УДК *338.24*

ЭТАПЫ РАЗВИТИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ПО ОТНОШЕНИЮ К ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ЧАСТНОГО И ГОСУДАРСТВЕННОГО СЕКТОРОВ

Мухина Е.Р.
к.э.н., доцент,
Пермский национальный исследовательский политехнический университет,
Пермь, Россия

Серебрянский Д.И.
студент,
Пермский национальный исследовательский политехнический университет,
Пермь, Россия

Аннотация

На примере России и Великобритании исследуется применение искусственного интеллекта как стратегического инструмента в совершенствовании безопасности информации. Предложено постепенное внедрение искусственного интеллекта в экономическую безопасность частного и государственного секторов экономики. Рассмотрена позиция Российской Федерации в развитии искусственного интеллекта как национального интереса государства. Проанализировав данные, использованные для написания работы, выведены интересы для государственного и частного инвестирования. Также сформулирована стратегия внедрения искусственного интеллекта в сферы деятельности государственных и частных секторов экономики.

Ключевые слова: искусственный интеллект, экономическая безопасность, информационная безопасность, конфиденциальность, частный сектор, государственный сектор.

THE STAGES OF DEVELOPMENT OF ARTIFICIAL INTELLIGENCE IN RELATION TO THE ECONOMIC SECURITY OF THE PRIVATE AND PUBLIC SECTORS

Mukhina E.R.

PhD, Associate Professor,
Perm National Research Polytechnic University, Perm, Russia

Serebryansky D.I.
student,
Perm National Research Polytechnic University, Perm, Russia

Annotation

The example of Russia and the United Kingdom explores the use of artificial intelligence as a strategic tool in improving the security of information. A gradual introduction of artificial intelligence into the economic security of the private and public sectors of the economy is proposed. The position of the Russian Federation in the development of artificial intelligence as a national interest of the state is considered. Analyzing the data used to write the work, the interests for public and private investment were withdrawn. The strategy of introducing artificial intelligence into the spheres of public and private sectors of the economy is also formulated.

Keywords: artificial intelligence, economic security, information security, privacy, private sector, public sector.

Обеспечение защиты информационной среды в частном или государственном секторе, достижение высокого уровня информационного обеспечения работы всех служб сегодня невозможно представить без применения информационных технологий.

В развитии искусственного интеллекта (далее ИИ) заинтересованы не только частные инвесторы, но и государство. К национальным интересам страны отнесены повышение эффективности государственного управления, развитие экономики и социальной сферы, а также формирование цифровой экономики в Стратегии. Указом Президента Российской Федерации утверждена "Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы" [1]. Одним из основных направлений развития российских информационных и коммуникационных технологий в Стратегии относится ИИ.

Для восприятия необходимости внедрения ИИ в сферу экономической безопасности (далее ЭБ), обратимся к таблице 1 и рассмотрим определение «искусственного интеллекта».

Таблица 1 – Сравнение точек зрения различных авторов об искусственном интеллекте

№	Автор	Понятие
1.	Райков А.	Искусственный интеллект – это компьютерная философия, компьютерная психология и продвинутая компьютерная наука [12].
2.	Воронович А.А., Крист И.В., Девятериков Д.А., Лысак И.Ю., Глухарева С.В.	Искусственный интеллект – это концепция формирования программных и аппаратных средств, способных осуществлять интеллектуальную деятельность, сравнимую с интеллектуальным функционированием человека [7].
3.	Рассел С., Норвиг П.	Искусственный интеллект – это проектирование и построение интеллектуальных агентов, которые воспринимают объекты окружающей среды и предпринимают действия, влияющие на окружающую среду [13].
4.	Батырканов Ж. И., Саитов Н.Ж.	Искусственный интеллект – это область информатики, цель которой разработка аппаратно-программных средств, позволяющих человеку-непрофессионалу ставить и решать интеллектуальные задачи [6].

Из представленных понятий (см. табл. 1) можно выделить второе. ИИ на сегодняшний день в первую очередь теория и практика создания аппаратных средств, способных осуществлять интеллектуальную деятельность.

Таким же образом введем понятие термина «экономическая безопасность» (см. табл. 2).

Таблица 2 – Сравнение точек зрения различных авторов об экономической безопасности

№	Автор	Понятие
1.	Климонова А.Н.	Экономическая безопасность – это сегмент государственной безопасности, узко координирующийся с ее другими компонентами, и, обозначающийся фундаментом снабжения таких элементов как военная, политическая, социальная, экологическая, технологическая, информационная и др. [10].
2.	Ефимова Г. В., Марущак С. М.	Экономическая безопасность предприятия – это экономическая категория, характеризующая условия функционирования

		предприятия [4].
3.	Лесных Ю.Г., Повойко И.В.	Экономическая безопасность – это совокупность координированных деталей (частных проявлений безопасности): глобальная, международная региональная, национальная безопасность, региональная безопасность страны, безопасность административно-территориальных образований, безопасность организации, безопасность индивида [12].
4.	Ахметова Б.Т.	Экономическая безопасность - это материальная основа национальной безопасности. Содержание понятия отражает такое состояние хозяйства страны, которое обеспечивает способность противостоять неблагоприятным внешнеэкономическим воздействиям [5].

ЭБ является материальной неотъемлемой и составной частью основы национальной безопасности. Последнее понятие является наиболее подходящим определением, по мнению авторов, так как выражает главную мысль, определяющую категорию безопасности.

Использование в органах государственной власти Российской Федерации новых (цифровых) технологий, внесено в список главных задач применения информационных и коммуникационных технологий для развития государственного управления и взаимодействия граждан и государства. ИИ признан подрывной технологией – такой, внедрение которой требует изменения бизнес-модели, если дело касается человеческой деятельности, и технической модели функционирования объекта, который перестраивается на автономный автоматический режим работы.

Например, ИИ в банковской сфере применяется во многих направлениях: позволяет улучшить качество обслуживания клиентов, дает персонализированные советы в режиме реального времени, способен снизить затраты и риски для банков. Помимо охвата перечисленных специфик, ИИ необходим для осуществления безопасности (в том числе конфиденциальности) экономической информации внутри обоих секторов (см. рис. 1).

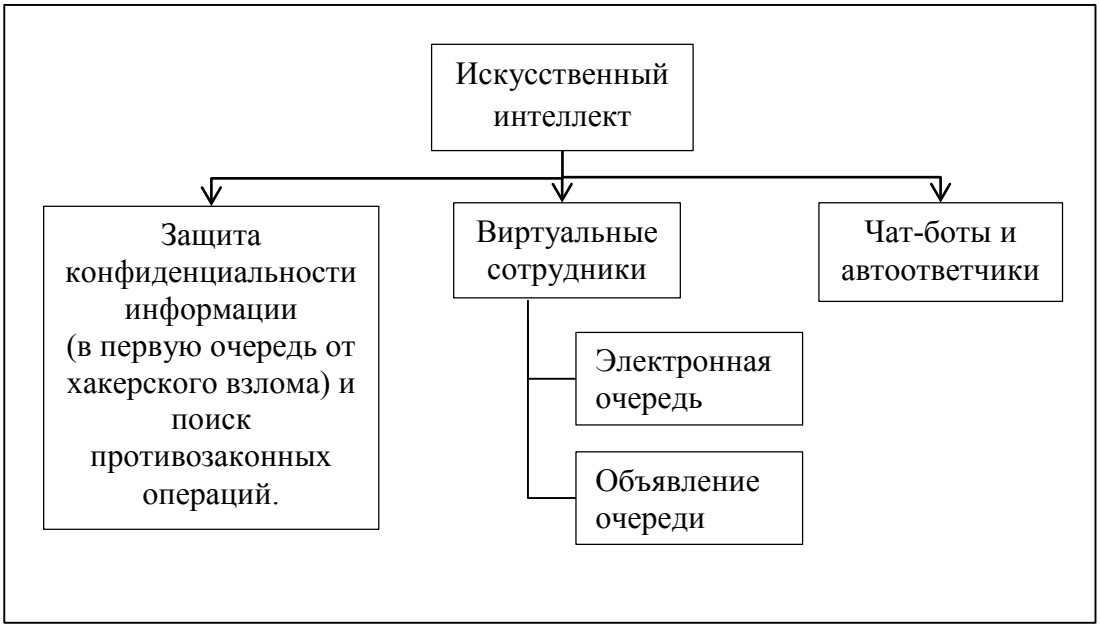

Рис. 1 – Система основных направлений применения искусственного интеллекта

На современном этапе ИИ заимствован киберпреступниками для организации более эффективных атак. Таким образом, предлагается постепенное внедрение ИИ в экономическую деятельность Российской Федерации. Защита безопасности (см. рис. 1) с помощью ИИ должна вовремя предпринимать меры по устранению неблагоприятного влияния на сферу деятельности, а также анализировать незаконные операции в государственной деятельности.

Рассмотрим практику применения ИИ в области обеспечения ЭБ в иностранных банках. Так, например, один из крупнейших банков в мире (по данным 2015 г. занимает 37-е место в списке самых дорогих брендов в мире) HSBC Holdings plc. использует ИИ в автоматизации процессов пресечения отмывания средств, шведский коммерческий банк Nordea Bank AB применяет виртуальных сотрудников в области обработки информационных процессов, банки The Royal Bank of Scotland Plc, Bank of America и др. пользуются услугами чат-ботов, которые обрабатывают административные задачи, дают советы по управлению, информируют об угрозах сотрудников отдела экономической безопасности банка [3].

Реализация технологии ИИ распространена и в России, однако не так широко как в Великобритании. Российский коммерческий банк «Тинькофф Банк», специализирующийся исключительно на дистанционном обслуживании клиентов, с целью повышения ЭБ использует встроенную в банкоматы систему компьютерного зрения. Банк «Открытие», признанный «Банком года» (2015), применяет ИИ для идентификации Клиентов с использованием системы по анализу биометрии лица. Модульбанк - единственный в России банк, который работает только с малым бизнесом, - повышает уровень ЭБ с помощью технологии автоматического определения рейтинга надежности клиента [8].

Индивидуальные технологии становятся все лучше при выполнении конкретных задач. Эти технологии называют когнитивными технологями и именно на них должны сосредоточить свое внимание руководители бизнеса и государства.

Становится необходимым добиваться уровня компьютеризованного управления на более высоком уровне. На уровне, приближенном к человеческому мышлению. Безопасность различных частных и государственных организаций будет защищена на наиболее высоком уровне с помощью ИИ, внимание которого будет направлено к защите и сохраняться в течение всего времени работы и отдыха.

В англосаксонских странах весомые инвестиции государство и бизнес вкладывают в поддержку соответствующих стартапов и НИР и ОКР в учебных и исследовательских учреждениях [2].

Такая программа как Amelia способна подстраиваться под разговор собеседника или же под запросы и правила компании. Она легко «понимает более 20-ти языков, а также приспосабливаться к проводимым бизнес-процедурам» [9]. В Соединенных Штатах уже существует система – «технология на базе нейросетей, которая позволяет сносно писать новостную ленту» [7]. Система Amelia обладает способностью анализировать и обрабатывать информацию и выполнять работу справочной службы, но принимать решения в отношении управления она не способна.

Уже сегодня компания Microsoft разрабатывает ИИ-ботов. Компания с мировым именем понимает, что для облегчения общения с компьютером, операционная система должна понимать язык человека и свободно им владеть. Конечно, это приведет ко многим успехам и в области безопасности.

Вопросам безопасности развития систем ИИ уделяется определенное внимание и в России, например, исследуются проблемы возможного появления своеобразных ловушек на пути развития ИИ в XXI веке и предлагаются подходы и методы их преодоления [12].

В ходе исследования затронут опрос менеджеров ста компаний, работающих на российском рынке. Интервьюируемые занимают посты ИТ-руководителей, а также руководителей департаментов цифровых сервисов или цифровой трансформации. Вместе с тем, в ходе исследования привлекались данные аналитических компаний, в том числе IDC, Gartner и Markets and Markets. Доля сведений поступила от консалтинговых компаний, таких как PwC и Teradata, а также вендоров, включая SAP.

Авторы исследования отмечают, что российский рынок ИИ и машинного обучения только начинает развиваться, проявляя отставание от зарубежных рынков. Утвердительное влияние аналогичных технологий на бизнес-процессы не подтверждается в России яркими примерами. Одна из причин – фирмы не разглашают результаты успешных внедрений, остерегаясь раскрыть конкурентам источник своего преимущества. Также внедрение ИИ и машинного обучения замедляется в России из-за недостатка вычислительных мощностей и невысокого уровня автоматизации.

К сравнению еще в 2016 году инвестиции в цифровые технологии Великобритании достигли £6,8 млрд., что на 50% больше, чем в самых передовых странах Европы (см. рис. 2).

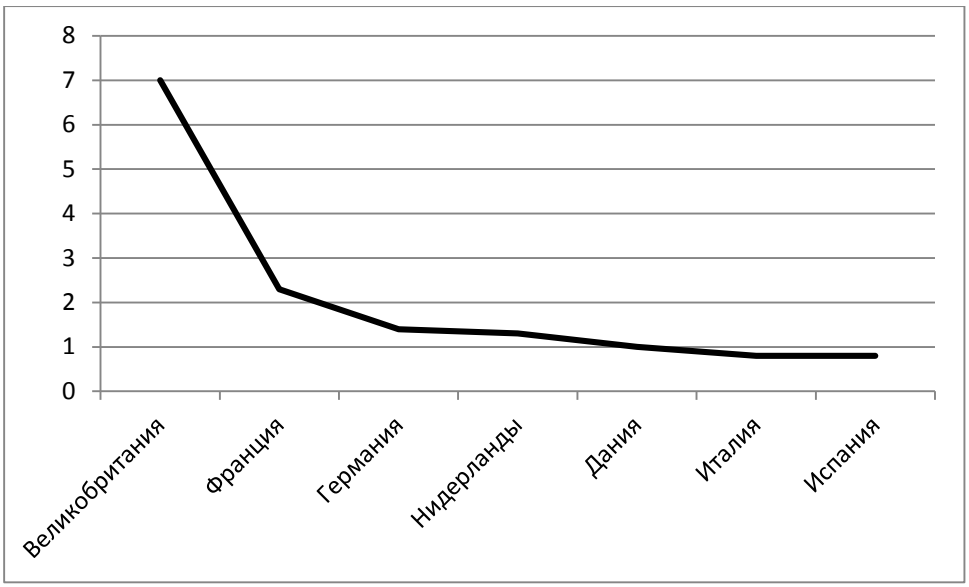

Рис. 2 – Инвестиции в цифровые технологии в самых развитых странах Европы, 2016 г., £ млрд.

Великобритания опережает страны Европы на несколько позиций (см. рис. 2). Франция отстает на 4,7 позиций, Германия и Нидерланды на 5,6, Дания на 6, Италия и Испания на 6,2.

Опыт внедрения механизмов машинного обучения в ритейле в сегменте товарных предложений демонстрирует, что с их помощью конверсию можно повысить на 15%, одновременно снизив в 50 раз количество операций, осуществляемых вручную, отмечают участники исследования. Менеджеры, которые работают в пяти крупнейших банках России, заявляют, что в течение пяти лет доля ИИ в принятии решений в их организациях достигнет 80%, а заказчиков уже через три года в 50% случаев будут обслуживаться «ботами». Степень проникновения подобных технологий в промышленность в настоящее время ниже, но тем не менее, фигурирует на третьем месте в списке лидеров по внедрению ИИ (см. рис. 3).

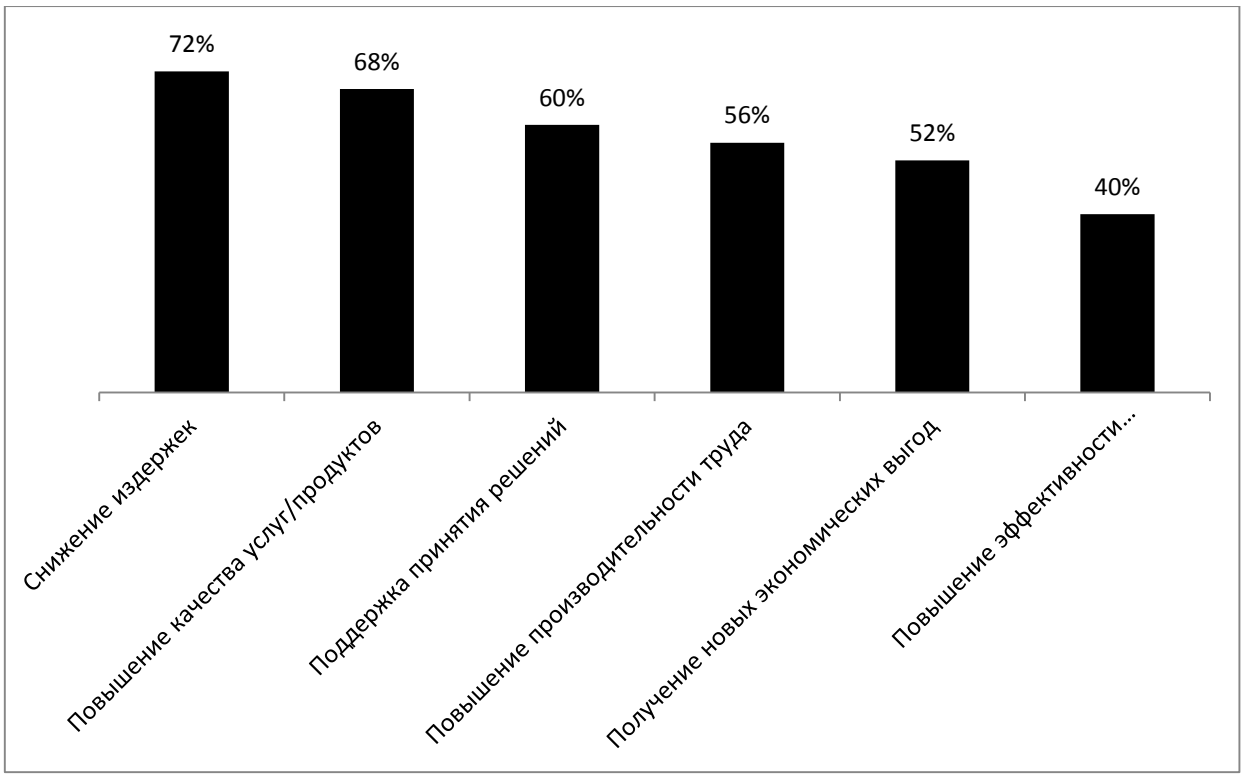

Рис. 3 – Цели внедрения машинного обучения и искусственного интеллекта

Более половины респондентов намерены повысить затраты на ИИ и машинное обучение в следующие 3-5 лет. Предполагаемый годовой рост затрат составляет 15-20%. У 30% участников отсутствует понимание, какая именно часть ИТ-бюджета компании расходуется на ИИ. Еще 30% предприятий тратят на такие технологии от 5% до 10%. 17% респондентов оценивают этот сегмент ИТ-бюджета менее чем в 5%. 13% фирм тратят на ИИ и машинное обучение более 15% ИТ-бюджета, еще 9% предприятий – от 10% до 15% ИТ-бюджета.

В настоящее время, вопреки существованию большого числа подходов, как к осмыслению задач ИИ, так и образованию интеллектуальных информационных систем, отмечаются фундаментальные пути к построению и созданию ИИ (см. рис. 4).

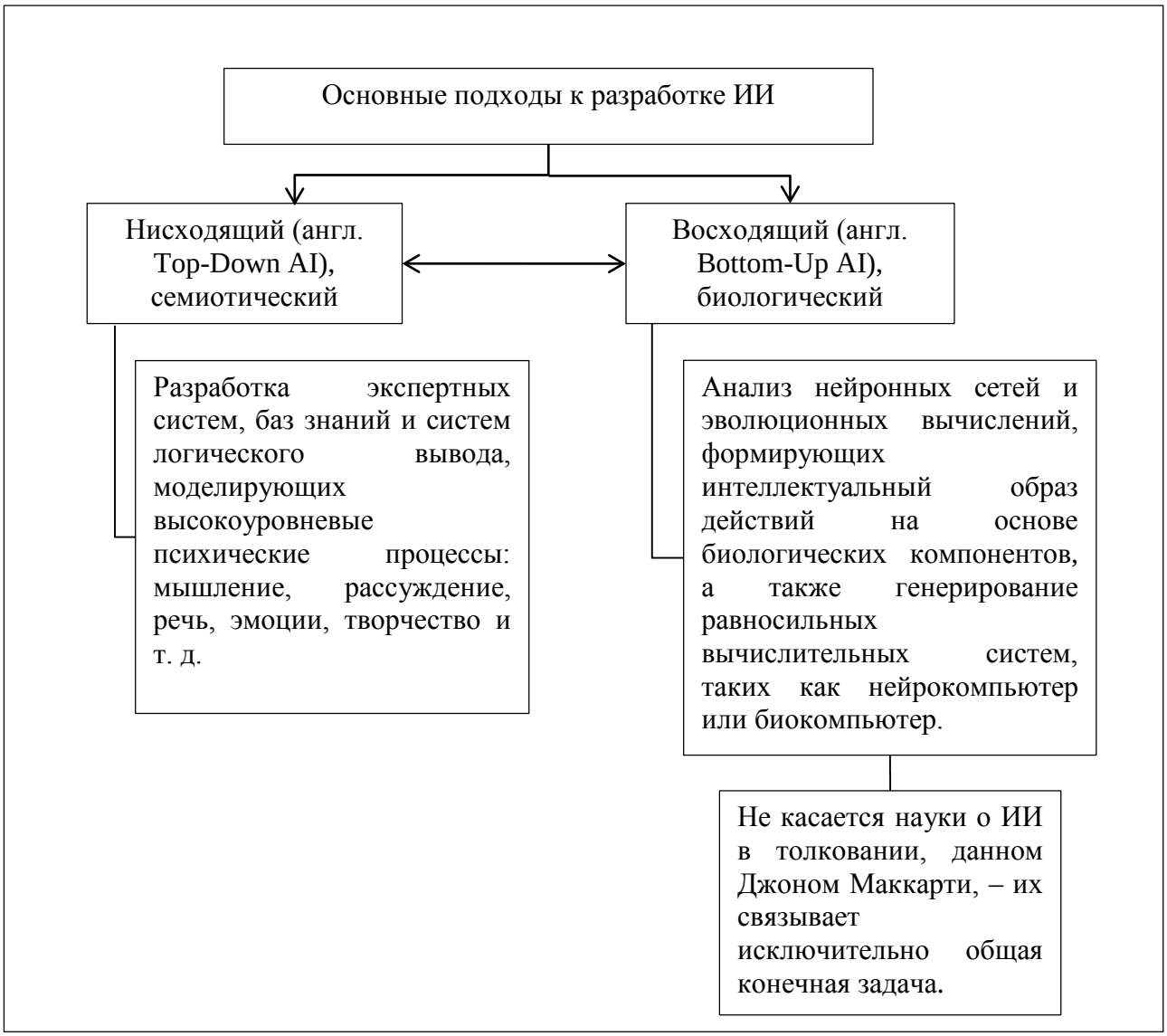

Рис. 4 – Основные подходы к разработке ИИ

Таким образом, проделав работу, авторами предлагается Стратегия развития ИИ по отношению к частному и государственному секторам экономики:

1. Анализирование и усвоение зарубежного опыта.

2. Расширение границ разработки ИИ в Российской Федерации.

3. Опора на экономическую безопасность государства.

4. Разработка и формирование национальных интересов по отношению к информационной безопасности частного и государственного секторов экономики.

5. Заинтересованность к сохранению безопасности информации самими частными или государственными партнерами.

6. Приобретение разработки в собственную сферу деятельности.

Предпосылки для продолжения работы над ИИ есть и в России, учитывая сотрудничество с иностранными партнерами. Их только необходимо начать. Именно так Российская Федерация смогла бы успешно конкурировать с одной (-ими) из объединившихся стран на глобальном рынке дистанционных когнитивных вычислений.

Библиографический список

1. О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы: Указ президента Российской Федерации от 9 мая 2017 г. № 203 // Собрание законодательства Российской Федерации. – 2017. - № 20. – ст. 2901.

2. David Schatsky, Craig Muraskin, Ragu Gurumurthy. Demystifying artificial intelligence. What business leaders need to know about cognitive technologies. -- November 04, 2014, https://dupress.deloitte.com/dup-us-en/focus/cognitive-technologies/what-is-cognitive-technology.html

3. Sennaar K. AI in Banking – An Analysis of America’s 7 Top Banks. [Электронный ресурс]. Режим доступа: https://www.techemergence.com/ai-inbanking-analysis (дата обращения 09.02.2018).

4. Yefimova G.V., Maruschak S.M. Definition of the «economic security of an enterprise» and «safe development of an enterprise» notions // Бизнес информ. 2013. № 11. С. 8-13.

5. Ахметова Б.Т. Экономическая безопасность - как экономическая категория // Актуальные проблемы современности. 2016. № 2 (12). С. 78-82.

6. Батырканов Ж.И., Саитов Н.Ж. Проблемы построения экспертных систем // Известия Кыргызского государственного технического университета им. И.Раззакова. 2010. Т. 19. С. 60-65.

7. Воронович А.А., Крист И.В., Девятериков Д.А., Лысак И.Ю., Глухарева С.В. Искусственный интеллект в системе кадровой безопасности предприятия // В сборнике: Экономическая безопасность: финансовые, правовые и IT-аспекты Материалы первой Всероссийской научно-практической онлайн-конференции. 2017. С. 8-15.

8. Гонтарь А.А. Искусственный интеллект в системе обеспечения экономической безопасности банка // В сборнике: Фундаментальная наука и технологии - перспективные разработки Материалы XIII международной научно-практической конференции . н.-и. ц. «Академический». 2017. С. 133-136.

9. Искусственный интеллект заменит работников диспетчерской службы. [Электронный ресурс]. – Режим доступа: http://neuronus.com/news-tech/591iskusstvennyj-intellekt-zamenit-rabotnikov-dispetcherskoj-sluzhby.html (дата обращения 09.02.2018).
10. Климонова А.Н. Основные подходы к исследованию понятий «экономическая безопасность» и «экономическая безопасность государства» // Социально-экономические явления и процессы. 2014. Т. 9. № 8. С. 54-60.
11. Лепихина Т.Л., Серебрянский Д.И. Использование информационно-коммуникативных технологий как стратегическая задача государственной политики // Инновационное развитие экономики: тенденции и перспективы. 2016. Т. 1. С. 131-137.
12. Лесных Ю.Г., Повойко И.В. Риски и угрозы экономической безопасности России со стороны мирового финансового рынка в новых геоэкономических условиях // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. 2015. № 112. С. 1462-1474.
13. Райков А. Ловушки для искусственного интеллекта // Экономические стратегии. Базовые компетенции. 2016. № 6. С. 172-179.
14. Рассел С., Норвиг П. Искусственный интеллект: современный подход // Ответственный искусственный интеллект. 2009.
15. Серебрянский Д.И., Южанинов В.И. Финансовая безопасность Российской Федерации // Инновационное развитие экономики: тенденции и перспективы. 2016. Т. 1. С. 391-396.