 лет реанимировать работу по выработке ряда методических документов в информационно-телекоммуникационном комплексе. К таковым целесообразно отнести:

− критерии и оценки развития собственного производства компьютерной индустрии (класс 26, группы 28.99.2, 33.13, 62.02.2 по ОКВЭД-2);

− оценки показателей управления рисками информационной безопасности при интеграции в цифровую экономику стран блока БРИКС (Бразилия, Россия, Индия, Китай и ЮАР), их текущие и целевые значении ввиду перспективы расширения блока на 5-10 новых членов;

− оценки показателей безопасности межмашинного взаимодействия в рамках Евроазиатского экономического союза и стран блока БРИКС для киберфизических систем;

− оценки целевых показателей знаний информационной и кибербезопасности в рамках независимой квалификации образовательной системы;

− критерии хранения и недопущения модификации суверенных больших данных;

− оценки целевых значений показателей использования в рамках БРИКС больших данных;

− целевые значения показателей доли российской продукции и доли продукции российского изготовления в области информационной безопасности и кибербезопасности в условиях цифровой экономики;

− целевые значения показателей управления рисками кибербезопасности и информационной безопасности;

− целесообразность и критерии гармонизации с "западной" цифровой экономикой.

Учет выявленных угроз экономической безопасности в ходе реализации описанных негативных тенденций позволяет сделать существенные дополнения при вычислении обобщенного индекса экономической безопасности России. В текущих условиях возрастающее значение имеет "человеческий фактор" − наличие кадров, обладающих познаниями и навыками в области информационной безопасности и кибербезопасности, а также компетенциями у самого широкого круга лиц, получающих высшее образование либо проходящих переподготовку или получающих дополнительное образование. Для страны необходимы специалисты с высокой квалификацией и мотивом патриотизма.

Список источников

1. Указ Президента РФ от 05.12.2016 г. № 646 "Об утверждении Доктрины информационной безопасности Российской Федерации".

2. Федеральный закон от 27.07.2006 г. № 149-ФЗ (ред. от 29.12.2022) "Об информации, информационных технологиях и о защите информации" (с изм. и доп., вступ. в силу с 09.01.2023).

3. Сайт "Онлайн-карта слов и выражений русского языка". − https://kartaslov.ru/карта-знаний/Цифровые+технологии.

4. National Academies of Sciences, Engineering, and Medicine. 1995. Maximizing U.S. Interests in Science and Technology Relations with Japan: Report of the Defense Task Force. Washington, DC: The National Academies Press. https://doi.org/10.17226/9294/

5. Указ Президента РФ от 02.07.2021 г. № 400 "Об утверждении Стратегия национальной безопасности Российской Федерации".

6. Evans Data Corporation. - https://evansdata.com/company.

7. Указ Президента РФ от 09.05.2017 г. № 203 "О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы".

8. Приказ Минпромторга РФ от 20.08.2020 г. № 2775 "Об утверждении Требований по уровню локализации производства телекоммуникационного оборудования и Методики оценки уровня локализации производства телекоммуникационного оборудования в целях присвоения телекоммуникационному оборудованию статуса телекоммуникационного оборудования российского происхождения".

9. Паспорт Национальной программы "Цифровая экономика Российской Федерации" (утв. протоколом заседания президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 4 июня 2019 г. № 7).

10. Рахметов Р. Анализ международных документов по управлению рисками информационной безопасности / Р. Рахметов. – сайт компании "Хабр Блокчейн Паблишинг ЛТД" (Кипр). - https://habr.com/ru/post/495236.

11. Закон о национальной безопасности. Общая концепция национальной безопасности Китайской Народной Республики. − https://www.gov.cn/index.htm.

12. Закон о сетевой безопасности Китайской Народной Республики. − http://www.gov.cn/xinwen/2016-11/07/content_5129723.htm.

13. ISO and IEC Joint Technical Committee (JTC 1) for information technology, is a consensus-based, voluntary international standards group. − https://jtc1info.org.

14. Блог "Кадрового агентства IT and Digital". − https://dzen.ru/a/X_q4jq8ULwsXzdaM.

15. ИТ-кадры для цифровой экономики в России. Оценка численности ИТ-специалистов в России и прогноз потребности в них до 2024 г. / Ассоциация предприятий компьютерных и информационных технологий. Москва, 2020 г. − https://apkit.ru/files/it-personnel%20research_2024_APKIT.pdf.

16. Официальный сайт Федеральной налоговой службы РФ. Сервис "Прозрачный бизнес" − https://pb.nalog.ru.

17. Ежелый С. М., Ежелый Н. С. Некоторые проблемы экономической безопасности, связанные с развитием сквозных цифровых технологий // Балтийский экономический журнал. 2022. № 1(37). С. 4−16.

References

1. Decree of the President of the Russian Federation No. 646 dated 05.12.2016 "On the Approval of the Information Security Doctrine of the Russian Federation" (In Russ.).

2. Federal Law No. 149-FZ of 27.07.2006 (as amended on 29.12.2022) "On Information, Information Technologies and Information Protection" (with amendments and additions, intro. effective from 09.01.2023) (In Russ.).

3. The website "Online map of words and expressions of the Russian language". - https://kartaslov.ru/карта-знаний/Цифровые+технологии (In Russ.).

4. National Academies of Sciences, Engineering, and Medicine. 1995. Maximizing U.S. Interests in Science and Technology Relations with Japan: Report of the Defense Task Force. Washington, DC: The National Academies Press. https://doi.org/10.17226/9294/

5. Decree of the President of the Russian Federation No. 400 dated 02.07.2021 "On approval of the National Security Strategy of the Russian Federation" (In Russ.).

6. Evans Data Corporation. - https://evansdata.com/company/

7. Decree of the President of the Russian Federation dated 09.05.2017 No. 203 "On the Strategy for the development of the Information Society in the Russian Federation for 2017-2030" (In Russ.).

8. Order of the Ministry of Industry and Trade of the Russian Federation dated 08.20.2020 No. 2775 "On approval of the Requirements for the level of localization of telecommunications equipment Production and Methods for Assessing the level of localization of telecommunications equipment production in order to assign telecommunications equipment the status of telecommunications equipment of Russian origin". (In Russ.).

9. Passport of the National Program "Digital Economy of the Russian Federation" (approved by the minutes of the meeting of the Presidium of the Presidential Council for Strategic Development and National Projects dated June 4, 2019 No. 7). (In Russ.).

10. Rakhmetov R. Analysis of international documents on information security risk management – website of the company "Habr Block Chain Publishing LTD" (Cyprus). - https://habr.com/ru/post/495236 (In Russ.).

11. The Law on National Security. The general concept of national security of the People's Republic of China. - https://www.gov.cn/index.htm (In Chin.).

12. The Law on Network Security of the People's Republic of China. - http://www.gov.cn/xinwen/2016-11/07/content_5129723.htm (In Chin.).

13. ISO and IEC Joint Technical Committee (JTC 1) for information technology, is a consensus-based, voluntary international standards group. - https://jtc1info.org.

14. Web-blog of "HR-agency "IT and Digital". - https://dzen.ru/a/X_q4jq8ULwsXzdaM (In Russ.).

15. IT personnel for the digital economy in Russia. Estimation of the number of IT specialists in Russia and the forecast of the need for them until 2024 / Association of Computer and Information Technology Enterprises. –Moscow, 2020 - https://apkit.ru/files/it-personnel%20research_2024_APKIT.pdf (In Russ.).

16. Official website of the Federal Tax Service of the Russian Federation. ProZrachny Business service https://pb.nalog.ru. (In Russ.).

17. Ezhely S. M., Ezhely N. S. Some problems of economic security related to the development of end-to-end digital technologies // Baltic Economic Journal. 2022. 1(37):4-16. (In Russ.).

Статья поступила в редакцию 10.02.2023; одобрена после рецензирования 11.02.2023; принята к публикации 14.02.2023.
The article was submitted 10.02.2023; approved after reviewing 11.02.2023; accepted for publication 14.02.2022.