pISSN 2073-2872
eISSN 2311-875X

Экономическая политика государства

ПРОБЛЕМЫ ЦИФРОВИЗАЦИИ ПРОМЫШЛЕННОГО СЕКТОРА

Гилян Васильевна ФЕДОТОВА

доктор экономических наук, профессор кафедры менеджмента и финансов
производственных систем и технологического предпринимательства,
Волгоградский государственный технический университет, Волгоград, Российская Федерация
g_evgeeva@mail.ru
https://orcid.org/0000-0002-2066-8628
SPIN-код: 2353-5794

История статьи:
Получена 17.09.2018
Получена в доработанном виде 11.10.2018
Одобрена 07.11.2018
Доступна онлайн 15.02.2019

УДК 338.45
JEL: G21, G28, G29

Ключевые слова:
государство, цифровая экономика, промышленность, безопасность, угрозы

Аннотация

Тема. Построение новой модели экосистемы цифровой национальной экономики, которая будет способствовать выстраиванию партнерских отношений в процессах эксплуатации информационных ресурсов между организациями и развитию существующих систем обеспечения необходимого уровня экономической и информационной безопасности.

Цели. Оценка трансформации существующих систем промышленного сектора, обеспечивающих реализацию государственных программ цифровизации национальной экономики, а также ситуации в отрасли и анализ уровня цифровизации промышленного сектора.

Методология. Исследование проводится с применением методов логического и сравнительного анализа, графического представления информации и массивов данных, финансового анализа, трендового анализа, методов сопоставления, аналогии и систематизации, комплексного обзора академической и отраслевой литературы, статистической информации и оценки.

Результаты. В соответствии с процессами цифровизации отраслей промышленного сектора национальной экономики предложены направления дальнейшего развития и трансформации систем экономической безопасности, обеспечивающие бесперебойность и защиту информации онлайн-платформ. Для разработки предложенных направлений был проведен системный анализ динамики развития промышленного сектора, оценены результаты формирования системы ГИСП на базе Министерства промышленности и торговли РФ, рассмотрены основные целевые индикаторы Дорожной карты «Технет».

Область применения. Результаты исследования могут быть использованы для разработки будущих стратегических ориентиров планирования государственной экономической и промышленной политики России, ориентиров перспективного развития страны.

Выводы. Рассмотренные в данной статье направления развития и становления информационной платформы промышленности России вскрыли ряд проблем с безопасностью онлайн-систем, связанных с ее внедрением, которые необходимо решить в ближайшей перспективе.

Для цитирования: Федотова Г.В. Проблемы цифровизации промышленного сектора // Национальные интересы: приоритеты и безопасность. – 2019. – Т. 15, № 2. – С. 273 – 283.
https://doi.org/10.24891/ni.15.2.273

Специфика отечественной практики построения информационной экономики отражена в многочисленных исследованиях и публикациях, среди которых можно выделить таких авторов, как А.В. Боговиз, А.В. Болотин, А.В. Комарова, С.В. Лобода, Т.Н. Литвинова, И.А. Морозова, Ю.В. Рагулина, занимающихся вопросами модернизации, финансирования и контроля процессаов цифровизации общественного сектора [1, 2]. Среди зарубежных исследователей вопросам информатизации общественного сектора

уделили внимание А. Аристовник, А. Обадик, А. Насир, М. Шахзад, С. Анвар, С.И. Рашид и др. [3, 4]. Существующие на данный момент возможности и перспективы совершенствования процесса управления построением информационной экономики в современной России рассмотрены в трудах таких авторов, как А.А. Гонтарь, Т.Ю. Гавриленко, Ю.Г. Бондаренко, И.П. Проворова, Р.Р. Чугумбаев, Н.Н. Чугумбаева и др.[1] [5–8].

Однако, несмотря на обилие публикаций по смежным темам, вопросы цифровизации промышленного сектора в рамках модели информационной экономики до сих пор являются малоизученными. В аспекте разработки оптимизационной модели информационной экономики требуется пересмотр регламентированных на государственном уровне индикаторов развития промышленного сектора и их дополнение для повышения результативности реализации мероприятий по цифровизации промышленности.

На сегодняшний день известны три основных варианта развития цифровой экономики: #DigitizeEU (межгосударственная программа ЕС по модернизации промышленности, 2011 г.), Made in China 2025 (создана на основе INDUSTRY 4.0, 2013 г.), «Цифровая экономика» (российская национальная технологическая инициатива, 2017 г.) [1, 3].

Программа «Цифровая экономика» утверждена Правительством Российской Федерации в июле 2017 г., ее выполнение рассчитано до 2024 г.. Провозглашенный Правительством РФ переход к цифровой экономике представляет собой важный вектор развития современной государственной промышленной политики, которая должна обеспечивать необходимый уровень развития производственной сферы нашей страны. Процесс перехода и трансформации существующих систем организации деятельности предприятий всех сфер требует перестройки всей экономической модели в соответствии с требованиями четвертой промышленной революции и концепции «Индустрия 4.0».

России очень сложно трансформировать собственную промышленность под цифровую платформенную экономику, так как отсутствуют системы глобальных цифровых платформ, и только малая часть компаний имеет навык работы и выход на высокотехнологичные рынки. Безусловно, мы движемся в этом направлении, но на данный момент цифровизация затронула только информационно-коммуникационный сектор экономики, финансовую сферу, онлайн-торговлю [5].

Реализуемая сегодня политика информатизации промышленного сектора сводится к созданию единой государственной информационной системы промышленности (ГИСП) на базе Минпромторга России. В рамках данного сервиса создана единая кросс-отраслевая платформа B2B, на которой и проводится взаимодействие между участниками производственного цикла: предприятиями, институтами развития и инвесторами, отраслевыми ассоциациями, союзами, сертифицированными центрами, органами государственной власти. По итогам 2017 г. оборот электронной торговой площадки ГИСП составил 1 140 000 млн руб. Помимо сервиса торговли ГИСП предоставляет финансовые услуги, сервисы трансфера технологий и кадров, взаимодействия с органами государственной власти, информационные сервисы[2]. Сегодня ГИСП представляет собой единую цифровую инфраструктуру. Так, в 2017 г. она включала в себя: 868 мер государственной поддержки для всех предприятий; 256 регионально значимых предприятий; 44 промышленных предприятия; 197 системообразующих предприятий; 783 предприятия по отраслям; 6 809 промышленных продуктов; 9 821 объект

[1] *Гонтарь А.А.* Нейросетевое моделирование в оценке уровня экономической безопасности систем: материалы Смотра-конкурса научных, конструкторских и технологических работ студентов Волгоградского государственного технического университета. Волгоград: Изд-во Волгоградского гос. техн. ун-та, 2018. С. 181–182.

[2] Там же.

инжиниринговой деятельности; 103 913 пользователей.

В процессе цифровизации национальной экономики важную роль играет государство, которое обеспечивает нормативно-правовое сопровождение и финансирование данных проектов. Так, согласно постановлению Правительства РФ «О реализации Национальной технологической инициативы» от 18.04.2016 № 317 разработан план мероприятий «Дорожная карта «Технет», который четко определяет целевые ориентиры развития цифрового и интеллектуального производства. Если дорожная карта будет реализована, то к 2035 г. Россия сможет войти в топ-10 стран мира, внедривших производственные передовые технологии в свой промышленный сектор. Основными индикаторами процесса цифровизации станут ключевые целевые показатели дорожной карты (*табл. 1*).

Оценка целевых индикаторов дорожной карты цифровизации промышленности России показывает, что Россия ставит вполне достижимые цели для выхода на мировой рынок IT-технологий и реализации собственной информационной перестройки производственного комплекса. Также стоит подчеркнуть, что цифровизация промышленности России представляет собой стратегическое направление деятельности государства, которое является интегратором происходящих процессов, одновременно контролируя весь ход перехода на онлайн-платформу. В этом процессе именно государство будет играть роль интегратора, инициировать создание инфраструктуры цифровизации и обеспечивать доступность системы для потенциальных участников, а компании – уже сами развивать цифровую промышленность.

Однако в данной ситуации следует учесть все риски и угрозы, сопровождающие структурную перестройку экономических субъектов. Основными рисками выступают атаки кибермошенников – итоги одного только 2016 г. показали значительный рост атак и взломов информационных систем различных предприятий и организаций. В связи с этим имеется необходимость оценки существующих рисков и вызовов, связанных с расширением спектра и сферы цифровых услуг, в том числе в промышленности.

В условиях реализации программы «Цифровая экономика» нужна трансформация существующих подходов к обеспечению экономической безопасности предприятия. Особую актуальность приобретает задача создания системы мониторинга, анализа и оценки уровня экономической безопасности производственной системы, в основе которой лежит модель экономической безопасности[3] [9].

Отрасли промышленности крайне неоднородны и сложны для управления и организации производственного процесса. Они включают в себя помимо производственного сектора также добывающий, перерабатывающий и обрабатывающий секторы. Более того, сами подотрасли дифференцируются между собой масштабом, номенклатурой и сложностью производимой продукции, длительностью производственного цикла, сложностью или серийностью продукции, особенностями ее транспортировки и реализации, наличием огромного количества подрядчиков. Если всю данную систему перевести на онлайн-платформу, то при ее сбое или взломе может возникнуть состояние хаоса, но при этом можно существенно оптимизировать данную цепочку, усилить контроль на всех этапах производственного цикла.

В то же время достаточно сложно оценить всю промышленность в целом и сделать выводы по ее организации. Для этого воспользуемся унифицированными показателями оценки развития промышленного сектора[4] [4]. В качестве такого показателя можно привести индикатор, применяемый Росстатом на протяжении многих лет – индекс

[3] Там же.

[4] «Лаборатория Касперского»: злоумышленники стали чаще атаковать пользователей MAC-устройств. URL: https://kaspersky.ru/blog/kaspersky-top3-2017/19713

промышленного производства, то есть динамику темпов роста за период по сравнению с прошлым аналогичным периодом (*рис. 1*).

Оценка развития промышленного сектора России по индексу промышленного производства за 2014–2018 гг. показывает неоднозначные результаты. Так, в январе 2014 г. рост показателя составил 101,1%, затем в январе 2016 г. он упал до уровня 99,5%, а в январе 2018 г. составил 102,4%. В целом динамика за исследуемый период позитивная, хотя если рассматривать темпы роста в разрезе укрупненных подотраслей, можно заметить, что не во всех сферах тенденция является положительной[5].

Из данных *рис. 1* видно, что в добывающей отрасли за рассматриваемый период показатель темпа роста снизился и упал до уровня 100,8% в январе 2018 г. Это связано прежде всего с тем, что Россия пыталась сократить экспорт сырья на международный рынок[6]. Это подтверждает и темп роста обрабатывающей промышленности, который вырос до уровня 104,3% в январе 2018 г. по сравнению с 101,6% в 2014 г. Улучшилась ситуация с обеспечением газом, электроэнергией, паром, кондиционированным воздухом – рост показателя достиг 99,3% в январе 2018 г. по сравнения с уровнем 2014 г. (98,9%). Показатель роста отрасли «Водоснабжение, водоотведение, организация сбора и утилизация отходов, ликвидация загрязнения» в январе 2018 г. упал до уровня 94,5% по сравнению с январем 2014 г. (96,7%). Таким образом, можно заключить, что рост общего показателя произошел в основном за счет перерабатывающей отрасли[7].

Подводя итог оценке динамики роста промышленного сектора, заметим, что отрасль трансформируется и переходит от добычи к переработке, что является свидетельством нового качественного уровня производства, что требует пересмотра существующих промышленных информационных платформ. Как правило, происходит переход на онлайн-платформы, но в данном случае неизбежно будет возникать другая проблема – обеспечение безопасности данных такой цифровой среды. Встает масса вопросов, связанных с сохранностью данных, с ростом угроз пользователям, бизнесу, государству, ростом компьютерной преступности, низким уровнем развития и конкурентоспособности отечественных телекоммуникационных технологий, недостатком квалифицированных кадров в данной области[8] [9]. Для решения перечисленных проблем в Стратегии развития цифровой экономики государство отдельным направлением выделяет вопрос обеспечения информационной безопасности. Основными принципами формирования безопасной информационной среды являются[9]:

– единство, устойчивость и безопасность информационно-телекоммуникационной инфраструктуры России во всем информационном пространстве;

– формирование нормативно-правовой базы для защиты гражданина, бизнес-единицы, государства в цифровом пространстве;

[5] Обзор несанкционированных переводов денежных средств за 2017 г. Данные Банка России. URL: http://cbr.ru/statichtml/file/14435/survey_transfers_17.pdf; Топ-10 тенденций развития биометрических технологий и цифровой идентификации в 2017 году. URL: https://marketer.ua/top-10-tendentsij-rozvitku-biometrichnih-tehnologij-i-tsifrovoyi-identifikatsiyi-v-2017-rotsi

[6] Threats to Food Security of the Russia's Population in the Conditions of Transition to Digital Economy. URL: https://link.springer.com/content/pdf/bfm%3A978-3-319-75383-6%2F1.pdf; *Абдуев Т.Э., Федотова Г.В.* Анализ рынка промышленного производства России: материалы VI международной научно-практической конференции «Современные подходы к трансформации концепций государственного регулирования и управления в социально-экономических системах». Курск: Изд-во Юго-Западного гос. ун-та, 2017. С. 6–9.

[7] Там же.

[8] *Федотова Г.В., Церенова Б.И.* Управление эффективностью экономических систем в условиях перехода к цифровой экономике: материалы международной научно-практической конференции «Актуальные проблемы менеджмента: производительность, эффективность, качество». СПб: Изд-во Санкт-Петербургского гос. ун-та, 2017. С. 69–71.

[9] Официальный сайт Федеральной службы государственной статистики. URL: http://gks.ru/wps/wcm/connect/rosstat_main/rosstat/ru/statistics/accounts

– формирование условий, обеспечивающих лидерство РФ на мировых рынках IT-технологий к 2024 г.;

– повышение до 75% доли субъектов экономики, применяющих стандарты безопасности при взаимодействии в онлайн бизнес-среде;

– снижение доли внутреннего сетевого трафика сети Интернет посредством иностранных серверов до 5%.

Итак, основным вектором повышения информационной, в том числе и экономической безопасности, должен стать переход преимущественно на российское программное обеспечение и оборудование, отечественные технологии поддержания целостности, конфиденциальности, аутентификации, защиты информации и данных с применением отечественных криптографических стандартов[10].

Для перевода промышленности на работу по принципам «Индустрии 4.0» помимо создания централизованной информационной платформы ГИСП была создана рабочая группа, в состав которой вошли лидеры отрасли электроники и информационной безопасности – компании «СТАН», «Лаборатория Касперского», НПП «Итэлма». В рамках созданной рабочей группы по совместной инициативе Минпромторга России и ведущих инновационных компаний (НПП «ИТЭЛМА», «Лаборатория Касперского», «Сименс», «СТАН») разработана базовая модель концепции «4.0 RU»[11] [2, 10].

Особенностью построения российского промышленного цифрового пространства является целый комплекс цифровых технологий, предполагаемый к внедрению на всех этапах промышленного производства. В качестве примера цифровизации приведем опыт ОК «РУСАЛ», которая приступила к сквозной цифровизации всех структурных подразделений и филиалов компании. Сквозная цифровизации складывается из трех направлений: 1) максимального наполнения процессов контрольно-измерительными приборами (датчиками, сенсорами, аппаратурой); 2) внедрения специализированных программных комплексов (MES-систем) для управления и синхронизации производственных процессов; 3) внедрения и совершенствования корпоративных систем. Кроме того, на некоторых предприятиях компании совместно с Yandex Data Factory запущены и проходят испытания проекты по искусственному интеллекту и машинному обучению[12]. Подобная киберфизическая среда дает возможность для оптимизации времени производственного цикла, улучшает степень гибкости производства продукции, повышение конкурентоспособности российского промышленного сектора. Поставленные задачи частично решаются посредством установления антивирусных программ, которые в то же время имеют определенные недостатки и не гарантируют 100%-ной защиты баз данных в информационной среде. Именно поэтому необходим комплексный подход к формированию системы информационной безопасности [6].

Основным поставщиком систем безопасности для российского цифрового пространства выбрана «Лаборатория Касперского», которая по итогам 2017 г., приняв участие в 86 независимых тестах и обзорах, в 72 тестах заняла 1-е место и 78 раз вошла в тройку лучших компаний аналогичного направления. Основные лидеры рейтинга представлены в *табл. 2*.

По данным аналитических исследований «Лаборатории Касперского», в современных информационных системах корпоративных структур, в том числе промышленных, основную угрозу составляют целевые кибератаки и сложные угрозы.

[10] О Стратегии социально-экономического развития Волгоградской области до 2025 г.: Закон Волгоградской области от 21.11.2008 № 1778-ОД.
URL: http://base.garant.ru/20139355/#ixzz4LlMUClGc

[11] Критерии и показатели оценки уровня экономической безопасности кредитной организации, 2016.
URL: http://bavari.ru/stufs-667-3.html

[12] Цифровизация промышленности. Опыт РУСАЛА. URL: https://integration24.ru/2018/06/09/cifrovizaciya-romyshlennosti-opyt-rusala

Особенностью целевых кибератак является их длительность – они могут продолжаться неделями, месяцами и даже годами, оставаясь незамеченными, и все это время их организатор будет собирать информацию и находить новые способы использования уникальных уязвимостей в системе «жертвы». В отличие от обычного вредоносного ПО, целевые атаки осуществляются под активным контролем и управлением злоумышленника. Преступники стремятся закрепиться внутри корпоративного периметра и получить незаметный и зачастую полный контроль над системами. Организаторы таких атак терпеливо и очень тщательно исследуют жертву и готовы ждать, пока их старания не будут щедро вознаграждены. Успеху злоумышленников, ведущих целевые атаки против IT-инфраструктур, способствует ряд ключевых факторов, включая следующие [7, 8]:

- отсутствие профилактики и завышенная оценка возможностей имеющейся защиты;
- недостаточная осведомленность сотрудников о рисках информационной безопасности;
- непрозрачность IT-среды и в особенности сетевой маршрутизации;
- собственное и устаревшее ПО и операционные системы;
- отсутствие у специалистов по безопасности знаний в области исследования вредоносных программ, цифровой криминалистики, реагирования на инциденты и аналитики угроз.

Основная масса простых киберугроз устраняется и блокируется традиционными технологиями формирования системы безопасности, основанными на основе сигнатур и/или элементов эвристического анализа, однако сегодня хакеры и киберпреступники проводят все более сложные атаки, нацеленные на конкретные промышленные предприятия. Современные целевые атаки, в том числе APT-класса, представляют собой одну из наибольших опасностей для предприятий. В то время как угрозы – и приемы, которыми пользуются хакеры и киберпреступники – развиваются, многие предприятия не адаптируют к ним собственную стратегию обеспечения безопасности. Целевые атаки и комплексные угрозы становится все труднее обнаруживать и зачастую еще труднее устранять, поэтому для борьбы с ними требуется комплексная и гибкая стратегия[13].

В качестве решения может послужить адаптивная стратегия обеспечения безопасности, представленная наиболее перспективной защитной архитектурой. Такой подход предполагает циклическое выполнение действий в четырех основных областях:

1) *предотвращение* – снижение риска комплексных целевых атак;
2) *обнаружение* – выявление действий, которые могут свидетельствовать о ведении целевой атаки;
3) *реагирование* – устранение брешей в системе безопасности и расследование атак;
4) *прогнозирование* – предположение о том, где и когда ожидать новых целевых атак.

В завершении отметим, что процесс трансформации систем информационной безопасности промышленных предприятий представляет собой сложную процедуру перехода всего производственного цикла на цифровую платформу. При наличии преимуществ такого перехода (оптимизация производственного цикла, полная прозрачность производства, сокращение времени на переговоры и поиск контрагентов) существуют и угрозы роста вероятности кибератак на информационные системы. Именно поэтому вопросы обеспечения информационной безопасности должны стать

[13] «Лаборатория Касперского»: злоумышленники стали чаще атаковать пользователей MAC-устройств. URL: https://kaspersky.ru/blog/kaspersky-top3-2017/19713/; Критерии и показатели оценки уровня экономической безопасности кредитной организации, 2016. URL: http://bavari.ru/stufs-667-3.html

первоочередными при запуске данной платформы. Отечественный производитель решений безопасности – компания «Лаборатория Касперского» ведет работу в данном направлении и проводит исследования изменения характера кибератак. Их результаты показали, что единого решения по безопасности нет, здесь необходим комплексный подход и постоянное обновление защитных технологий.

Таблица 1
Целевые показатели Дорожной карты «Технет»

Table 1
Benchmark indicators of TechNet Road Map

Показатель	**2017**	**2018**	**2019 (прогноз)**	**2025 (прогноз)**	**2035 (прогноз)**
Доля России на мировых рынках «Фабрик будущего» в сегменте инжиниринга и конструирования, %	0,3	0,4	0,5	0,9	1,5
Количество компаний – поставщиков услуг по созданию «Фабрик будущего» в рейтинге топ-50 технологических газелей РФ, ед.	–	1	3	10	20
Позиция России в Global Manufacturing Competitiveness Index (или сопоставимый), место	33	30	28	20	10
Объем экспорта продукции, полученный с использованием ППТ, тыс. руб.	–	–	1 500 000	80 000 000	800 000 000
Число созданных «Фабрик будущего» «Технет», ед.	–	3	5	17	40
Число создаваемых испытательных полигонов (TestBeds) «Фабрик будущего», ед.	2	3	4	10	25
Количество экспериментальных цифровых центров (лабораторий) сертификации РФ, ед.	–	1	3	10	15
Число специалистов, прошедших программы подготовки и переподготовки по передовым производственным технологиям	Менее 200	1 000	2 000	20 000	50 000

Источник: официальный сайт Министерства промышленности и торговли РФ.
URL: http://minpromtorg.gov.ru

Source: The official website of the Ministry of Industry and Trade of the Russian Federation.
URL: http://minpromtorg.gov.ru (In Russ.)

Таблица 2
Наиболее эффективные поставщики решений безопасности по итогам 2017 г.

Table 2
The most effective suppliers of security solutions following 2017

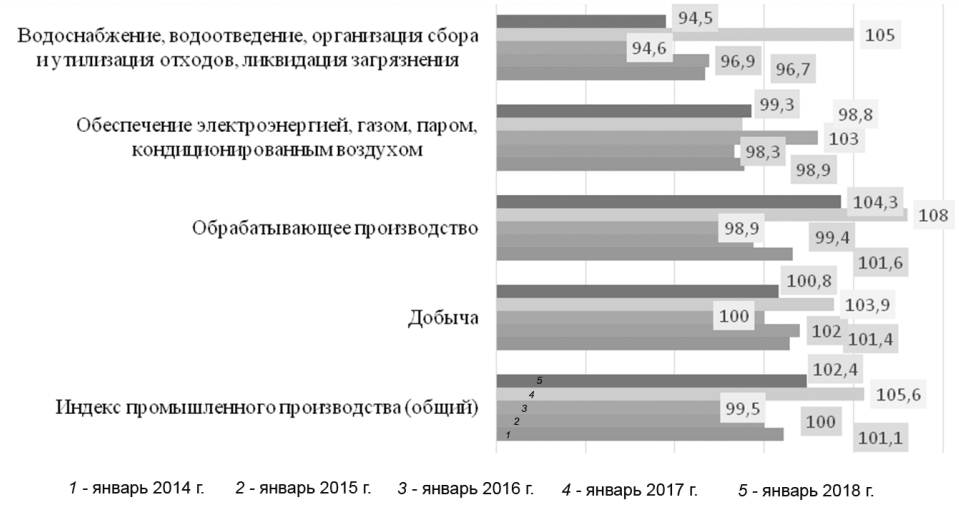
Компания	Количество пройденных тестов	Количество мест в ТОП-3	Доля мест в ТОП-3, %	Количество первых мест
Лаборатория Касперского	86	78	91	72
BitDefender	61	44	72	36
Symantec	66	40	61	27
Trend Micro	68	32	47	28
ESET	60	31	52	18
Avast	50	19	38	14
AVG	42	14	33	9
Sophos	30	13	43	8
Avira	32	12	38	7
GData	38	11	29	11
McAfee	45	11	24	9
F-Secure	37	4	11	4
Microsoft	38	–	–	–

Источник: составлено автором по материалам «Лаборатории Касперского».
URL: https://kaspersky.ru/blog/kaspersky-top3-2017/19713

Source: Authoring based on Kaspersky Lab data.
URL: https://kaspersky.ru/blog/kaspersky-top3-2017/19713 (In Russ.)

Рисунок 1
Темпы роста промышленного сектора РФ за период 2014–2018 гг., %

Figure 1
The growth rate of the industrial sector of the Russian Federation, 2014–2018, percentage points



Источник: официальный сайт Федеральной службы государственной статистики.
URL: http://gks.ru/wps/wcm/connect/rosstat_main/rosstat/ru/statistics/enterprise/industria

Source: The official website of the Federal State Statistics Service.
URL: http://gks.ru/wps/wcm/connect/rosstat_main/rosstat/ru/statistics/enterprise/industrial (In Russ.)

Список литературы

1. *Bogoviz A.V., Ragulina Y.V., Morozova I.A., Litvinova T.N.* Experience of Modern Russia in Managing Economic Growth. In: Studies in Systems, Decision and Control. Vol. 135. Springer, 2018, pp. 147–154.
2. *Bogoviz A.V., Ragulina Y.V., Komarova A.V. et al.* Modernization of the Approach to Usage of Region's Budget Resources in the Conditions of Information Economy Development. *European Research Studies Journal*, 2017, vol. 20, iss. 3, pp. 570–577. URL: https://ersj.eu/dmdocuments/2017-xx-3-b-53.pdf
3. *Aristovnik A., Obadić A.* The Impact and Efficiency of Public Administration Excellence on Fostering SMEs in EU Countries. *Amfiteatru Economic*, 2015, vol. 17, no. 39, pp. 761–774.
4. *Nasir A., Shahzad M., Anwar S., Rashid S.* Digital Governance: Improving Solid Waste Management Through ICT Reform in Punjab. ICTD' 17 Proceedings of the Ninth International Conference on Information and Communication Technologies and Development. ACM, 2017. URL: https://doi.org/10.1145/3136560.3136600
5. *Бондаренко Ю.Г.* Підвищення ефективності державного управління в інвестиційній діяльності // Актуальні Проблеми Економіки. 2015. Т. 172. № 10. С. 89–94.
6. *Гавриленко Т.Ю., Проворова И.П.* Сетевая экономика как феномен информационного общества // Российский технологический журнал. 2016. № 1. С. 53–61.
7. *Чугумбаев Р.Р., Чугумбаева Н.Н.* Маржинальный анализ гудвилла как инструмент экономического обоснования инноваций социального совершенствования // Человек. Общество. Инклюзия. 2017. № 2. С. 108–119.
8. *Чугумбаев Р.Р., Чугумбаева Н.Н.* Среда функционирования бизнеса как источник развития его внутреннего потенциала // Экономический анализ: теория и практика. 2016. Т. 15. Вып. 11. С. 127–142. URL: https://cyberleninka.ru/article/v/sreda-funktsionirovaniya-biznesa-kak-istochnik-razvitiya-ego-vnutrennego-potentsiala
9. *Федотова Г.В., Гонтарь А.А.* Информационная безопасность региональных социально-экономических систем: приоритетные направления // Инновационная экономика: перспективы развития и совершенствования. 2017. № 1. С. 369–374. URL: https://cyberleninka.ru/article/v/informatsionnaya-bezopasnost-regionalnyh-sotsialno-ekonomicheskih-sistem-prioritetnye-napravleniya
10. *Plotnikov V.A., Fedotova G.V., Popov E.G., Kastyurina A.A.* Harmonization of Strategic Planning Indicators of Territories' Socioeconomic Growth. *Regional and Sectoral Economic Studies*, 2015, vol. 15-2, pp. 105–114.

Информация о конфликте интересов

Я, автор данной статьи, со всей ответственностью заявляю о частичном и полном отсутствии фактического или потенциального конфликта интересов с какой бы то ни было третьей стороной, который может возникнуть вследствие публикации данной статьи. Настоящее заявление относится к проведению научной работы, сбору и обработке данных, написанию и подготовке статьи, принятию решения о публикации рукописи.

pISSN 2073-2872
eISSN 2311-875X

Economic Policy of the State

DIGITIZATION ISSUES OF THE MANUFACTURING SECTOR

Gilyan V. FEDOTOVA

Volgograd State Technical University (VSTU), Volgograd, Russian Federation
g_evgeeva@mail.ru
https://orcid.org/0000-0002-2066-8628

Article history:
Received 17 September 2018
Received in revised form
11 October 2018
Accepted 7 November 2018
Available online
15 February 2019

JEL classification: G21, G28, G29

Keywords: State, digital economy, industry, security, threat

Abstract

Subject The research pursues to model the environment of the digitized national economy, which will contribute to partnership relations of entities running IT resources and development of the existing mechanisms for economic and information security.

Objectives The research evaluates the transformation of the existing industrial sector's mechanisms ensuring the implementing of national digitization programs. I also focus the situation in the sector and analyze the digitization level of the manufacturing sector.

Methods I apply methods of logic and comparative analysis, graphic visualization and data sets, financial analysis, trend analysis, methods of comparison, analogy and systematization, comprehensive review of academic and sectoral literature, statistical data, and assessment.

Results Considering digitization processes in the manufacturing sector of the national economy, I make my suggestions on further development and transformation of economic security systems ensuring the reliability and protection of online platforms' data. For this, I conducted a systems analysis of trends in the manufacturing sector's development, evaluated the formation of the GISP (Governmental Information Systems for Manufacturing Sector) with resources of the RF Ministry for Industry and Trade, and reviewed key benchmarks of TechNet Road Map.

Conclusions and Relevance Having examined development aspects and formation of Russia's information platform for the manufacturing sector, I revealed some security issues of online systems. The findings can be used to outline the future strategic milestones for planning the national economic and industrial policy of Russia and development priorities.

Please cite this article as: Fedotova G.V. Digitization Issues of the Manufacturing Sector. *National Interests: Priorities and Security*, 2019, vol. 15, iss. 2, pp. 273–283.
https://doi.org/10.24891/ni.15.2.273

References

1. Bogoviz A.V., Ragulina Y.V., Morozova I.A., Litvinova T.N. Experience of Modern Russia in Managing Economic Growth. In: Studies in Systems, Decision and Control. Vol. 135. Springer, 2018, pp. 147–154.
2. Bogoviz A.V., Ragulina Y.V., Komarova A.V. et al. Modernization of the Approach to Usage of Region's Budget Resources in the Conditions of Information Economy Development. *European Research Studies Journal*, 2017, vol. 20, iss. 3, pp. 570–577.
URL: https://ersj.eu/dmdocuments/2017-xx-3-b-53.pdf
3. Aristovnik A., Obadić A. The Impact and Efficiency of Public Administration Excellence on Fostering SMEs in EU Countries. *Amfiteatru Economic*, 2015, vol. 17, no. 39, pp. 761–774.
4. Nasir A., Shahzad M., Anwar S., Rashid S. Digital Governance: Improving Solid Waste Management Through ICT Reform in Punjab. ICTD' 17 Proceedings of the Ninth International Conference on Information and Communication Technologies and Development. ACM, 2017.
URL: https://doi.org/10.1145/3136560.3136600

5. Bondarenko Yu.G. [Public Administration Efficiency Increase in Investment Management]. *Актуальні Проблеми Економіки*, 2015, vol. 172, no. 10, pp. 89–94.

6. Gavrilenko T.Yu., Provorova I.P. [Network economy as phenomenon of information society]. *Rossiiskii tekhnologicheskii zhurnal = Russian Technological Journal*, 2016, no. 1, pp. 53–61. (In Russ.)

7. Chugumbaev R.R., Chugumbaeva N.N. [Margin analysis of goodwill as a tool to substantiate societal improvement innovation economically]. *Chelovek. Obshchestvo. Inklyuziya = Human. Society. Inclusion*, 2017, no. 2, pp. 108–119. (In Russ.)

8. Chugumbaev R.R., Chugumbaeva N.N. [Business environment as a source of internal potential development of a business]. *Ekonomicheskii analiz: teoriya i praktika = Economic Analysis: Theory and Practice*, 2016, vol. 15, iss. 11, pp. 127–142.
URL: https://cyberleninka.ru/article/v/sreda-funktsionirovaniya-biznesa-kak-istochnik-razvitiya-ego-vnutrennego-potentsiala (In Russ.)

9. Fedotova G.V., Gontar' A.A. [Information security of regional socio-economic systems: Priority aspects]. *Innovatsionnaya ekonomika: perspektivy razvitiya i sovershenstvovaniya = Innovation Economy: Prospects for Development and Improvement*, 2017, no. 1, pp. 369–374.
URL: https://cyberleninka.ru/article/v/informatsionnaya-bezopasnost-regionalnyh-sotsialno-ekonomicheskih-sistem-prioritetnye-napravleniya (In Russ.)

10. Plotnikov V.A., Fedotova G.V., Popov E.G., Kastyurina A.A. Harmonization of Strategic Planning Indicators of Territories' Socioeconomic Growth. *Regional and Sectoral Economic Studies*, 2015, vol. 15-2, pp. 105–114.

Conflict-of-interest notification

I, the author of this article, bindingly and explicitly declare of the partial and total lack of actual or potential conflict of interest with any other third party whatsoever, which may arise as a result of the publication of this article. This statement relates to the study, data collection and interpretation, writing and preparation of the article, and the decision to submit the manuscript for publication.