НОВЫЕ ЭЛЕМЕНТЫ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ: НАЦИОНАЛЬНЫЙ И МЕЖДУНАРОДНЫЙ АСПЕКТ

Карцхия А. А.[1]

Аннотация

Цель исследования *состоит в исследовании правовых аспектов структурного развития национальной безопасности для выявления тенденций и факторов, влияющих на формирование национальных интересов отдельного государства и международных отношений, а также исследование системы национальной безопасности с правовых позиций.*

Метод исследования: *сравнительно-правовой анализ актуального национального российского и зарубежного законодательства и стратегий развития, международных договоров и соглашений по вопросам национальной безопасности и практики их применения.*

Результат: *исследование выявило объективные предпосылки для формирования новых самостоятельных элементов системы национальной безопасности Российской Федерации, включая биобезопасность, кибербезопасность, криптобезопасность и инвестиционную безопасность. Эти новые элементы формируют свой самостоятельный предмет и способы обеспечения национальных интересов и национальной безопасности в указанных сферах, имеют свою законодательную базу и особенности правового регулирования, что с несомненной очевидностью определяет необходимость их выделения в самостоятельные структурные элементы национальной безопасности для последующего законодательного регулирования и практического осуществления с точки зрения защиты национальных интересов.*

Ключевые слова: *суверенитет, конституционные права, международные соглашения, иностранные инвестиции, цифровые права, биобезопасность, кибербезопасность, криптобезопасность.*

DOI: 10.21681/2311-3456-2020-06-72-82

1.Введение

Современное состояние мировых экономических и торговых отношений в совокупности с международным научным и техническим сотрудничеством и кооперацией в условиях транснационального применения цифровых технологий, услуг и сервисов сети Интернет и других возможностей глобальных коммуникаций, социальных сетей и иных IT-технологий испытывает все усиливающееся влияние односторонней протекционистской и антиконкурентной санкционной политики в отношении России, Китая и некоторых других стран со стороны США и их союзников, а в ряде случаев жесткая конкуренция проявляется и между самими «западными партнерами». Характерным примером в этом отношении является ситуация с Brexit, когда только 25 декабря 2020 г. удалось достигнуть всеобъемлющего Соглашения об условиях выхода Великобритании из состава ЕС - практически в самый последний момент истекающего срока и под влиянием нарастающих торговых конфликтов и беспорядков на временно закрытых ввиду опасности распространения пандемии Covid-19 пограничных переходах между Великобританией и Францией. Соглашение в объеме 1256 страниц охватывает не только торговлю товарами и услугами, но и широкий круг других областей в интересах ЕС и Великобритании, таких как инвестиции, конкуренция, государственная помощь, налоговая прозрачность, воздушный и автомобильный транспорт, энергетика и устойчивость, рыболовство, защита данных и координация социального обеспечения.[2]

Общемировая ситуация усугубляется и множеством локальных военных конфликтов и противостояний практически на всех континентах нашей планеты.

Как отмечалось в докладе Всемирного экономического форума «О глобальных рисках 2020»[3], мощные экономические, демографические и технологические процессы в мире формируют новый баланс сил, результатом чего является неурегулированный геополитический ландшафт, в котором государства все чаще рассматривают возможности и вызовы через односторонние интересы. Это формирует новую архитектуру глобальных рисков в условиях геополитической и геоэкономической неопределенности. К их числу таких рисков относятся:

- макроэкономическая нестабильность и финансовое неравенство;

2 https://ec.europa.eu/transparency/regdoc/rep/1/2020/EN/COM-2020-857-F1-EN-ANNEX-1-PART-1.PDF

3 The Global risks report 2020 // WEF. – 2020. – P. 6–10. URL: https://www.weforum.org/reports/ the-global-risks-report-2020.

1 Карцхия Александр Амиранович, доктор юридических наук, доцент, профессор кафедры гражданско-правовых дисциплин РГУ нефти и газа (НИУ) им. И.М. Губкина, Москва, Россия. Email: arhz50@mail.ru

- нарастающие климатические угрозы и риски ускоряющейся утраты биоразнообразия;
- фрагментация киберпространства цифровых технологий как угроза дальнейшему технологическому развитию последующих поколений технологий;
- неспособность системы общественного здравоохранения противостоять неинфекционным заболеваниям и угрозам пандемий ввиду изменения социальных, экологических, демографических и технологических моделей, которые угрожают свести на нет важнейшие достижения в области благополучия и процветания.

Стратегия национальной безопасности Российской Федерации[4] отмечает возрастающее влияние политических факторов на экономические процессы, а также попытки применения отдельными государствами экономических методов, инструментов финансовой, торговой, инвестиционной и технологической политики для решения своих геополитических задач ослабляют устойчивость системы международных экономических отношений.

Вместе с тем, глобальные торговые и экономические отношения испытывают сильное давление со стороны санкций и иных мер давления публичного характера.

Так, 31 июля 2014 года Европейский Союз принял пакет ограничительных мер против подрыва или угрозы суверенитету и территориальной целостности Украины, который направлен на отраслевое сотрудничество и обмены с Российской Федерацией и состоит из мер, нацеленных на ограничение доступа российских государственных финансовых институтов на рынки капитала ЕС, эмбарго на торговлю оружием, запрет на экспорт товаров двойного назначения для военного назначения и конечных пользователей, а также ограничения доступа к некоторым чувствительным технологиям, особенно в нефтяном секторе[5].

В дополнении к этим финансовым санкциям 7 декабря 2020 года Совет Европейского Союза принял Регламент о глобальном режиме санкций в области прав человека[6], аналогичный программе санкций Магнитского, которую использует Управление по контролю за иностранными активами Министерства финансов США (Department of the Treasury's Office of Foreign Assets Control - OFAC). Несмотря на то, что этот Регламент не имеет силы законодательного акта, он нацелен на отдельных лиц, организации и органы, будь то государственные или негосударственные субъекты, а также на тех, кто оказывает техническую, финансовую или материальную поддержку лицам, которые "несут ответственность, участвуют или связаны с серьезными нарушениями прав человека и злоупотреблениями во всем мире, независимо от того, где они произошли". Это включает в себя введение целенаправленных санкций за такие акты, как геноцид, преступления против человечности и другие серьезные нарушения или злоупотребления в области прав человека (например, пытки, рабство, произвольные казни, произвольные задержания и т. д.), а также другие широко распространенные, систематические и серьезные нарушения прав человека (например, торговля людьми, сексуальные и гендерные нарушения, нарушения или злоупотребления свободой собраний, ассоциаций, слова, религии). Регламент позволяет государствам-членам ЕС или Верховному представителю ЕС по иностранным делам и политике безопасности предлагать любые санкции в указанных рамках, которые затем будут приняты Советом ЕС, который, в свою очередь, может ввести ограничительные меры, такие как запрет на въезд, замораживание денежных средств или запрет указанным физическим и юридическим лицам прямо или косвенно предоставлять финансирование и кредиты.

Новая программа расширяет полномочия ЕС вводить санкции в отношении физических и юридических лиц, независимо от их местонахождения, которые обвиняются в нарушениях прав человека. Программа появилась всего через несколько месяцев после первых санкций, введенных в рамках аналогичной программы в Соединенном Королевстве и программы США в рамках экспортного контроля OFAC. Однако, еще предстоит выяснить, присоединится ли новая программа ЕС к США и Великобритании в активном использовании их нового санкционного режима в ближайшее время.

При этом следует учесть, что в условиях глобализации мирового рынка, социальных и экономических связей в международной и национальной правоприменительной практике последних десятилетий все чаще возникают вопросы, связанные с подсудностью коммерческих и инвестиционных споров из трансграничных сделок, а также проблема экстерриториальности решений судов в отношении субъектов права иностранных государств. Решение таких вопросов должно отвечать национальным интересам в обеспечении незыблемости конституционного строя, суверенитета, независимости, государственной и территориальной целостности Российской Федерации. Показательно в связи с этим определение Конституционного Суда РФ от 24 декабря 2020г. № 2867-О-Р о разъяснении Постановления Конституционного Суда Российской Федерации от 27 марта 2012 года № 8-П по делу о проверке конституционности пункта 1 статьи 23 Федерального закона «О международных договорах Российской Федерации»[7], в котором Конституционный Суд РФ подтвердил, что правила ратифицированного Российской Федерацией международного договора, если они нарушают основные конституционные положения России, не могут и не должны применяться в национальной правовой системе, основанной на верховенстве Конституции Российской Федерации, не до-

4 Указ Президента РФ от 31.12.2015 N 683 «О Стратегии национальной безопасности Российской Федерации» // СЗ РФ, 04.01.2016, N 1 (часть II), ст. 212

5 Council Regulation (EU) No 960/2014 (amended by Council Regulation (EU) No 1290/2014 and Council Regulation (EU) 2015/1797), Regulation (EU) No 833/2014. URL: https://www.gov.uk/ government/publications/financial-sanctions-ukraine-sovereignty-and-territorial-integrity.

6 COUNCIL REGULATION (EU) 2020/1998 of 7 December 2020 concerning restrictive measures against serious human rights violations and abuses. URL: http://data.europa.eu/eli/reg/2020/1998/oj

7 Определение Конституционного Суда РФ от 24 декабря 2020г. №2867-О-Р. URL: http://doc.ksrf.ru/decision/KSRFDecision507357.pdf

пуская нарушений основ конституционного строя. Правовая позиция Конституционного Суда РФ определена в связи с решением международного коммерческого арбитражного суда в Гааге (2020г.) по делу компании «Юкос» и в части невозможности распространения компетенции международного коммерческого арбитража на разрешение инвестиционных споров с участием государства, подсудных только национальным судам в силу национального законодательства. Такая правовая позиция полностью соответствует положениям Венской конвенции о праве международных договоров (1969г.) и Федеральному закону от 15 июля 1995 года № 101-ФЗ «О международных договорах Российской Федерации».

Сложившуюся ситуацию необходимо оценивать с позиции соответствия Стратегии национальной безопасности РФ по обеспечению национальных интересов и созданию стабильной и устойчивой системы международных отношений, опирающейся на международное право и основанной на принципах равноправия, взаимного уважения, невмешательства во внутренние дела государств, взаимовыгодного сотрудничества, политического урегулирования глобальных и региональных кризисных ситуаций.

В наши дни мы наблюдаем подтверждение прогнозов в Стратегии национальной безопасности РФ, которая определила перспективы негативного воздействия на экономическую безопасность посредством введенных против Российской Федерации ограничительных экономических мер, а также иные угрозы, включая глобальные и региональные экономические кризисы, усиление недобросовестной конкуренции, неправомерное использование юридических средств.

В этих условиях особо пристальное внимание Россия и многие другие страны уделяют проблемам национальной безопасности.

2. Формирование новых элементов структуры национальной безопасности

Национальная безопасность определяется в Стратегии национальной безопасности РФ как состояние защищенности личности, общества и государства от внутренних и внешних угроз, при котором обеспечиваются реализация конституционных прав и свобод граждан Российской Федерации, достойные качество и уровень их жизни, суверенитет, независимость, государственная и территориальная целостность, устойчивое социально-экономическое развитие Российской Федерации. Национальная безопасность включает в себя оборону страны и все предусмотренные законом виды безопасности, прежде всего государственную, общественную, информационную, экологическую, экономическую, транспортную, энергетическую безопасность, безопасность личности. Эти составные части рассматриваются автором в качестве элементов национальной безопасности. Вместе с тем, полагаем, что в последние годы формируются новые самостоятельные элементы национальной безопасности, о которых пойдет речь ниже.

Биобезопасность. В последние годы отчетливо прослеживается тенденция по формированию нового элемента национальной безопасности – биологической безопасности. Как указывается в Стратегии национальной безопасности РФ, наряду с сохранением рисков увеличения числа стран - обладателей ядерного оружия, распространения и использования химического оружия, есть неопределенность относительно фактов обладания иностранными государствами биологическим оружием, наличия у них потенциала для его разработки и производства. На территориях соседних с Россией государств расширяется сеть военно-биологических лабораторий США (п.19).

Ряд ведущих стран, включая Россию, разработали законы и стратегии по вопросам биологической защиты и биобезопасности, предусматривающие защиту населения и окружающей среды от воздействия опасных биологических факторов и противодействие биологическим угрозам и рискам, устранения их негативных последствий.

Наиболее серьезные угрозы связаны с биологическим оружием и таким явлением, как биотерроризм, использующим высокопатогенные и инфекционные бактерии, вирусы и токсины в военных и иных террористических операциях с целью вызвать инфекцию, болезни и смертность среди людей, животных или растений и поставить под угрозу социальную стабильность и национальную безопасность государства. Не случайно, поэтому, часть современных биотехнологий включены в список «оружия массового уничтожения» *(''weapons of mass destruction"*) [1]. Стратегии биологической безопасности разработаны в Великобритании (*UK Biological Security Strategy*)[8], в США- Национальная стратегия биологической защиты (*National Biodefense Strategy*)[9] для защиты страны от биологических угроз, предотвращения биоинцедентов и борьбы с их последствиями. В КНР, наряду с принятием закона о ядерной безопасности как составной части национальной безопасности, разработан закон о биологической безопасности в целях обеспечения безопасности национальных биоресурсов, стимулировании и защите развития биотехнологий, предотвращении и запрете применения биологических агентов или биотехнологий, которые могут нанести ущерб национальной безопасности страны.

В Российской Федерации придается большое значение выработке правовых основ национальной биологической безопасности. В силу этого и в целях реализации Основ государственной политики Российской Федерации в области обеспечения химической и биологической безопасности на период до 2025 года и дальнейшую перспективу[10] в 2020г. Государственной Думой принят в первом чтении проект федерального закона «О биологической безопасности Российской

8 UK biological security strategy. 30 July 2018 // URL: https://www.gov.uk/government /publications/biological-security-strategy.

9 National Biodefense Strategy. September 18, 2018 // URL: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Biodefense-Strategy.pdf.

10 Утверждены Указом Президента РФ от 11.03.2019 г. № 97 // СЗ РФ, 18.03.2019 г., № 11, ст. 1106.

Федерации»[11], предусматривающий комплексное регулирование вопросов обеспечения биологической безопасности как системы взаимоувязанных мер, функционирующей на основе взаимодействия заинтересованных органов государственной власти в целях противодействия возникновению биологических угроз, организации защиты населения и охраны окружающей среды, а также ликвидации последствий воздействия опасных биологических факторов. Законопроект определяет биологическую безопасность как состояние защищенности населения и окружающей среды от воздействия опасных биологических факторов, при котором обеспечивается допустимый уровень биологического риска, формулирует также и основные биологические угрозы (опасности), с которыми связаны биологические риски, представляющие собой вероятность причинения вреда (с учетом его тяжести) здоровью человека, животным, растениям и (или) окружающей среде в результате воздействия опасных биологических факторов. Биологическими угрозами (опасностями) считаются опасные биологические факторы, способные привести к возникновению и (или) распространению массовых болезней (эпидемий, эпизоотий, эпифитотий и отравлений), ухудшению ситуации в области обеспечения биологической безопасности и (или) перерастанию ее в чрезвычайную ситуацию.

В большинстве случаев биобезопасность определяется способностью нации эффективно реагировать на биологические угрозы и риски, поддерживать и защищать национальную безопасность и интересы своих граждан, включая меры по борьбе с основными инфекционными заболеваниями, защитные меры против биологического оружия и биотерроризма, злоупотребления достижениями биотехнологий, предотвращение вторжения чужеродных организмов, опасных для человека и окружающего его мира. Несомненно, что биобезопасность, как показывает практика сегодняшнего дня в условиях глобальной борьбы с пандемией Covid-19, является одним из важнейших элементов национальной безопасности каждого государства и базисным фактором для защиты национальных интересов страны как объективно значимые потребности личности, общества и государства в обеспечении их защищенности и устойчивого развития.

В связи с этим, как полагает автор [1] и другие эксперты [2], [3], исключительно актуальным в настоящее время является стремление к развитию международного сотрудничества и национального правового регулирования в сфере биологической безопасности. По мнению автора, стремительное развитие биотехнологий и широкомасштабная интеграция в этой области способствовало развитию биобезопасности как важного элемента национальной безопасности как с позиции биозащищенности (*biosafety*), так и с позиции биобезопасности (*biosecurity*), исходя из их определения Всемирной организации здравоохранения[12] и укрепления режима Конвенции ООН о запрещении разработки, производства и накопления запасов бактериологического (биологического) и токсинного оружия и об их уничтожении[13] и других международных конвенций, включая вопросы генетических исследований, диагностики, скрининга генома, определения правового режима трансплантации органов и тканей человеческого происхождения, а также вопросы исследования человеческих эмбрионов *in vitro*.

Кибербезопасность. Кибербезопасность формируется как новый элемент национальной безопасности. В 2015 году Стратегия национальной безопасности РФ отмечала усиливающееся противоборство в глобальном информационном пространстве, обусловленное стремлением некоторых стран использовать информационные и коммуникационные технологии для достижения своих геополитических целей, а также появление новых форм противоправной деятельности, в частности с использованием информационных, коммуникационных и высоких технологий (п.21,22).

В настоящее время многие страны имеют национальные стратегии и иные документы в сфере кибербезопасности, и в частности: Австралия, Великобритания, Израиль, Канада, Нидерланды, Норвегия, США, ЮАР, Япония [4]. Новая цифровая реальность киберпространства требует нового понимания взаимоотношений между людьми и нациями. Учитывая предысторию, кибербезопасность в государственной политике формализует решение, которым страна объявляет сферу своей цифровой территории, где будет осуществляться национальный суверенитет, с пониманием того, что виртуальное пространство разделено между другими государствами и обладает национальной синергией.

Учитывая глобальный характер киберугроз, обеспечение политики кибербезопасности приобретает исключительное значение не только для частных компаний и холдинговых корпоративных структур, но и на национальном уровне государственной безопасности. В настоящее время кибербезопасность, как таковая не регулируется самостоятельно на международном уровне, учитывая то, что явно устаревшая международная конвенция по киберпреступности (Convention on Cybercrime, Budapest, 23 ноября 2001) регулирует ограниченный круг вопросов киберпреступности [5]. Поэтому роль международных организаций в обеспечении кибербезопасности в настоящее время стала особенно значимой. На национальном уровне в России законодательно выделена профилактика правонарушений в сфере противодействия терроризму и экстремистской деятельности, защиты потенциальных объектов террористических посягательств, в том числе критически важных и (или) потенциально опасных объектов инфра-

11 Проект Федерального закона № 850485-7 «О биологической безопасности Российской Федерации» (ред., принятая ГД ФС РФ в I чтении 21.01.2020) [Электронный ресурс] // URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=PRJ&n=190962#0765056376529383

12 PIP Framework Advisory Group Technical Expert Working Group (TEWG) on GSD. Final Report to the PIP Advisory Group. Geneva: World Health Organization, 2014, pp. 12–15.

13 URL: https://www.un.org/ru/documents/decl_conv/conventions/bacweap.shtml

структуры и жизнеобеспечения, а также мест массового пребывания людей[14].

Вместе с тем, как показали исследования [6], независимо от сходных целей, включая обеспечение киберустойчивости, выбранные подходы к гармонизации и координации различными странами мира, а также нормы национальных стратегий кибербезопасности имеют различия.

Однако кибербезопасность представляет собой более широкое понятие, охватывающее в том числе информационную безопасность, представляющую собой, как определила Доктрина информационной безопасности Российской Федерации[15], состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина. Кибербезопасность направлена, в том числе, на защиту критической инфраструктуры государства на национальном и международном уровне[16] с использованием современных цифровых технологий.

К примеру, ЕС выстраивает определенную общеевропейскую структуру кибербезопасности. Первоначально утвержденная Директива ЕС 2016/1148 о безопасности сетей и информационных систем (Директива NIS)[17] преследовала цель достижения высокого общего уровня безопасности сети и информационных систем в рамках Европейского Союза в условиях распространения электронных услуг, новых технологий, информационных систем и противодействия инцидентам вызывающим нарушение работы ИТ-сервисов и критически важной инфраструктуры. Директива NIS обязывает государства-члены обеспечить, чтобы операторы основных IT-услуг принимали соответствующие технические и организационные меры для управления рисками, связанными с безопасностью своих сетей и информационных систем, а также меры по предотвращению инцидентов, влияющих на безопасность систем для обеспечения непрерывности таких услуг.

В 2020 году Европейская комиссия утвердила новую Стратегию кибербезопасности ЕС[18]. Целью Стратегии определяется укрепление коллективной устойчивости Европы к киберугрозам и обеспечение всех граждан и предприятий надежными и безопасными услугами и цифровыми инструментами. Как отмечается в Стратегии, цифровая трансформация общества, усиленная кризисом COVID-19, расширила ландшафт угроз и породила новые вызовы, требующие адаптированных и инновационных ответных мер. Число кибератак продолжает расти, причем все более изощренные атаки исходят из широкого круга источников как внутри ЕС, так и за его пределами. Поэтому ЕС предпринимает усилия по безопасной цифровизации, являясь движущей силой в решениях мирового класса и стандартов кибербезопасности для основных услуг и критической инфраструктуры, а также для разработки и применения новых технологий. Новая Стратегия направлена на обеспечение глобального и открытого интернета с сильными гарантиями там, где существуют риски для безопасности и основных прав граждан в Европе, и содержит три главных компонента, а именно: нормативные, инвестиционные и политические инициативы. Они будут касаться трех областей деятельности ЕС:

- устойчивость, технологический суверенитет и лидерство;
- оперативный потенциал по предотвращению, сдерживанию и реагированию;
- сотрудничество для продвижения глобального и открытого киберпространства. Устанавливается, что новая Стратегия кибербезопасности ЕС на цифровое десятилетие служит ключевым компонентом формирования цифрового будущего Европы, а также основой плана и стратегии безопасности Европейского Союза на 2020-2025 годы.

В декабре 2020 Европейская комиссия рассмотрела проекты Закона и цифровых рынках, который предлагает новые правила конкуренции для участников цифровых платформ, и Закона о цифровых услуга, который регулирует правила модерации контента для крупных онлайн-платформ. Новые законы призваны создать правовое пространство для цифрового рынка финансовых и иных имущественных активов, что несомненно, потребует обеспечение соответствующего уровня кибербезопасности уже в области цифровых рыночных отношений.

В США утверждена в 2018 г. Национальная киберстратегия США[19] в целях повышения безопасности и устойчивости национальных информационных и других информационных систем, которая предусматривает следующие ключевые приоритеты:

- защита федеральных киберсетей и информации;
- обеспечение безопасности национальной критической инфраструктуры;
- борьба с киберпреступностью и улучшение отчетности о кибер-инцидентах. В частности, одним из главных приоритетов управления кибербезопасности, энергетической безопасности и реагирования на чрезвычайные ситуации является обе-

14 Федеральный закон от 23.06.2016 N 182-ФЗ «Об основах системы профилактики правонарушений в Российской Федерации»// СЗ РФ, 27.06.2016, N26(Часть I), ст. 3851.

15 Указ Президента РФ от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»// СЗ РФ, 12.12.2016, N 50, ст. 7074.

16 Резолюция, принятая Генеральной Ассамблеей 21 декабря 2009 г. [по докладу Второго комитета (A/64/422/Add.3)] 64/211. Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур. URL:https://www.un.org/ga/search/view_doc.asp? symbol=A/RES/64/211&referer=https://www.google.ch/&Lang=R.

17 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. URL: https://eur-lex.europa.eu/ legal-content/EN/TXT/ ?uri=CELEX%3A32016L1148

18 The EU's Cybersecurity Strategy for the Digital Decade, JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL,16.12.2020 JOIN(2020). URL: https://ec.europa.eu/digital-single-market/en/cybersecurity-strategy

19 NATIONAL CYBERSTRATEGY of USA (2018). URL: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

спечение устойчивости национальной электросети и нефтегазовой инфраструктуры к киберугрозам, повышение безопасности, надежности и отказоустойчивости системы электроснабжения для преодоления последствий кибер-инцидента и сохранения стабильности критически важных функций системы, а также контроль в области кибербезопасности на организационном и технологическом уровнях, эффективности реагирования и восстановления после кибер-инцидентов. Важным приоритетом является также повседневный контроль на федеральном уровне за кибербезопасностью для определения приоритетов и координации деятельности по укреплению безопасности и устойчивости критической инфраструктуры в различных секторах, а также постоянное сотрудничество с частными компаниями поставщиками, владельцами коммунальных услуг и операторами электроэнергетического и нефтегазового секторов для укрепления кибербезопасность критической энергетической и иной инфраструктуры от текущих и будущих угроз.

В дополнении к ранее принятым законам штатов по кибербезопасности в декабре 2020 г. в США принят федеральный Закон о повышении кибербезопасности Интернета вещей[20], который регламентирует определение минимальных стандартов безопасности для обменивающихся данными по беспроводным сетям устройств Интернета вещей, принадлежащих или контролируемых федеральным правительством в целях обеспечения режима конфиденциальности и безопасности.

Национальная стратегия кибербезопасности Великобритании на 2016-2021гг.[21] определяет цель правительства сделать Великобританию безопасной и устойчивой к киберугрозам в новых реалиях цифрового мира, включая следующие приоритеты:

- защита от развивающихся киберугроз, эффективного реагирования на инциденты, обеспечения защиты и устойчивости национальных сетей, данных и систем;
- сдерживание всех форм агрессии в киберпространстве и пресечение враждебных действий;
- развитие индустрии кибербезопасности, опирающаяся на ведущие мировые научные исследования и разработки для удовлетворения национальных потребностей в государственном и частном секторах;
- углубление существующих связей с ближайшими международными партнерами для укрепления коллективной безопасности и защитить интересы Великобритании за рубежом, в том числе через ЕС, НАТО и ООН. Стратегия выделяет факторы влияния, и в частности: развитие IT-технологий; вызванная цифровизацией трансформация экономики, управления государством и предоставление основных услуг зависимость от целостности киберпространства, инфраструктуры, систем и данных; уязвимость систем и технологий, лежащих в основе повседневной жизни (умные устройства, электросети, системы управления воздушным движением, спутники, медицинские технологии, промышленные предприятия, подключенные к Интернету); защита от злоумышленников и враждебных атак отдельных лиц, государств или преступных и террористических организации. Все эти факторы определяют кибербезопасность как сферу национального приоритета.

В процессе применения положений Национальной стратегии кибербезопасности, как показало опрос-исследование [7], все британские компании подвержены рискам кибербезопасности, которые растут из года в год, а кибербезопасность имеет высокий приоритет для большинства компаний, включая малый и средний бизнес. Это придает исключительное актуальность фактору оценки и осознания компаниями природы и значимости киберугроз.

3. Инвестиционная и предпринимательская деятельность в ракурсе национальной безопасности

В последние годы основные юрисдикции, включая США, Европейский Союз, Индию, Австралию, Германию, Японию и Великобританию приняли, либо больше расширили сферу действия своих существующих законов, связанных с регулированием иностранных инвестиций на своей территории. Пандемия COVID-19 также значительно усилила озабоченность правительств многих стран, как в сфере экономики, так и в области безопасности .

Стратегия национальной безопасности РФ определила важность развития международных деловых контактов, привлечение иностранных инвестиций и технологий, реализацию совместных проектов, расширение рынков сбыта российской продукции, противодействие попыткам иностранных государств регулировать мировые рынки исходя из их политических и экономических интересов (п.62).

Как показывает практика, современное международное торговое и инвестиционное право получает «санкционную окраску», принципы свободы торговли и автономии воли уступают протекционистской политике под нажимом публично-правовых факторов и политических оценок.

Законотворческая деятельность и бизнес-практика во многих странах свидетельствует о том, что предпринимательская деятельность также стала оцениваться и регулироваться с позиции защиты национальной безопасности страны и соблюдения её национальных интересов.

Важным направлением для экономики России является, как определено в Федеральном законе от 09.07.1999 N 160-ФЗ (ред. от 31.05.2018) «Об иностранных инвестициях в Российской Федерации», привлечение и эффективное использование в экономике

20 The Internet of Things Cybersecurity Improvement Act of 2020. URL: https://www.congress.gov/bill/116th-congress/house-bill/1668/text

21 The UK National Cyber Security Strategy 2016 to 2021. https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

Российской Федерации иностранных материальных и финансовых ресурсов, передовой техники и технологии, управленческого опыта, обеспечение стабильности условий деятельности иностранных инвесторов и соблюдение соответствия правового режима иностранных инвестиций нормам международного права и международной практике инвестиционного сотрудничества. В ст. 4 Закона установлено общее правило, предусматривающее, что правовой режим деятельности иностранных инвесторов не может быть менее благоприятным, чем правовой режим деятельности и использования полученной от инвестиций прибыли, предоставленный российским инвесторам, за изъятиями, устанавливаемыми федеральными законами (*режим наибольшего благоприятствования*). Тем не менее, допускаются изъятия ограничительного характера для иностранных инвесторов, которые могут быть установлены федеральными законами только в той мере, в какой это необходимо в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. Государство также предоставляет гарантии от неблагоприятного изменения для иностранного инвестора и коммерческой организации с иностранными инвестициями российского законодательства. Однако такие гарантии не распространяются на изменения в российском законодательстве, вводимые в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства (ст.9 Закона).

Особое внимание с точки зрения безопасности уделяется стратегически важным предприятиям, формирующим критически важную инфраструктуру страны, особенно в сфере национального топливно-энергетического комплекса. В частности, законодательно установлены требования безопасности объектов топливно-энергетического комплекса и требования антитеррористической защищенности объектов топливно-энергетического комплекса[22]. В соответствии с Федеральным законом от 29.04.2008 N 57-ФЗ (ред. от 31.07.2020) «О порядке осуществления иностранных инвестиций в хозяйственные общества, имеющие стратегическое значение для обеспечения обороны страны и безопасности государства»[23] регламентирован порядок осуществления предварительного согласования Правительственной комиссии по контролю за осуществлением иностранных инвестиций сделок, иных действий, влекущих за собой установление контроля иностранных инвесторов (группы инвесторов) над хозяйственными обществами, имеющими стратегическое значение для обеспечения обороны страны и безопасности государства, а также сделок, предусматривающих приобретение в собственность, владение или пользование имущества, которое относится к основным производственным средствам хозяйственного общества, имеющего стратегическое значение, и стоимость которого составляет более 25% его активов.

К примеру, в США Министерством энергетики утверждена Стратегия кибербезопасности в энергетике (DOE Cybersecurity Strategy) 2018-2020[24], направленная на поддержания системы ядерного сдерживания США, снижения угрозы ядерного распространения, контроля за энергоснабжением страны, противодействия постоянно растущим и сложным киберугрозам, организацию защиты кибербезопасности в масштабах предприятий энергетики.

В конце 2020 г. Парламент Великобритании обсудил законопроект о национальной безопасности и инвестициях[25], который рассматривает национальную безопасность с концептуальной точки зрения, получающую все более широкое определение и выходящую далеко за рамки чисто оборонных интересов, распространяющуюся на сферу иностранных инвестиций и контроля над слияниями и поглощениями с участием иностранных инвесторов в целях защиты национальной безопасности, обеспечивая при этом предприятиям и инвесторам уверенность и прозрачность для ведения бизнеса в Великобритании. Закон предоставит Правительству UK новые беспрецедентные полномочия по расследованию и блокированию корпоративных сделок, которые, по его мнению, могут угрожать безопасности Великобритании, включая китайские инвестиции в АЭС Hinkley Point и участие Huawei в британской сети 5G. Закон определяет сектора, имеющие значение для национальной безопасности, и в частности: современные материалы, продвинутая робототехника и искусственный интеллект, ядерная энергетика и ТЭК, связь и вычислительное оборудование, криптографическая аутентификация, инфраструктура данных и их защита, инженерная биология, военные технологии и технологии двойного назначения, квантовые технологии, спутниковые и космические технологии, транспорт. Предусмотрена оценка проектов с точки зрения потенциальных рисков для национальной безопасности.

КНР проявляет все более активный подход в отношении регулирования национальной безопасности в сфере иностранных инвестиций на основе новой редакции Закона об иностранных инвестициях КНР, который вступил в силу 1 января 2020 года[26]. Законом

22 Федеральный закон от 21.07.2011 N 256-ФЗ (ред. от 24.04.2020) «О безопасности объектов топливно-энергетического комплекса»// СЗ РФ, 25.07.2011, N 30 (ч. 1), ст. 4604; Федеральный закон от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»// СЗ РФ, 31.07.2017, N 31 (Часть I), ст. 4736; «Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации» (утв. Президентом РФ 03.02.2012 N 803);

23 Собрание законодательства РФ, 05.05.2008, N 18, ст. 1940

24 U.S. Department of Energy Cybersecurity Strategy. URL: https://www.energy.gov/national-security-safety/cybersecurity

25 National Security and Investment Bill (11 November 2020). URL: https://www.gov.uk/government/collections/national-security-and-investment-bill

26 Measure for the Security Review of Foreign Investment (Decree No.37 of the National Development and Reform Commission and the Ministry of Commerce) promulgated by the National Development and Reform Commission and the Ministry of Commerce on 19 December 2020. URL: https://www.chinalawinsight.com/2020/12/articles/corporate-ma/ma/china-releases-national-security-review-rules-version-2-0/#_ftnref1

приняты меры в связи с усилением режима правового регулирования и обеспечения национальной безопасности в отношении иностранных инвестиций, которые предприняли все развитые страны. Обнародование мер также является ответом Китая на быстро меняющуюся нормативную базу во всем мире.

Сфера антимонопольного регулирования в ближайшее время также может быть включена в элементы защиты национальных интересов. Примером может служить возбужденное в конце 2020 года Министерством юстиции США и рядом штатов антимонопольное разбирательство против компании Google и глобальной социальной сети Facebook по обвинению этим мировых гигантов в нарушении правил конкуренции и монополизации рынка[27].

Юрисдикционный иммунитет и разрешение споров. В условиях протекционизма и санкционного давления повышается значение международного коммерческого и инвестиционного арбитража, особенно в части разрешения споров государства и иностранными инвесторами в рамках двусторонних международных соглашений о защите инвестиций. Как отмечает Конституционный Суд РФ[28], «международный инвестиционный арбитраж следует отличать от международного коммерческого арбитража, основанного на автономии воли сторон. Предметом рассмотрения в рамках инвестиционного арбитража становятся суверенные действия (бездействие) государства, которые совершаются от его имени всеми – законодательным, исполнительными, судебными – органами власти и которые в отсутствие положения о таком арбитраже в международном договоре рассматривались бы в судах соответствующего государства. Специфические черты такого арбитража, как отмечается в названном определении Конституционного Суда, нашли отражение в международной практике. Например, Суд Европейского союза указывает на отличие инвестиционного арбитража от коммерческого, основанного на соглашении сторон, и на изъятие международным договором соответствующих споров из юрисдикции государственных судов для рассмотрения их инвестиционным арбитражем (заключение Суда Европейского союза от 16 мая 2017 года № 2/15 и решение Большой палаты Суда Европейского союза от 6 марта 2018 года по делу № C-284/16 «Словакия против «Акмеа БВ» (*Slovak Republic v. Achmea BV*). В Докладе Европейского союза и его государств-членов для Рабочей группы III Комиссии ООН по праву международной торговли от 18 января 2019 года отмечается наличие у инвестиционного арбитража черт, сходных с процедурой конституционного или административного судебного контроля. В силу этого наделение международного инвестиционного арбитража полномочиями по разрешению споров и, как следствие, изменение (исключение) компетенции государственных судов не могут быть осуществлены без принятия федеральным парламентом закона о ратификации соответствующего международного договора».

Кроме того, Конституционный Суд РФ также указал (п.5), что «право государства осуществлять судебную юрисдикцию на своей территории в отношении возникающих на ней правовых споров и вытекающая отсюда законодательная прерогатива допускать разрешение такого рода споров в зарубежных и международных юрисдикциях – неотъемлемые составляющие государственного суверенитета, который служит конституционной основой для международного сотрудничества и заключения международных договоров». Это правило распространяется и на разрешение международным арбитражем споров между Российской Федерацией и иностранными инвесторами, возникших в связи с осуществлением ими инвестиций и предпринимательской деятельности на территории Российской.

Кибербезопасность операций с криптовалютами. Исключительно актуальным в настоящее время является направление по формированию механизмов кибербезопасности в связи с расширяющимся по всему миру использованием криптовалют и иных цифровых финансовых активов, цифровых прав. Показательным в этом смысле служит Отчет 2020 года о применении криптовалют специальной группы при генеральном прокуроре США[29], в котором отмечалось, что широкое применение современных технологий распределенного реестра (блокчейн) с гарантиями безопасности и криптографическими механизмами, например, в сфере продовольствия и безопасности пищевых продуктов, в области исследований и экспериментов, экспериментов с потенциальными вариантами использования цифровых валют, а также разработки и тестирования гипотетической цифровой валюты Центрального банка создает привлекательные условия для криптовалюты, которая представляет собой трансформирующий способ хранения и обмена ценности. Однако, несмотря на свое относительно недолгое существование, блокчейн технология уже играет определенную роль во многих наиболее значимых преступлениях и угрозах национальной безопасности. Как установила целевая группа, незаконное использование криптовалюты обычно делится на три категории:

1. финансовые операции, связанные с совершением преступлений;
2. отмывание денег и уклонение от налоговых, отчетных или иных установленных законом правовых требований;
3. преступления, такие как кража, мошенничество, непосредственно связанные с самим рынком криптовалют. Складываются преступные бизнес-модели с использованием криптовалютных биржи (площадок, киосков и казино) и цепочки противоправных действий, которые могут способствовать преступной деятельности.

Тем не менее, многие центробанки мира активно обсуждают введение цифровых валют центральных

27 https://fm.cnbc.com/applications/cnbc.com/resources/editorialfiles/2020/10/20/Complaint.pdf

28 Определение Конституционного Суда РФ от 24 декабря 2020г. № 2867-О-Р.

29 Cryptocurrency Enforcement Framework Report. Report Of The Attorney General's Cyber Digital Task Force. U.S. Department of Justice,2020. URL: https://www.justice.gov/cryptoreport

банков. Центральный Банк Российской Федерации также рассматривает вопрос о возможности выпуска цифрового рубля[30], исходя из того, что в России и в мире расширяется применение цифровых финансовых технологий, в повседневных расчетах все чаще используются безналичные деньги. В этих условиях общество формирует запрос на повышение скорости, удобства и безопасности денежных расчетов с использованием современных технологий. Цифровой рубль - это цифровая форма российской национальной валюты, которую Банк России будет выпускать в дополнение к существующим формам денег (наличным и безналичным рублям). Применение передовых технологий при разработке цифрового рубля будет способствовать снижению издержек на проведение расчетов и повышению финансовой доступности, а также даст толчок дальнейшему совершенствованию платежных технологий. Вместе с тем цифровые активы как объекты правового регулирования уже нашли свое закрепление в ст.141.1 Гражданского кодекса РФ (ст.141.1 ГК РФ) а Федеральный закон от 31.07.2020 N 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» определил особенности инвестирования в цифровые активы.

Комиссия ЕС также обеспокоена созданием своего законодательства в сфере криптовалют[31], применимой к эмитентам криптоактивов и поставщикам услуг криптоактивов в целях обеспечение защиты интересов инвесторов, целостности рынка и финансовой стабильности, путем создания структуры, на основе которой мог бы развиваться более крупный трансграничный рынок криптоактивов и криптоуслуг.

В целом, как отмечает Еврокомиссия[32], современная технологическая революция, обеспечившая поворот к экономике данных и искусственному интеллекту, растущее значение новых технологий, таких как блокчейн, 3D печать и Интернет вещей (IoT), а также развитие новых бизнес-моделей платформенной экономики и экономика открывает уникальное окно возможностей для модернизации подхода к защите цифровых и нематериальных активов, интеллектуальной собственности.

Следует отметить, что имеются и отдельные направления, требующие особой защиты национальной безопасности в сфере интеллектуальной собственности. К примеру, национальные интересы в чрезвычайных обстоятельствам служат основанием для ограничения гражданских прав, в частности - интеллектуальных прав на результаты интеллектуальной деятельности, преодолевая установленную законом правовую монополию исключительных прав. Так, в условиях чрезвычайных событий (эпидемий, эпизоотий, стихийных бедствий и т.п.), а также в интересах обороны и национальной безопасности Правительство РФ вправе разрешить использование изобретения, полезной модели или промышленного образца без согласия патентообладателя с уведомлением его об этом в кратчайший срок и с выплатой ему соразмерной компенсации (ст.1360 ГК РФ).

Выводы

Исследование показало объективные предпосылки для формирования новых самостоятельных элементов системы национальной безопасности Российской Федерации, включая биобезопасность, кибербезопасность, криптобезопасность и инвестиционную безопасность. Эти новые элементы формируют свой самостоятельный предмет и способы обеспечения национальных интересов и национальной безопасности в указанных сферах, имеют свою законодательную базу и особенности правового регулирования, что с несомненной очевидностью определяет необходимость их выделения в самостоятельные структурные элементы национальной безопасности для последующего законодательного регулирования и практического осуществления с точки зрения защиты национальных интересов. Аналогичные выявленным элементам в структуре национальной безопасности находят свое выражение и в законодательстве, правовых системах и правоприменительной практике многих зарубежных стран, что подкрепляет довод об универсальности исследованных в настоящей статье новых составных элементах сферы национальной безопасности и национальных интересов отдельного государства. В целом система национальной безопасности с правовой точки зрения представляет собой систему законодательных и иных правовых актов, обеспечивающих государственный суверенитет страны, права и законные интересы ее граждан в соответствии с конституционно-правовыми положениями Конституции РФ, критически важную структуру страны и антитеррористическую защищенность объектов защиты. Эта система не ограничивается обороной страны и включает другие предусмотренные законом виды безопасности: государственную, общественную, информационную, экологическую, экономическую, транспортную, энергетическую безопасность, безопасность личности. В зависимости от появления новых угроз национальным интересам, новых вызовов внутреннего и внешнего характера могут появляться новые направления деятельности (элементы), защита которых требуют национальные интересы, или видоизменяются уже имеющиеся. Правовое регулирование сферы национальной безопасности должно отвечать требованиям обеспечения устойчивости и стабильности, надежности и отказоустойчивости, эффективности преодоления угроз и рисков, их последствий инцидентов для системы национальной безопасности в каждой конкретной области в соответствии с видом и структурой организации национальной безопасности.

30 Доклад Банка России для общественных консультаций «Цифровой рубль», октябрь 2020. URL: www.cbr.ru

31 Proposal for a Regulation of the European Parliament and the Council on Markets in Crypto-assets and amending Directive (EU) 2019/1937. URL: https://eur-lex.europa.eu/ legal-content/ EN/TXT/ ?uri=CELEX%3A52020PC0593

32 Communication from the Commition to the European Parliament. Making the most of the EU's innovative potential An intellectual property action plan to support the EU's recovery and resilience, Brussels, 25.11.2020 COM(2020) 760.URL:https://ec.europa.eu/docsroom/ documents/ 43845

Литература:

1. Карцхия А.А. Правовое регулирование о возможности современных биотехнологий // Интеллектуальная собственность. Промышленная собственность. 2020. № 8. С. 33-46.
2. Жаворонкова Н.Г., Агафонов В.Б. Теоретико-методологические проблемы правового обеспечения экологической, биосферной и генетической безопасности в системе национальной безопасности Российской Федерации // Lex russica. 2019. № 9. С. 96–108.
3. Романовский Г.Б. Правовое регулирование генетических исследований в России и за рубежом // Lex russica. 2016. № 7. С. 93–102.
4. R. Sabillon, V.Cavaller, J.Cano. National Cyber Security Strategies: Global Trends in Cyberspace International Journal of Computer Science and Software Engineering (IJCSSE), Volume 5, Issue 5, May 2016. P.67-81. www.IJCSSE.org
5. Молчанов Н.А., Матевосова Е.К. Концептуально-политический и формально-юридический анализ Парижского призыва к доверию и безопасности в киберпространстве и российские инициативы в области международного права // Актуальные проблемы российского права. 2020. № 1. С. 133 - 141. DOI: 10.17803/1994-1471.2020.110.1.133-14
6. Štitilis, D., Pakutinskas, P. & Malinauskaitė, I. EU and NATO cybersecurity strategies and national cyber security strategies: a comparative analysis. Secur J 30, 1151–1168 (2017). https://doi.org/10.1057/s41284-016-0083-9
7. R. Klahr, J.Shah, P. Sheriffs, T.Rossington,G. Ipsos . Cyber security breaches survey 2017. Main report. 2017. URL: http://www.ipsos-mori.com/terms

NEW ELEMENTS OF NATIONAL SECURITY: NATIONAL AND INTERNATIONAL ASPECTS

***Kartskhiya A.A.*[33]**

Abstract

The purpose *of the study is to study the legal aspects of the structural development of national security to identify trends and factors that influence the formation of national interests of an individual state and international relations, as well as to study the national security system from a legal standpoint.*

The method of research: *a comparatively legal comparison and analysis of current national Russian and foreign legislation and development strategies, international treaties and agreements on national security issues and their application.*

Result: *The study revealed objective prerequisites for the formation of new independent elements of the Russian Federation's national security system, including biosecurity, cybersecurity, cryptosecurity and investment security. These new elements form their own subjects and ways of ensuring national interests and national security in these areas, have their own legislative framework and legal regulation, which clearly determines the need to allocate them into independent structural elements of national security for further legislative regulation and practical implementation in terms of protecting national interests.*

Keywords: *sovereignty, constitutional rights, international agreements, foreign investment, digital rights, biosecurity, cybersecurity, cryptosecurity.*

References

1. Kartchiia A.A. Pravovoe regulirovanie o vozmozhnosti sovremenny`kh biotekhnologii` // Intellektual`naia sobstvennost`. Promy`shlennaia sobstvennost`. 2020. № 8. S. 33-46.
2. Zhavoronkova N.G., Agafonov V.B. Teoretiko-metodologicheskie problemy` pravovogo obespecheniia e`kologicheskoi`, biosfernoi` i geneticheskoi` bezopasnosti v sisteme natcional`noi` bezopasnosti Rossii`skoi` Federatcii // Lex russica. 2019. № 9. S. 96–108.
3. Romanovskii` G.B. Pravovoe regulirovanie geneticheskikh issledovanii` v Rossii i za rubezhom // Lex russica. 2016. № 7. S. 93–102.

33 Alexander Kartskhiya, Dr.Sc. (in Law), Associate Professor, Department of Civil and Legal Sciences of the Russian State University and Petroleum (National Research University) named after I.M. Gubkin, Moscow, Russia. E-mail: arhz50@mail.ru

4. R. Sabillon, V.Cavaller, J.Cano. National Cyber Security Strategies: Global Trends in Cyberspace International Journal of Computer Science and Software Engineering (IJCSSE), Volume 5, Issue 5, May 2016. R.67-81. www.IJCSSE.org
5. Molchanov N.A., Matevosova E.K. Kontceptual`no-politicheskii` i formal`no-iuridicheskii` analiz Parizhskogo prizy`va k doveriiu i bezopasnosti v kiberprostranstve i rossii`skie initciativy` v oblasti mezhdunarodnogo prava // Aktual`ny`e problemy` rossii`skogo prava. 2020. № 1. S. 133 - 141. DOI: 10.17803/1994-1471.2020.110.1.133-14
6. Štitilis, D., Pakutinskas, P. & Malinauskaitė, I. EU and NATO cybersecurity strategies and national cyber security strategies: a comparative analysis. Secur J 30, 1151–1168 (2017). https://doi.org/10.1057/s41284-016-0083-9
7. R. Klahr, J.Shah, P. Sheriffs, T.Rossington,G. Ipsos . Cyber security breaches survey 2017. Main report. 2017. URL: http://www.ipsos-mori.com/terms