ФАКТОРНЫЕ ОГРАНИЧЕНИЯ РАЗВИТИЯ БИЗНЕС-СРЕДЫ ЭКОСИСТЕМНОЙ НАПРАВЛЕННОСТИ В ОТРАСЛИ ИКТ

Е. В. Павлова, *к.э.н., Санкт-Петербургский государственный университет телекоммуникаций им. проф. Бонч-Бруевича, epavlova.pnd-9@yandex.ru.*

УДК 338

Аннотация. Трансформация экономических, политических, социальных аспектов предпринимательской деятельности посредством цифровых технологий привела к появлению новых организационных форм ведения бизнеса в российской экономике и в отрасли информационно-коммуникационных технологий (далее – ИКТ) в частности. Наряду с существующими и потенциальными преимуществами, которые несут в себе платформенные модели ведения бизнеса, во внешней среде появляются факторы, препятствующие дальнейшему развитию и распространению вышеуказанных предпринимательских цифровых платформ и экосистем отрасли ИКТ. В данной статье проведено исследование инвайроментальных факторов, ограничивающих развитие предпринимательских бизнес-единиц цифровой и экосистемной направленности в отрасли ИКТ.

Ключевые слова: информационно-коммуникационные технологии; отрасль ИКТ, цифровая платформа; бизнес-экосистема; критическая информационная инфраструктура; обеспечение информационной безопасности.

FACTORIAL CONSTRAINTS ON THE DEVELOPMENT OF AN ECOSYSTEM-ORIENTED BUSINESS ENVIRONMENT IN THE ICT INDUSTRY

E. V. Pavlova, *St. Petersburg State University of Telecommunications named after Prof. M. A. Bonch-Bruevich.*

Annotation. The transformation of the economic, political, and social aspects of entrepreneurial activity through digital technologies has led to the emergence of new organizational forms of doing business in the Russian economy and in the information and communication technology (hereinafter - ICT) industry in particular. Along with the existing and potential advantages that platform business models bring, factors appear in the external environment that hinder the further development and dissemination of the above-mentioned entrepreneurial digital platforms and ecosystems of the ICT industry. This article examines the environmental factors limiting the development of entrepreneurial business units of digital and ecosystem orientation in the ICT industry.

Keywords: information and communication technology; ICT industry; digital platform; business ecosystem; critical information infrastructure; information security.

Введение

Распространение экосистем в бизнес-среде российской экономики в целом и отрасли ИКТ, в частности, представляет собой закономерный этап развития Индустрии 4.0, так как масштабная цифровизация бизнес-процессов, происходящих на предприятиях всех отраслей экономики, привела к трансформации существующих моделей ведения бизнеса [1-2]. В основе функционирования любой экосистемы находится платформенная технология, так как экосистема представляет собой совокупность разнообразных онлайн-сервисов, объединенных между собой посредством единой цифровой платформы [3].

Цифровая платформа в отрасли ИКТ, в свою очередь, является базой экосистемы, так как обеспечивает беспрепятственный вход пользователя к любому его сервису посредством единого *ID*, так как на смену общественным идентификационным документам потребителя приходит персональный *ID* (с английского *identifier*), который является «единым паспортом» клиента в цифровом информационном пространстве [4].

Целью проведенного исследования, результаты которого отражены в статье, является идентификация факторов негативного влияния внешней среды на развитие и распространение цифровых экосистем в отрасли ИКТ.

Понятие термина «цифровая платформа»

Определение понятия «цифровая платформа» не приводится в нормативно-правовых актах, устанавливающих сущность, порядок работы и назначение государственных единых цифровых платформ, например, в социальной сфере, в сфере занятости и трудовых отношений «Работа в России», таких как «Одно окно экспортера», «ГосТех», «Госмаркет», «Национальная система пространственных данных», «Цифровая аналитическая платформа предоставления статистических данных» и др.[1]

Тем не менее в Постановлении Правительства РФ от 30 апреля 2019 г. № 529 «Об утверждении Правил предоставления субсидий российским организациям на возмещение части затрат на разработку цифровых платформ и программных продуктов в целях создания и (или) развития производства высокотехнологичной промышленной продукции» приводится определение «цифровой платформы», под которой понимается совокупность информационных технологий и технических средств, направленных на решение различных технологических задач и взаимодействие субъектов экономической деятельности в промышленной сфере[2]. Данный термин не дает определение понятия «цифровая платформа» в широком смысле и может использоваться только применительно к предприятиям промышленной сферы деятельности [5].

В более широком смысле термин «цифровая платформа» раскрыт в докладе Центрального банка России от апреля 2021 г. о регулировании экосистемной модели ведения бизнеса, в котором поднимаются вопросы отрицательного влияния

---

[1] Постановление Правительства РФ от 13 мая 2022 г. N 867 «О единой цифровой платформе в сфере занятости и трудовых отношений «Работа в России» – URL: https://base.garant.ru/404612909/ (дата обращения: 11.05.2024).

Постановление Правительства РФ от 29 декабря 2023 г. N 2386 «О государственной информационной системе «Единая централизованная цифровая платформа в социальной сфере» – URL: https://base.garant.ru/408324253/ (дата обращения: 18.07.2024).

Постановление Правительства РФ от 30 ноября 2022 г. № 2194 «Об утверждении Положения о федеральной государственной информационной системе «Управление единой цифровой платформой Российской Федерации «ГосТех» и Положения о федеральной государственной информационной системе «Госмаркет» – URL: https://base.garant.ru/405875901/ (дата обращения: 10.06.2024).

Постановление Правительства РФ от 7 июня 2022 г. № 1040 «О федеральной государственной информационной системе «Единая цифровая платформа «Национальная система пространственных данных» – URL: https:// base.garant.ru/404817579/ (дата обращения: 15.06.2024).

Постановление Правительства РФ от 22 июня 2021 г. N 956 «О государственной информационной системе «Цифровая аналитическая платформа предоставления статистических данных» – URL: https://base.garant.ru/401391213/ (дата обращения: 01.08.2024).

[2] Постановление Правительства РФ от 30 апреля 2019 г. N 529 «Об утверждении Правил предоставления субсидий российским организациям на возмещение части затрат на разработку цифровых платформ и программных продуктов в целях создания и (или) развития производства высокотехнологичной промышленной продукции» – URL: https://base.garant.ru/72237228/ (дата обращения: 15.07.2024).

экосистем на общество в целом и конкурентную среду национальной экономики, рассматриваются вопросы нормативно-правового регулирования деятельности экосистем в Китае, Европейском Союзе и США и возможность адаптации данных законодательных практик применительно к российской экономике [6]. В вышеуказанном докладе под цифровой платформой понимается информационная система, функционирующая посредством сети интернет и обеспечивающая взаимодействие различных субъектов экономических отношений, представленных на ней, через процессы распределения и обмена товарами и услугами[3].

Так как цифровая платформа и электронные технологии являются ключевым ядром экосистемных форм ведения бизнеса отрасли ИКТ, то приоритетное значение в данных моделях уделяется вопросам, связанным с обеспечением информационной безопасности всех сервисов, компонентов и составных элементов платформы [7]. Обусловлена подобная необходимость значительными масштабами вовлечения в деятельность платформы ее субъектов-участников рынка ИКТ, к которым относятся группы разработчиков, потребителей и поставщиков услуг, а также наличием больших объемов персональных данных [8].

Взаимосвязь цифровых платформ отрасли ИКТ и объектов критической информационной инфраструктуры

Определение цифровой платформы как информационной системы и наличие значительного объема идентификационных данных пользователей приводит к тому, что разнообразные сегменты экосистемы, основанные на цифровых технологиях, становятся объектами критической информационной инфраструктуры (далее – КИИ). К объектам КИИ в соответствии с федеральным законом от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» относятся информационные системы, автоматизированные системы управления и информационно-телекоммуникационные сети[4]. Соответственно, государственные учреждения, госорганы и любые юридические лица, в том числе и бизнес-экосистемы, которые являются владельцами или арендаторами объектов КИИ, автоматически становятся субъектами КИИ [9].

В этой связи цифровые платформы бизнес-экосистем отрасли ИКТ попадают под действия положений и требований нормативно-правовых актов, направленных на обеспечение безопасности объектов КИИ [10]. Определение критической информационной инфраструктуры также приведено в Федеральном законе от 26 июля 2017 г. № 187-ФЗ, который относит в данную категорию объекты КИИ, а также сети электросвязи, с помощью которых обеспечивается взаимодействие между данными объектами. Перечень отраслей КИИ достаточно обширен и согласно Государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации включает в себя следующие сферы: связь, топливно-энергетический комплекс, здравоохранение, оборонную промышленность, банковскую сферу, науку, горнодобывающую промышленность, атомную

[3] Экосистемы: подходы к регулированию / Доклад для общественных консультаций. Центральный банк Российской Федерации. Апрель 2021 г. – URL: https://cbr.ru/Content/Document/File/119960/Consultation_Paper_02042021.pdf (дата обращения: 29.07.2024).

[4] Федеральный закон от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» – URL: https://base.garant.ru/71730198/ (дата обращения: 03.06.2024).

энергетику, химическую промышленность, транспорт, ракетно-космическую промышленность, энергетику, металлургическую промышленность и сферу регистрации прав на недвижимое имущество.

В качестве примера объектов КИИ негосударственных коммерческих предприятий экосистемной направленности в докладе Центрального банка Российской Федерации приводятся разнообразные цифровые сервисы экосистемы компании «Яндекс», так как на применении сервисов платформы «Яндекс.Карты», «Яндекс.Транспорт», «Яндекс.Навигатор» основано распределение дорожного трафика в Москве. Отнесение цифровых платформ и сервисов экосистем к объектам КИИ влечет за собой не право, а обязанность субъектов КИИ обеспечивать безопасность КИИ [11]. Под безопасностью КИИ следует понимать ее бесперебойное функционирование в период проведения компьютерной атаки и после ее завершения.

Мероприятия для обеспечения информационной безопасности цифровых платформ отрасли ИКТ как объектов критической информационной инфраструктуры

Для обеспечения безопасности КИИ от собственников экосистем требуется на постоянной и непрерывной основе проводить комплексные мероприятия по обеспечению информационной безопасности, внедрять на приоритетной основе меры по предотвращению компьютерных атак на экосистему в целом и ее участников в частности[5]. В соответствии с федеральным законом от 26 июля 2017 г. № 187-ФЗ под компьютерной атакой понимается специальная адресная процедура влияния на объекты КИИ и сетей электросвязи для вывода из строя вышеуказанных объектов либо нанесение ущерба безопасности их информационным данным, а под компьютерным инцидентом понимается событие, заключающееся в сбое или завершении работоспособности объекта или объектов КИИ, а также применяемой для их взаимосвязи сети электросвязи, или несоблюдении безопасности информационных данных вышеуказанных объектов по причине компьютерной атаки.

Функционирование экосистемы как субъекта КИИ налагает на нее следующие обязанности:

1) взаимодействие посредством НКЦКИ с ФСБ России в части обнаружения, предупреждения и ликвидации последствий компьютерных атак;

2) немедленное извещение о компьютерных инцидентах и атаках ФСБ России через НКЦКИ;

3) незамедлительное оповещение Центрального банка России о компьютерных инцидентах и атаках, если компания является банковской организацией или работает в финансовой сфере;

4) принятие комплекса мер по устранению влияния компьютерных атак по установленному ФСБ России алгоритму;

5) предоставление данных в Государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (далее – ГосСОПКА) в соответствии с Приказом № 367, утвержденным ФСБ России[6];

---

[5] Приказ Федеральной службы по техническому и экспортному контролю от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» – URL: https://base.garant.ru/71901880/ (дата обращения: 10.06.2024).

[6] Приказ ФСБ России от 24 июля 2018 г. N 367 «Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации

6) взаимодействие с другими субъектами КИИ по вопросам обмена данными об атаках;

7) направление сотрудника компании в рабочую группу, создаваемую НКЦКИ из делегатов субъектов КИИ;

Для выполнения вышеуказанных обязанностей собственнику и менеджменту экосистемы как субъекту КИИ необходимо произвести комплекс следующих мероприятий:

1) подготовить защищенный канал межсетевого взаимодействия с НКЦКИ;

2) подключить предприятие к технической инфраструктуре НКЦКИ через личный кабинет;

3) провести инвентаризацию имеющихся на предприятии объектов КИИ: информационных систем, автоматизированных систем управления и информационно-телекоммуникационных сетей;

4) выполнить категорирование определенных в результате инвентаризации объектов КИИ, т. е. присвоить каждому объекту КИИ одну из четырех категорий[7];

5) провести согласование категории объектов КИИ с Федеральной службой по техническому и экспортному контролю;

6) осуществлять защитные меры, исходя из категории значимости объектов КИИ;

7) использовать специальные превентивные средства и средства элиминирования отрицательного воздействия атак;

8) обеспечить структурное подразделение по обеспечению информационной безопасности следующими специалистами:

- специалист по обнаружению компьютерных атак и инцидентов;
- специалист по обслуживанию средств;
- специалист по оценке защищённости;
- специалист по ликвидации последствий компьютерных инцидентов;
- специалист по установлению причин компьютерных инцидентов.

9) проводить тренировки и специальные киберучения работников на регулярной основе;

10) проводить систематическое повышение квалификации ответственных сотрудников в сфере информационной безопасности;

11) обеспечить участие работников компании в специализированных соревнованиях по информационной безопасности;

12) разработать план, сценарии и инструкции по реагированию на инциденты, предупреждения и ликвидации последствий компьютерных атак.

Как видно из вышеперечисленного, реализация всех вышеизложенных мероприятий требует от экосистемы наличия значительных финансовых резервов денежных средств на проведение всего комплекса превентивных и итеративных мер по обеспечению информационной безопасности компонентов и сервисов экосистемы, что для владельцев локальных цифровых платформ, не связанных с

последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» – URL: https://normativ.kontur.ru/document?moduleId=1&documentId=443301 (дата обращения: 05.07.2024).

[7] Постановление Правительства РФ от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» – URL: https://base.garant.ru/71876120/ (дата обращения: 22.05.2024).

крупным бизнесом и экосистемами, будет завышать стоимость предоставляемых ими услуг и снижать конкурентную привлекательность на клиентском рынке [12].

Ответственность и надзорная деятельность за выполнением требований по обеспечению безопасности цифровых платформ отрасли ИКТ

Для осуществления методической и надзорной деятельности за выполнением задач по обеспечению безопасности объектов КИИ в соответствии с Указом Президента Российской Федерации от 15 января 2013 года № 31с создана Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, которая представляет собой систему, включающую в себя силы и средства обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты[8]. К силам ГосСОПКА относятся структуры Федеральной службы безопасности России, Национальный координационный центр по компьютерным инцидентам (далее – НКЦКИ) и субъекты КИИ. В задачи ФСБ РФ входит выполнение работ по организации ГосСОПКА, создание методических рекомендаций по обнаружению атак, по формированию защиты и разработка алгоритма обмена информацией об инцидентах между участниками процессов обеспечения безопасности объектов КИИ.

За невыполнение требований по предоставлению необходимой информации и обеспечению безопасности объектов КИИ предусмотрены меры административной ответственности в соответствии с Федеральным законом от 26 мая 2021 года № 141-ФЗ в размере до 500 000 рублей[9].

Административная ответственность также налагается на юридические и физические лица, владеющие значимыми объектами КИИ, в случае нарушения алгоритма извещения о случаях компьютерных атак или инцидентов. Степень значимости определяется присвоением одной из четырех категорий и включением в реестр значимых объектов КИИ в соответствии с приказом Федеральной службы по техническому и экспортному контролю от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов КИИ Российской Федерации». Категорирование объектов КИИ осуществляется на основании пяти аспектов: социальной, экономической, политической, экологической значимости и критериев безопасности. Всего устанавливаются три категории значимости: первая, вторая и третья, но объекты, которые в соответствии с критериями значимости не попадают ни в одну из перечисленных категорий значимости, образуют четвертую группу «без категории». Отнесение объекта КИИ к той или иной категории определяется на основании перечня критериев по каждому из пяти блоков значимости [13].

За нарушения в сфере обеспечения безопасности объектов КИИ помимо административной предусмотрена уголовная ответственность. Так, в Уголовный кодекс Российской Федерации введена статья 274.1 Федеральным законом «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной

[8] Указ Президента РФ от 15 января 2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» – URL: https://base.garant.ru/70299068/ (дата обращения: 18.06.2024).

[9] «Кодекс Российской Федерации об административных правонарушениях» от 30.12.2001 № 195-ФЗ – URL: https://base.garant.ru/12125267/ (дата обращения: 01.07.2024).

инфраструктуры Российской Федерации» от 26.07.2017 N 194-ФЗ. Статья 274.1 Уголовного кодекса устанавливает ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации. Неправомерность действий может быть выражена в следующем:

- нарушении правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации объектов КИИ;
- нарушение правил доступа к информации объектов КИИ.

По вышеуказанной статье предусмотрено максимальное наказание в виде лишения свободы на срок до десяти лет.

В настоящее время в российской практике имеются примеры применения норм уголовного права за невыполнение требований по предоставлению необходимой информации и обеспечению безопасности объектов КИИ [14]. В апреле 2024 г. был задержан заместитель генерального директора по информационным технологиям и производству ООО «Сирена-Трэвел» по статье 274.1 УК в связи со взломом в сентябре 2023 г. базы данных компании в результате масштабной *DDoS*-атаки хакерской группировки, в результате чего у авиакомпаний «Аэрофлот», «Уральских авиалиний» и *Red Wings* возникли перебои с регистрацией пассажиров, так как компания «Сирена-Трэвел» является разработчиком российской системы бронирования авиабилетов «Леонардо», на которую в 2022 г. перешли значимые отечественные авиаперевозчики, такие как группы компаний «Аэрофлот» и *S*7, с целью замещения иностранного программного обеспечения американских систем *Sabre* и *Navitaire*, а также испанской *Amadeus* в сфере бронирования авиабилетов для исключения рисков утечки персональных данных клиентов авиакомпаний и минимизации прочих рисков отрасли авиаперевозок. По информации ООО «Сирена-Трэвел» компания исполнила свои обязательства по своевременному уведомлению органов ГосСОПКИ о произошедшем инциденте в сфере информационной безопасности.

С целью исключения возможности попадания под вышеуказанные меры административной и уголовной ответственности владельцам и менеджменту платформенного бизнеса и экосистемных моделей следует:

- соблюдать сроки извещения Национального координационного центра по компьютерным инцидентам о компьютерных инцидентах не позднее 3 часов с момента обнаружения для значимых объектов КИИ и не позднее 24 часов для иных объектов КИИ;
- при включении объекта КИИ в реестр значимых объектов КИИ подготовить и утвердить план ответных мер на компьютерные атаки и инциденты с направлением копии в Национальный координационный центр по компьютерным инцидентам не позднее 7 календарных дней;
- ежегодно подготавливать и осуществлять тренировки по применению мероприятий плана ответных мер.

Необходимо отметить, если для обеспечения безопасности объектов КИИ необходимо оказывать защиту другим информационным ресурсам, которые не являются субъектами КИИ, то компании-владельцы вышеуказанных ресурсов также могут быть отнесены к системе ГосСОПКА и обязаны будут обеспечивать выполнение выше обозначенного комплекса мер и обязанностей [15].

Заключение

Проведение комплекса вышеизложенных действий и мероприятий, направленных на выполнение положений федерального закона от 26 июля 2017 г.

№ 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» по обеспечению безопасности объектов КИИ, отвлекает у компаний отрасли ИКТ значительные объемы трудовых и финансовых ресурсов.

Выделить средства, достаточные для закупки априорных мер защиты (защитные меры, эксплуатация которых сокращает качественно или количественно существующие уязвимости объектов защиты информационных активов, тем самым снижая вероятность реализации соответствующих угроз информационной безопасности, например, средства защиты от несанкционированного доступа) и апостериорных защитных мер (защитные меры, эксплуатация которых сокращает степень тяжести последствий нарушения свойств информационной безопасности информационных активов, например, средства резервного копирования и восстановления информации) могут себе позволить только собственники крупных цифровых платформ и бизнес-экосистем отрасли ИКТ, при этом малый и средний бизнес становятся невалидными на конкурентном рынке ИКТ.

Таким образом, невозможность проведения мероприятий по обеспечению безопасности объектов КИИ имеет негативное влияние на предложение услуг со стороны цифровых платформ малого и среднего бизнеса отрасли ИКТ, а также выражается в повышении себестоимости и, как следствие, ценового предложения со стороны крупных участников цифрового экосистемного рынка.

Следствием этих тенденций будет существенное удорожание стоимости услуг предприятий экосистемной направленности отрасли ИКТ для конечного потребителя, монополизация рынка ИКТ и сокращение объемов спроса со стороны цифрового клиентского рынка ИКТ.

Литература

1. Павлова Е.В., Свистунов Л.О. Цифровизация экономики как часть процесса индустрии 4.0 // В сборнике: Современный менеджмент: проблемы и перспективы // Сборник статей по итогам XVIII национальной научно-практической конференции с международным участием. Санкт-Петербург, 2023. – С. 22-25.
2. Шитиков И.Е., Кваша Н.В. Актуальные направления устойчивого развития экономики России // В сборнике: Интеллектуальная инженерная экономика и Индустрия 5.0 (ИНПРОМ-2024). Сборник трудов X Международной научно-практической конференции. В 2-х томах. Санкт-Петербург, 2024. – С. 367-369.
3. Павлова Е.В., Куганов В.Г. Экономические проблемы цифровизации отдельных отраслей и сфер деятельности // Национальные концепции качества: роль качества в научно-технологическом развитии страны: сб. материалов Национал. науч.-практ. конф. с междунар. участием. СПб., 2023. – С. 263-266.
4. Павлова Е.В., Кулакова Ю.В. Перспективы развития нейросетевых технологий в условиях цифровизации экономики // Экономика и качество систем связи, 2024. – № 1 (31). – С. 10-17.
5. Александров М.А., Макаров В.В., Слуцкий М.Г. Инновационные услуги телекоммуникационного предприятия, обусловленные процессами цифровой трансформации // Журнал правовых и экономических исследований, 2021. – № 2. – С. 139-144.
6. Жолобова А.И., Макаров В.В., Павлова Е.В. Проблемы развития рынка информационных технологий в условиях пандемии // Евразийское Научное Объединение, 2021. – № 10-3 (80). – С. 181-184.
7. Жолобова А.И., Макаров В.В., Павлова Е.В. Информационные технологии в цифровой экономике // Экономика и бизнес: теория и практика, 2021. – № 7 (77). – С. 59-62.

8. Макаров В.В., Павлова Е.В. Влияние экосистем на цифровую трансформацию экономики // Журнал правовых и экономических исследований, 2024. – № 2. – С. 209-214.
9. Куганов В.Г., Лобанов М.А. Обеспечение конкурентоспособности малого бизнеса в условиях цифровизации экономики // В сборнике: Современный менеджмент: проблемы и перспективы. Сборник статей по итогам XVI международной научно-практической конференции. Санкт-Петербург, 2021. – С. 523-527.
10. Макаров В.В., Гусев В.И., Воронин А.Г. Методологическая парадигма исследования интеллектуального капитала в условиях информационного общества // Российский гуманитарный журнал, 2012. – Т. 1. – № 1. – С. 78-83.
11. Исаков А.В., Свиридов И.В., Фёдорова М.Ю. Спрос и структура рынка инфокоммуникационных услуг в России // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). Сборник научных статей: в 4-х томах. Санкт-Петербург, 2021. – С. 439-442.
12. Макаров В.В., Слуцкий М.Г., Устриков Н.К. Проблемы и задачи цифровой трансформации экономики России // Международный журнал гуманитарных и естественных наук, 2020. – № 4-1 (43). – С. 174-177.
13. Куганов В.Г., Лобанов М.А. Особенности функционирования предприятий в условиях цифровизации // В сборнике: Современный менеджмент: проблемы и перспективы // Сборник статей по итогам XVIII национальной научно-практической конференции с международным участием. Санкт-Петербург, 2023. – С. 17-21.
14. К разработчику системы бронирования «Леонардо» пришли силовики. – URL: https://www.rbc.ru/politics/03/04/2024/660d55bb9a79473dc22a5041/ (дата обращения: 04.04.2024).
15. Как и кому необходимо подключаться к ГосСОПКА – URL: https://gossopka.ru/pub/kak-i-komu-neobkhodimo-podklyuchatsya-k-gossopka/ (дата обращения: 03.05.2024).