Цифровой комплаенс как фактор развития экономики региона

Калмыкова С.В., кандидат педагогических наук, доцент Высшей инженерно-экономической школы, директор Центра открытого образования, ФГАОУ ВО «Санкт-Петербургский политехнический университет Петра Великого», Санкт-Петербург, Россия

Кобышева М.С., преподаватель Высшей инженерно-экономической школы, ФГАОУ ВО «Санкт-Петербургский политехнический университет Петра Великого», Санкт-Петербург, Россия

Сергеев Д.А., кандидат экономических наук, доцент Высшей инженерно-экономической школы, ФГАОУ ВО «Санкт-Петербургский политехнический университет Петра Великого», Санкт-Петербург, Россия

Аннотация. Проблематика рисков и угроз серьезно разрабатывается в рамках теории и практики государственного управления и управления бизнесом. В условиях глобальной цифровизации необходимы надлежащие средства обеспечения стабильности бизнеса, такие как комплаенс-платформы. У российского бизнеса постепенно формируется понимание того, что комплаенс — это неотъемлемый элемент системы корпоративного управления. В 2012 г. ведущие бизнес объединения подписали Антикоррупционную хартию российского бизнеса и утвердили порядок ее реализации. Программный документ впервые определил единые критерии высоких стандартов ведения российского бизнеса в отношении нетерпимости всех форм коррупции не только при выстраивании взаимоотношений с государством, но, и в корпоративных отношениях.

Ключевые слова: экономическая безопасность, цифровая экономика, комплаенс-контроль, менеджмент, управление рисками.

Digital compliance as a factor in the development of the regional economy

Kalmykova S.V., Candidate of Pedagogical Sciences, Associate Professor of the Higher School of Engineering and Economics, Director of the Center for Open Education, Federal Autonomous Educational Institution of Higher Education Peter the Great St. Petersburg Polytechnic University, St. Petersburg, Russia
Kobysheva M.S., Lecturer of the Higher Engineering and Economics School, Federal Autonomous Educational Institution of Higher Education Peter the Great St. Petersburg Polytechnic University, St. Petersburg, Russia
Sergeev D.A., Candidate of Economic Sciences, Associate Professor of the Higher School of Engineering and Economics, Federal Autonomous Educational Institution of Higher Education Peter the Great St. Petersburg Polytechnic University, St. Petersburg, Russia

Annotation. The issue of risks and threats is seriously developed within the framework of the theory and practice of public administration and business management. Russian business is gradually developing an understanding that compliance is an integral part of the corporate governance system. In 2012, leading business associations signed the Anti-Corruption Charter of Russian business and approved the procedure for its implementation. The program document for the first time defined uniform criteria of high standards of Russian business regarding intolerance of all forms of corruption not only in building relations with the state, but also in corporate relations.

Keywords: economic security, digital economy, compliance control, management, risk management.

Целью данного исследования является определение рисков и угроз для предприятий различных категорий и классификаций в условиях цифровой трансформации. Выделение комплаенс-рисков и предложение методик для комплаенс-контроля на предприятии в цифровую эпоху.

Для достижения этих целей необходимо решить следующие задачи:

– выявить комплаенс-риски;

– классифицировать угрозы для предприятия, в случае реализации этих риском;

– предложить методы построения системы комплаенс-контроля на предприятии.

Для нашего общества, понятие «экономическая безопасность» относительно новый термин. Существует множество определений экономической безопасности, а также множество определений этого понятия, с разбором факторов возникновения угроз.

Комплаенс означает создание внутренних политик компании, направленных на соответствие нормам закона и стандартам, на снижение внешних рисков.

В условиях цифровой экономики, когда ключевым активом становятся данные и основанные на них инновации, особое значение приобретает соблюдение стандартов в области цифровой безопасности и неприкосновенности частной жизни.

Возможность противостоять рискам обеспечивает конкурентоспособность компании в условиях цифровизации, что позволяет ей занимать более устойчивое положение.

Решающее значение для компаний приобретает цифровой комплаенс - правила внутренней политики.

В обобщенном понимании экономическая безопасность — это состояние национальной экономики, обеспечивающее удовлетворение жизненно важных потребностей страны в материальных благах независимо от возникновения в мировой экономической системе или внутри страны форс-мажорных обстоятельств социально-политического, экономического или экологического характера [3].

В научном подходе, под сущностью экономической безопасности, понимается такое «состояние экономики и институтов власти, при котором

обеспечивается гарантированная защита национальных интересов, социально направленное развитие страны в целом, достаточный оборонный потенциал даже при наиболее неблагоприятных условиях развития внутренних и внешних процессов»[1].

Под экономической безопасностью предприятия понимается состояние защищенности жизненно-важных интересов предприятия от внутренних и внешних угроз, формируемое руководством и коллективом предприятия путем реализации мероприятий правового, экономического, организационного, инженерно-технического и социально-психологического направлений. Экономическая безопасность предприятия связана с производством продукции, выполнением работ и оказанием услуг. От того насколько эффективно работают наши предприятия, зависит экономическое благосостояние всей страны, особенно в цифровую эпоху.

Всемирный опыт показывает, что именно обеспечение экономической безопасности в условиях цифровой трансформации и является гарантией независимости государства, условие его стабильности и эффективность жизнедеятельности всего общества.

Исследования в области экономической безопасности в Советском Союзе являлись закрытыми материалами. Все разработки в этой области были засекречены и носили больше прикладной характер. Под экономической безопасностью понимались условия, обеспечивающие сохранение и развитие экономической системы СССР, а также социалистических стран, входящих в Совет Экономического Взаимопомощи. При Советской власти ничего не говорилось об экономической безопасности предприятий, регионов, организаций, т.к. считалось, что их безопасность обеспечивает государство.

В приоритете было выделение средства на развитие военно-промышленного комплекса, поддержку стран, где к власти пришел коммунистический режим. Это привело к тому, что на воспроизводство

[1] Пузиков, В.В. Экономическая безопасность и экономическая преступность / В.В. Пузиков, А.И. Грамович. Минск: Армита — Маркетинг, Менеджмент, 2001.

населения, особенно на повышение его благосостояния ресурсы выделялись по остаточному принципу.

В итоге экономическая, идеологическая, политическая, социально-психологическая безопасность государства оказалась в корне подорвана. С 1991 года полностью развалилась огромная держава под названием СССР.

Экономика страны оказалась в руках неграмотных экономистов. Проведение неадекватной хозяйственным условиям политики перестройки еще больше усугубило положение. Открытость экономики позволила зарубежным производителям захватить российский рынок, вследствие чего в экономике России начался резкий спад производства, который, к сожалению, еще продолжается. Под угрозой находилась национальная безопасность России. Резкое падение уровня доходов и жизни населения представляет угрозу государственности России. Всему этому виной - состояние экономики

Во времена перестройки в нашу страну стали проникать идеи экономической безопасности. Проблемы экономической безопасности страны правительством долгое время игнорировались. Предпринимались попытки создания комитетов по изучению проблем экономической безопасности (Комитет по защите экономических интересов России при Президенте [1], Рабочая группа по экономической безопасности при Правительстве РФ), но они не имели успеха.

Развитая экономика сводит роль государства (по отношению к частному капиталу) лишь к защите бизнес-активов и поддержанию среды, благоприятной для функционирования рыночной системы. Такая парадигма ставит проблему корпоративного мошенничества в западных странах на приоритетные места в системе государственного управления. Тем более учитывая определяющую роль частного капитала в процессе экономического развития этих стран.

Обязанность введения частными компаниями направленного, в том числе на противодействие корпоративному мошенничеству (комплаенса), предусмотрена принятым в 1977 г. американским законом о противодействии

коррупции за рубежом (Foreign Corrupt Practices Act [7]) и британским антикоррупционным законом (UK Bribery Act [8]) 2010 г.

Оба документа определяют и общую (единую для всех компаний) методику противодействия коррупции и мошенничеству. При этом государство предоставляет определенные преференции компаниям, имеющим систему цифрового комплаенса, направленную не только на борьбу с корпоративным мошенничеством, но и на подкуп государственных чиновников. Наличие комплаенс-системы, а также публичная активность компании в расследовании фактов коррупции своих сотрудников могут значительно уменьшить размер наказания самой компании.

Особенностью UK Bribery Act является признание преступлением даже не предотвращение компаниями коррупционных проявлений, если не будет доказано, что принятые ими меры (система комплаенса) были достаточными. Цифровой комплаенс выступает своеобразным «иммунитетом» к ответственности.

Необходимость создания единой методики комплаенса и введения ее на практике признана на международном уровне.

Не существует общепризнанных научно разработанных понятий «угроза» и «риск». В «Толковом словаре» С.И. Ожегова записано: «Угроза - обещание причинить кому-нибудь вред, зло»[2].

В.И. Даль толковал угрозу как действие или намерение «угрожать, грозить, стращать, наводить опасность либо опасение, держать под страхом, под опаскою, пригражать»[3].

Мы будем пользоваться следующими определениями.

Угроза – объективный, т.е. внешний мало (не) контролируемый агентом тренд, событие, влекущее за собой опасность потерь, ущерба, вреда или воспринимаемое как таковое [6].

Коротко, угроза — это возможная опасность.

---

[2] Ожегов С.И. Словарь русского языка (1949, 22-е издание, 1990; с 1992 – «Толковый словарь русского языка», совместно с Н. Ю. Шведовой).

[3] Даль В.И. Толковый словарь живого великорусского языка: В 4 т. – Спб., 1863-1866.

Возможность нежелательного события, потери, недостижения ожидаемых результатов деятельности агента или отклонений от них. Он связан с угрозами через фактор неопределенности, но непосредственно характеризует ситуацию через призму действий (или бездействия) самого агента. Интуитивной мерой оценки риска служит опасение. Риск часто связан с ситуацией выбора: между привлекательным, но менее надежным вариантом и менее привлекательным, но более надежным, а, следовательно, с принятием решений в условиях выбора [6].

Угроза – основополагающее понятие в сфере обеспечения безопасности. Угроза — это сочетание факторов и условий, возникающих в процессе взаимодействия различных объектов, которые могут оказать негативное воздействие на объект безопасности.

Негативные воздействия от угроз различаются по характеру наносимого вреда: степень изменения свойств объекта; возможность ликвидации последствий угрозы.

Выделяются два наиболее важных типа угроз: намерение нанести вред (умысел); возможность нанесения вреда, т.е. наличие сил и средств.

Особенностью первого типа угроз является неопределенность, желание есть, но будет ли возможность. А вот возможность нанесения вреда может быть осуществлена только самими субъектами угроз. Между угрозой и опасностью нанесения вреда существует прочная причинно-следственная связь, особенно эта связь проявляется в условиях цифровой трансформации, когда стоимость ошибки грань угрозой и опасностью становится тоньше.

Декларируемая в нашей стране рыночная экономика, не исключает регулирования государством экономических отношений, касается это и вопросов экономической безопасности. Экономическая безопасность является гарантом стабильности функционирования предприятия. Его устойчивости, конкурентоспособности на рынке. Экономическая устойчивость охраняется как от прямых, так и от потенциальных посягательств. Количеством принимаемых

нашим правительством нормативных актов показывает, что проблема очень серьезная и усугубляется в условиях цифровизации.

Самое слабое звено в структуре безопасности – это человек. Можно создать надежную систему защиты и написать очень подробные инструкции по безопасности, однако халатное обращение сотрудников с важными сведениями, их доверчивость и беспечное поведение способны свести на нет все усилия.

Примерно 80% проблем, связанных с нарушением безопасности хозяйствующего субъекта, являются результатом саботажа, умышленного хищения и неосторожности сотрудников компании.

Для полноценного обеспечения безопасности предприятия, необходимо разработать глубоко продуманную политику.

В настоящее время, все больше международных и российских компаний приходят к осознанию актуальности цифрового комплаенса. Сегодня это – один из важнейших принципов ведения бизнеса.

Уровень нефинансовых рисков постоянно растет и, в связи с этим, постоянно увеличивается ценность комплаенс-функции для любого предприятия. Руководство компании должно иметь информацию о возникающих и потенциальных комплаенс-рисках.

Одной из функциональных задач цифрового комплаенса является внедрение в организацию комплаенс–политики, методологии оценки комплаенс–рисков, правил информационного обмена между подразделениями для эффективного управления комплаенс-рисками, политики и процедур соответствия деятельности организации, ее внутренних документов действующему законодательству, кодексов этики и др.

В задачи комплаенса также входит осуществление регулярного мониторинга и оценки комплаенс-рисков организации.

В российском законодательстве нет официального определения данной функции, в связи, с чем у делового сообщества ещё не сложилось её единого понимания, но при этом, комплаенс – неотъемлемый элемент в управлении предприятием.

Цифровой комплаенс должен создать для компании дополнительную цифровую систему контроля, включая предупредительные и направленные на выявление совершенных нарушений процедуры и обучающие программы. Комплаенс обеспечивает основу контроля любой организации. Он рассматривается как обязательная составляющая системы управления. Одной из важнейших частей которой является система внутреннего контроля.

Ключевыми элементами цифрового комплаенса системы являются следующие:

– Оценка рисков – компания активно идентифицирует свои риски несоответствия законодательству и регулярно проводит их переоценку при развитии новых направлений или видов деятельности. Проводится изучение конкретных рисков несоответствия законодательству, которые могут возникнуть в каждом бизнес-подразделении или сфере деятельности.

– Контрольные точки – управление каждым риском осуществляется по определенным контрольным точкам. Контрольные точки подкрепляются установлением поведенческого и процедурного контроля. Процедурные механизмы охватывают и смягчают зоны высокого риска в операционной среде предприятия, а поведенческие механизмы усиливают политику компании по управлению этими рисками.

– Надлежащая цифровая документация – все усилия по обеспечению соответствия должным образом задокументированы, что гарантирует возможность их подтверждения в случае нарушения.

– Подотчетность – применяется для управления каждым элементом системы соблюдения законодательных требований.

– Постоянное улучшение – цифровые технологии позволяют компании оценивать свои результаты и подходы, чтобы убедиться, что они соответствуют ее деятельности.

Выбор и внедрение цифровых решений в сфере комплаенс, позволяющих максимально обезопасить бизнес, остается выбором компаний, но, в

современном мире игнорировать цифровые технологии и их возможности уже нельзя.

Сотрудничество комплаенс-контроля с бизнес-подразделениями обеспечивает на раннем этапе выявление и минимизацию либо устранение комплаенс-рисков.

Комплаенс-риски при возникновении угрозы бизнес-репутации, финансовой несостоятельности и др. Под воздействием вышеперечисленных факторов возникают комплаенс риски потерь следующего характера: материальные; временные; стоимостные; интеллектуальные; информационные; трудовые; специальные разновидности потерь (ущерб жизни и здоровью людей, природе, экологии, репутации предприятия).

Также могут реализоваться и юридические риски, например, если компания является кредитозаемщиком.

Риск, связанный с инцидентами в области цифровой безопасности, вошел в пятерку крупнейших бизнес-рисков в 2015 году (в 2014 кибер-риски занимали 8 место, а в 2013 – лишь 15). В 2019 году – они занимают уже второе место.

В условиях цифровой экономики киберпреступность, сбои в работе IT-инфраструктуры, утечки данных могут парализовать работу любой компании.

Расширение возможности подключения устройств к Интернету и общей IT-инфраструктуре делает все звенья в цепочке поставок уязвимыми для кибер-инцидентов.

Цифровой комплаенс должен помогать компаниям избегать ключевые риски цифровой безопасности, нарушения неприкосновенности, частной жизни, другие нефинансовые риски.

Функционал комплаенса тесно связан с определенными направлениями работы подразделений внутреннего контроля, финансового мониторинга, юридической службы, подразделения операционных рисков и службы персонала.

Комплаенс является важным звеном системы корпоративного управления предприятием в целом.

Резюмируя все вышесказанное, отметим, что:

– комплаенс-система — это часть системы внутреннего контроля и системы управления предприятия;

– комплаенс-система — это комплекс встроенных в бизнес-процессы предприятия видов контроля в разрезе людей, технических средств и документов в целях соблюдения внешних и внутренних требований;

– уровень комплаенса любой организации всегда превышает нулевой уровень, но при этом никогда не сможет достигнуть 100%-ной отметки.

При построении цифровой комплаенс системы на предприятии необходимо помнить о том, что ее необходимо органично вписать в структуру компании, эта проблема особенно актуальна в условиях цифровой трансформации, когда динамика изменений происходит на постоянной основе.

Следующее «золотое» правило, которого надо придерживаться, цена контроля, не должна превышать потери от отсутствия данного контроля. В зарубежной практике применяется термин «риск - аппетиты». Риск - аппетит — это то количество риска, которое компания готова понести в зависимости от ее финансовых и операционных возможностей. Какие максимальные потери готово понести предприятие, зависит и обоснованность затрат на контроль. Связь здесь обратно-пропорциональная: чем выше риск-аппетиты, тем меньше требуется затрат на контроль, и наоборот. Цена некомплаенса прямо влияет на цену контроля: чем серьезнее последствия некомплаенса, тем более обоснованы расходы на контроль.

В чем отличия цифровой комплаенс–системы от службы внутреннего контроля (СВК), которая есть практически на всех предприятиях. Возможно, на первый взгляд может показаться, что действительно функционал схож, но, следует отметить, что функционал комплаенс-системы должен быть намного шире функционала СВК и отвечать современным требованиям эпохи цифровизации.

Функцией внутреннего аудита является независимая проверка системы внутреннего контроля, а функцией структуры комплаенс-контроля является организация текущего контроля процедур по управлению комплаенс рисками.

Развитие цифрового комплаенса в компании возможно за счет использования современных IT-решений.

Перевод контрактных отношений в онлайн, а также регистрация контрактов на основе технологии блокчейн позволяет повысить транспарентность деятельности компании и цепочек поставок. А то уже действительность современности и цифровой эпохи.

Проведение анализа контрактных отношений с применением технологии искусственного интеллекта позволяет выявлять финансовые и нефинансовые риски компаний.

Еще одним очень важным отличительным признаком является временной аспект объекта контроля и комплаенс подразделения. Роль комплаенс-контроля, как элемента риск-менеджмента заключается в координации контроля комплаенс-рисков на уровне отдельных функциональных подразделений и агрегировании результатов комплаенс-контроля в оценку совокупного риска. Комплаенс-контроль работает в превентивном режиме, а сотрудники СВК проводят анализ свершившихся событий и соответствия требованиям на настоящий момент.

Комплаенс-контроль, базирующийся на оценке комплаенс-рисков. Этот вид комплаенс-контроля рекомендован иностранным организациям государственными регуляторами и международными организациями. Созданная и эффективно функционирующая на предприятии комплаенс–система, помогает управлять комплаенс–рисками. И это является конкурентным преимуществом компании и на микро, и на макроуровне.

С каждым годом ценность комплаенс – функции, для бизнеса увеличивается. У российского бизнеса постепенно формируется понимание того, что комплаенс — это неотъемлемый элемент системы корпоративного управления. Он служит основой для совершенного процесса принятия

руководством принципиальных решений, и, соответственно, содействует достижению установленных целей предприятия.

Механизм внедрения в жизнь компании цифрового комплаенса:

1. Разработка и принятие специального документа - Политика ответственного поведения, направленную на определение и устранение рисков.

2. Формирование системы оценки потенциальных и фактических рисков.

3. Разработка мер по предотвращению и смягчению последствий при реализации негативных рисков.

4. Периодически оценивать, какие предпринимаются меры по снижению рисков и какие риски были предотвращены.

5. Взаимодействовать с общественностью. Ключевые инструменты: ежегодные доклады предприятия об устойчивости или корпоративной ответственности, или другие формы раскрытия информации.

6. Принимать меры по восстановлению в случае наступления негативного воздействия (механизм страхования, в том числе и кибер-рисков.

В результате данного исследования были выделены комплаенс-риски, а также возможные угрозы, в случае реализации данного вида рисков, предложены методы построения системы комплаенс-контроля на предприятии.

В настоящее время наше государство проявляет активность по защите преимущественно собственного бюджета. Таким образом, государство приоритетно защищает свое имущество от действий своих чиновников – государственных служащих. Защита же частного капитала компаний от действий их же персонала зачастую отходит на второй план и возлагается на плечи исключительно самого бизнеса.

Такая ситуация, безусловно, замедляет процесс интеграции российской экономики в мировую, которая навязывает свои правила игры за неимением у российского бизнеса собственных.

В связи с этим российскому деловому сообществу приходится заботиться о своем будущем самому.

В сентябре 2012 г. ведущие бизнес объединения подписали Антикоррупционную хартию российского бизнеса и утвердили порядок ее реализации. Этот программный документ впервые определил единые критерии высоких стандартов ведения российского бизнеса в отношении нетерпимости всех форм коррупции не только при выстраивании взаимоотношений с государством, но, что не менее важно, в корпоративных отношениях.

Само по себе наличие одной лишь хартии не решит проблемы обеспечения экономической безопасности хозяйствующего субъекта. Для реализации ее положений необходимо законодательное закрепление содержащихся в хартии принципов делового поведения, обеспечение преференций бизнесу за их добросовестное исполнение, а также волевое решение каждого представителя бизнес-сообщества следовать общим стандартам и «правилам игры»).

Приоритетное значение в современном цифровом мире приобретают вопросы соблюдения стандартов ответственного ведения бизнеса, которые затрагивают несколько ключевых сфер: права человека; трудовые права; коррупцию; охрану окружающей среды; интеллектуальное право; защиту информации; налоги; конкуренцию; науку и технологии; правила раскрытия информации и защита прав потребителей.

Библиографический список

1. Указ Президента Российской Федерации «О Комитете по защите экономических интересов Российской Федерации при Президенте РСФСР» от 19.11.1991 № 222 // Собрание актов Президента и Правительства Российской Федерации.

2. Программа «Цифровая экономика Российской Федерации», утв. Распоряжением Правительства РФ от 28 июля 2017 г. № 1632-р [Электронный ресурс]. URL: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf

3. Градов А.П. Национальная экономика 2-е изд. – СПб.: Питер, 2005. — 240 с.

4. Demidenko, D.S., Malevskaya-Malevich, E.D. (2016). Risk management system application efficiency on enterprise, Proceedings of the 28th International Business Information Management Association Conference – Vision 2020: Innovation Management, Development Sustainability, and Competitive Economic Growth, p. 2046-2051.

5. Semenov, V.P., Sokolitsyn, A.S., Sokolitsyna, N.A. (2016, November). Forming production program with homogenous product in market environment uncertainty. In Strategic Partnership of Universities and Enterprises of Hi-Tech Branches (Science. Education. Innovations), 2016 IEEE V Forum (pp. 76-78). IEEE.

6. Rodionov, D.G., Kudryavtseva, T.J., Skhvediani, A.E. Human development and income inequality as factors of regional economic growth 2018 European Research Studies Journal

7. Schepinin, V., Skhvediani, A., Kudryavtseva, T. An empirical study of the production technology cluster and regional economic growth in Russia (2018) Proceedings of the European Conference on Innovation and Entrepreneurship, ECIE

8. Demidenko, D.S., Kulibanova, V.V., Maruta, V.G. Using the methods of the company's capitalization optimal management (2018) Proceedings of the 32nd International Business Information Management Association Conference

9. Mednikov, M.D., Sokolitsyn, A.S., Ivanov, M.V., Sokolitsyna, N.A., Yuryev, V.N. Forming optimal industrial enterprise management strategy (2018) Proceedings of the 32nd International Business Information Management Association Conference

10. Sokolitsyn, A.S., Ivanov, M.V., Sokolitsyna, N.A. Statistic modeling industrial enterprises production process parameters (2018) Proceedings of the 30th International Business Information Management Association Conference

11. Ivanova M.V., Garmasar, O., Yakovleva, T., Glyass, E. Evaluation of compliance costs interrelation with a level of innovative economic development (2018) IOP Conference Series: Materials Science and Engineering

12. Цифровая экономика: анализ развития в Российской Федерации [Текст] / Родионов Д.Г., Схведиани А.Е., Бондарев А.А. В книге: Тенденции

развития экономики и промышленности в условиях цифровизации / под ред. А.В. Бабкина. – Санкт-Петербург, 2017. – С. 68-93.

13. Родионов Д.Г., Кичигин О.Э., Селентьева Т.Н. Особенности оценки конкурентоспособности инновационного регионального кластера: институциональный подход // Научно-технические ведомости Санкт-петербургского политехнического университета. Экономические науки. – 2019. – №1. – С. 42-58.

References

1. Decree of the President of the Russian Federation «On the Committee for the Protection of Economic Interests of the Russian Federation under the President of the RSFSR» dated November 19, 1991 No. 222 // Collection of Acts of the President and Government of the Russian Federation.

2. The program «Digital Economy of the Russian Federation», approved. Order of the Government of the Russian Federation dated July 28, 2017 No. 1632-p [Electronic resource]. URL: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf

3. Gradov A.P. National Economics 2nd ed. – St. Petersburg: Peter, 2005. – 240 p.

4. Demidenko, D.S., Malevskaya-Malevich, E.D. (2016). Risk management system application efficiency on enterprise, Proceedings of the 28th International Business Information Management Association Conference – Vision 2020: Innovation Management, Development Sustainability, and Competitive Economic Growth, p. 2046-2051.

5. Semenov, V.P., Sokolitsyn, A.S., Sokolitsyna, N.A. (2016, November). Forming production program with homogenous product in market environment uncertainty. In Strategic Partnership of Universities and Enterprises of Hi-Tech Branches (Science. Education. Innovations), 2016 IEEE V Forum (pp. 76-78). IEEE.

6. Rodionov, D.G., Kudryavtseva, T.J., Skhvediani, A.E. Human development and income inequality as factors of regional economic growth 2018 European Research Studies Journal

7. Schepinin, V., Skhvediani, A., Kudryavtseva, T. An empirical study of the production technology cluster and regional economic growth in Russia (2018) Proceedings of the European Conference on Innovation and Entrepreneurship, ECIE

8. Demidenko, D.S., Kulibanova, V.V., Maruta, V.G. Using the methods of the company's capitalization optimal management (2018) Proceedings of the 32nd International Business Information Management Association Conference

9. Mednikov, M.D., Sokolitsyn, A.S., Ivanov, M.V., Sokolitsyna, N.A., Yuryev, V.N. Forming optimal industrial enterprise management strategy (2018) Proceedings of the 32nd International Business Information Management Association Conference

10. Sokolitsyn, A.S., Ivanov, M.V., Sokolitsyna, N.A. Statistic modeling industrial enterprises production process parameters (2018) Proceedings of the 30th International Business Information Management Association Conference

11. Ivanova M.V., Garmasar, O., Yakovleva, T., Glyass, E. Evaluation of compliance costs interrelation with a level of innovative economic development (2018) IOP Conference Series: Materials Science and Engineering

12. Digital economy: development analysis in the Russian Federation [Text] / Rodionov D.G., Skvediani A.E., Bondarev A.A. In the book: Trends in the Development of Economics and Industry in the Context of Digitalization / Ed. A.V. Babkina. – St. Petersburg, 2017. – P. 68-93.

13. Rodionov D.G., Kichigin O.E., Selentyeva T.N. Features of assessing the competitiveness of an innovative regional cluster: institutional approach // Scientific and Technical Journal of St. Petersburg Polytechnic University. Economic sciences. – 2019. – №1. – P. 42-58.