Федеральное государственное автономное образовательное
учреждение высшего образования
«Национальный исследовательский университет
«Высшая школа экономики»

На правах рукописи

Туробов Алексей Владимирович

ТРАНСФОРМАЦИИ СФЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПОД ВЛИЯНИЕМ ТЕХНОЛОГИЙ ЦИФРОВИЗАЦИИ И АВТОМАТИЗАЦИИ В ИННОВАЦИОННЫХ СТРАНАХ

РЕЗЮМЕ ДИССЕРТАЦИИ
на соискание ученой степени
кандидата политических наук

Научный руководитель:
кандидат политических наук, доцент
Михаил Григорьевич Миронюк

Москва – 2022

Актуальность исследования

Цифровизации в последнее время уделяется большое внимание как со стороны представителей государств, так и со стороны международных организаций. Согласно различным исследованиям, эффективная цифровая адаптация играет ключевую роль в достижении роста доходов и повышении удовлетворенности пользователей[1], то есть граждан. Цифровые технологии могут принести пользу обществу, облегчая доступ к государственным услугам, более высокие занятость и темпы экономического роста, что в конечном итоге может способствовать повышению уровня благополучия граждан[2]. Цифровизация, управляемая государством, дополняет и компенсирует традиционные и формальные механизмы взаимодействия граждан и правительства, создавая дополнительные (и (или) дополняющие традиционные институты) онлайн-институты. Более того, успешная цифровизация значительно изменила отношения между государством и обществом, повысив частоту и качество взаимодействий между гражданами и правительством[3].

Указанные процессы меняют структуру и содержание государственной политики и государственного управления[4]. Феномен цифровизации комплексный. С одной стороны, такие термины, как оцифровка (загрузка форм в Интернете), цифровизация (заполнение форм в Интернете) и цифровая трансформация (предоставление полного обслуживания в режиме онлайн), используются в литературе как взаимозаменяемые и часто сосредоточены только на первых двух функциях[5]. С другой – в основе непосредственно цифровизации лежит взаимосвязь различных типов цифровых технологий, а также система трех элементов: инфраструктура/архитектура, программное обеспечение взаимодействия технологий и пользователя, а также пользователей друг с другом посредством цифровых технологий.

---

[1] Dong Q. J. Moving a Mountain with a Teaspoon: Toward a Theory of Digital Entrepreneurship in the Regulatory Environment // Technological Forecasting and Social Change. — 2019. — Sept. — Vol. 146. — P. 923– 930.

[2] Galindo-Martin M.-A., Castano-Martinez M.-S., Mendez-Picazo M.-T. Digital Transformation, Digital Dividends and Entrepreneurship: A Quantitative Analysis // Journal of Business Research. — 2019. — Vol. 101(C), no. 146. — P. 522–527.

[3] Wong, Chu. Digital Governance as Institutional Adaptation and Development: Social Media Strategies between Hong Kong and Shenzhen // China Review. — 2020. — Aug. — Vol. 20, no. 3. — P. 43–70.

[4] Bretschneider, Mergel. Technology and Public Management Information Systems : Where we have been and where we are going // The state of public administration : issues, challenges, and opportunities. — 1st ed. — London:Routledge Taylor Francis Group, 2015. — P. 187–203.

[5] Mergel, Edelmann, Haug. Defining digital transformation: Results from expert interviews // Government Information Quarterly. — 2019. — Oct. — Vol. 36, no. 4. — P. 101385.

Для целей данного исследования применяется концептуализация, предложенная Мергелем, Эдельманном и Хаугом[6], сфокусированная на концепте цифровизации:

- оцифровка – переход от аналоговых к цифровым услугам с изменением «один к одному» в «доставке» контента/информации и с добавлением технологического канала связи;
- цифровизация – сосредоточение внимания на потенциальных изменениях в процессах (как социальных, экономических, так и политических), помимо простой оцифровки существующих процессов и форм;
- цифровая трансформация - полная реализация процессов в цифровой среде с учетом культурных, социальных и организационных особенностей с применением целостного подхода и получением различных результатов.

Цифровизация охватывает не только технологические достижения, но и институциональные изменения, такие как надежное соединение и стандарты качества, сеть Интернет и безопасность данных, финансовые и правовые основы, а также научный, инновационный и человеческий капитал[7]. Важно, что цифровизация представляется нами, в первую очередь, как политический процесс, а не сугубо технологический.

Несмотря на высокую степень внедрения цифровых технологий в ряде стран, само по себе их применение автоматически не приводит к повышению участия гражданского общества в политических процессах и не обеспечивает надлежащего качества государственного управления (см., например, исследование о потенциале влияния ИКТ, Интернета и электронного правительства на транспарентность правительств[8]; исследование о негативном влиянии использования Интернета на политическую вовлеченность[9]; исследование о политическом участии и «не успехах» теле-демократии

[6] Там же. С.12

[7] Конкретные типы технологий, как и концепция цифровизации во взаимосвязи типов цифровых технологий с достижением конкретных целей на примере сферы образования см. Антонова А., Туробов А. Мишени цифровых технологии через призму образования // Образовательная политика. — 2020. — т. 82, No 2. — с. 42— 55.

[8] Bertot J. C., Jaeger P. T., Grimes J. M. Using ICTs to create a culture of transparency: E-government and social media as openness and anticorruption tools for societies // Government Information Quarterly. — 2010. — Vol. 27, no. 3. — P. 264–271.

[9] Boulianne S. Does internet use affect engagement?: A meta-analysis of research // Political Communication. — 2009. — Vol. 26, no. 2. — P. 193– 211.

и исследование об увеличении политического участия посредством технологий, которые не приносят результата в краткосрочной перспективе[10], и пр.).

Цифровые технологии вызывают изменения и в сфере обеспечения безопасности. Цифровизация и стремительное развитие ИКТ привели к появлению новых, изобретательных и агрессивных способов мониторинга, прогнозирования и/или нейтрализации потенциальных угроз безопасности[11]. Эти «новые» практики и процессы обеспечения безопасности (например, широкое применение биометрии[12], наблюдения (surveillance)[13], дронов и целевых убийств[14], алгоритмической безопасности[15]) открыли теоретические и эмпирические возможности, а также поставили ряд новых проблем.

Одной из основных функций современного государства, причем вне зависимости от типа политического режима, остается обеспечение безопасности граждан (определенных групп граждан) и самого себя в целом. Качество реализации такой функции влияет на восприятие гражданами легитимности правительства, политических институтов и акторов. Обеспечение безопасности влияет на эффективность государства как внутри его границ, так и за их пределами. Сфера обеспечения безопасности расширяется и наполняется новыми элементами, такими как кибербезопасность, безопасность компьютерных сетей, информационная безопасность и т.д. Соответственно, за счет использования цифровых технологий увеличивается арсенал средств обеспечения безопасности.

Современные исследования сферы обеспечения безопасности фокусируются на трех феноменах: источники интересов акторов, выработка национальных коллективных целей и способность государства к действию (capacity for action)[16]. По мере роста сложности и совершенства цифровых технологий взаимосвязь и взаимозависимость

[10] Arterton F. C. Political Participation and «Teledemocracy» // PS: Political Science Politics. — 1988. — Vol. 21, no. 3. — P. 620–627. Его же. Teledemocracy: Can Technology Protect Democracy? — Newbury Park, CA.: SAGE Publications Ltd, 1987. — 222 p.
[11] Hendershot C., Mutimer D. Critical Security Studies // The Oxford Handbook of International Security. — Oxford University Press, 2018. — P. 1– 13.
[12] Muller B. Securing the Political Imagination: Popular Culture, the Security Dispositive and the Biometric State // Security Dialogue. — 2008. — Vol. 39, no. 2/3. — P. 199–220.
[13] Bell C. Surveillance Strategies and Populations at Risk: Biopolitical Governance in Canada's National Security Policy // Security Dialogue. — 2006. — Vol. 37, no. 2. — P. 147–6
[14] Grayson K. Cultural Politics of Targeted Killing: On Drones, Counter-Insurgency, and Violence. — New York: Routledge, 2016. — 230 p.
[15] Amoore L., Raley R. Securing with Algorithms: Knowledge, Decision, Sovereignty // Security Dialogue. — 2017. — Vol. 48, no. 1. — P. 3– 10.
[16] Krebs R. The Politics of National Security // The Oxford Handbook of International Security. — Oxford University Press, 2018. — P. 259–273:2

технических, информационных и цифровых направлений со сферой безопасности увеличивается.

Безопасность в политической науке рассматривается на различных уровнях, в том числе как на уровне самой политической системы (политическое выживание на всех уровнях: режима, институтов, акторов), так и на уровне общества (граждан, отдельных социальных сфер и пр.). Цифровые технологии на каждом уровне выступают и в качестве инструментов, укрепляющих и обеспечивающих, и как то, что создает пространство (цифровое пространство), где также необходимо обеспечивать безопасность.

Роль цифровых технологий в политике характеризуется двойственностью. С одной стороны, цифровые технологии служат инструментом изменения структуры ролей и обязанностей граждан и позволяют решить некоторые проблемы современных государств, такие как снижение электорального участия, увеличение дистанции между политической системой и населением, рост недоверия к традиционным политическим институтам[17]. Теоретически цифровая трансформация политической сферы соответствует идеалам прямой демократии и ориентирована на передачу власти от традиционных институтов и элит группам людей, и коллективные действия (при помощи технологических инструментов) направлены на демократизацию процессов управления. Указанная трансформация переходит на институциональный уровень - электронное голосование, электронное правительство.

С другой стороны, политические институты устанавливают «правила» индивидуального и коллективного поведения, передачи информации и социального выбора[18] и могут ускорить или замедлить социально-политические изменения[19]. Уровень технологического развития страны также влияет на степень и качество использования цифровых технологий в политической сфере, однако политическая институционализация усиливает эффективность такого применения[20]. Применительно к сфере национальной безопасности это означает, что *трансформациям под влиянием технологий цифровизации и автоматизации подвергаются институты и акторы*,

[17] Susha I., Gronlund A. Context clues for the stall of the Citizens' Initiative: Lessons for opening up e-participation development practice // Government Information Quarterly. — 2014. — Vol. 31, no. 3. — P. 454–465.
[18] Plott C. R. The application of laboratory experimental methods to public choice // Collective decision making: Applications from public choice theory. — Johns Hopkins University Press, 1979. — P. 137–160:156
[19] Jackman R. W., Miller R. A. Voter turnout in the industrial democracies during the 1980s // Comparative Political Studies. — 1995. — Vol. 27. — P. 467–492.
[20] Jho W., Song K. J. Institutional and technological determinants of civil e-Participation: Solo or duet? // Government Information Quarterly. — 2015. — Vol. 32, no. 4. — P. 488–495.

обеспечивающие безопасность, определяющие степень опасности конкретных угроз и меры противодействия им, а также *институты контроля и надзора* за институтами и акторами, обеспечивающими безопасность.

Масштабное внедрение инновационных цифровых подходов и технологий при отсутствии или недоступности публичных научно-обоснованных анализа и оценок рисков, вызовов, выгод и угроз цифровизации в сфере обеспечения безопасности определяют состояние и повестку академических дискуссий, а также формируют неопределенность в практической реализации политик в области безопасности. Критическое осмысление и оценка альтернатив, основанная на фактических данных, - масштабная и актуальная задача для формирования соразмерной, эффективной, основанной на доказательствах (evidence-based) и сбалансированной политики в области обеспечения безопасности.

Степень разработанности темы исследования

Ускоренное развитие цифровых технологий и их внедрение в различные сферы жизни современного общества влечет за собой фундаментальные изменения не только технологического и экономического характера, но и в сфере политики и управления. Изменения в области коммуникации, сбора и использования информации, цифрового взаимодействия государства с обществом привели к появлению новых концепций управления и политики: теледемократия[21], электронная демократия[2223], виртуальная демократия[24], электронное правительство[252627], GovTech и Algorithmic Government[28] и т.д. Эти концепции развивались в течение некоторого времени. Однако, академическое сообщество и политические деятели оказались не готовы к быстрому развитию

[21] Arterton F. C. Political Participation and «Teledemocracy» // PS: Political Science Politics. — 1988. — Vol. 21, no. 3. — P. 620–627. Его же. Teledemocracy: Can Technology Protect Democracy? — Newbury Park, CA. : SAGE Publications Ltd, 1987. — 222 p.
[22] Watson R. T., Mundy B. A strategic perspective of electronic democracy // Communications of the ACM. — 2001. — Vol. 44, no. 1. — P. 27–30.
[23] Carrizales T. Critical Factors in an Electronic Democracy: a Study of Municipal Managers // Electronic Journal of E-Government. — 2008. — Vol. 6, no. 1. — P. 23–30.
[24] Norris P. Virtual democracy // Harvard International Journal of Press/Politics. — 1998. — Vol. 3, no. 2. — P. 1–4.
[25] Brown D. Electronic government and public administration // International Review of Administrative Sciences. — 2005. — Vol. 71, no. 2. — P. 241– 254.
[26] Manoharan A., Carrizales T. J. Technological equity: An international perspective of e-government and societal divides // Electronic Government. — 2011. — Vol. 50, no. 1. — P. 56–66.
[27] Rose J., Flak L. S., Saebo O. Stakeholder theory for the E-government context: Framing a value-oriented normative core // Government Information Quarterly. — 2018. — Vol. 35, no. 3. — P. 362–374.
[28] Engin Z., Treleaven P. Algorithmic Government: Automating Public Services and Supporting Civil Servants in using Data Science Technologies // The Computer Journal. — 2019. — Vol. 62, no. 3. — P. 448–460.

современных цифровых технологий (например, сложные математические и статистические алгоритмы - машинное обучение, нейронные сети, искусственный интеллект; технология блокчейна; технология связи 5G; большие данные и т. д.).

Распространение цифровых технологий в политической жизни является хотя и относительно недавним, но признанным объектом исследования. Например, исследования глобальных политических коммуникаций и глобального политического управления[29], влияния цифрового разрыва на политическое участие[30], влияния использования Интернета и онлайн-деятельности на политическое участие[31], влияния информационных и цифровых технологий на электоральное поведение[32]; исследования институциональных и неинституциональных форм политического участия с применением информационных и цифровых технологий[33], «цифровых аборигенов» и «сетевого поколения»[34], негативного влияния Интернета и онлайн среды на политическую вовлеченность[35], электронного участия[36], электронного правительства[37] и пр.

Отдельный аспект касается феноменов «автоматизации» и «алгоритмизации». Данное исследование стремится выйти за рамки рассмотрения автоматизации как исключительно технологического процесса. Фокус нацелен на автоматизацию политики и государственного управления, где цифровые технологии выступают в качестве инструментов. Указанное возможно при формировании понимания автоматизации как более эффективного использования возможностей цифровизации за счет увеличения как скорости, так и масштабов внедрения цифровых технологий в политическую практику с целью изменения процессов (автоматизации) простых решений и повторяющихся когнитивных процессов, что сопровождается высвобождением времени сотрудников

[29] Castells. The new public sphere: Global civil society, communication networks, and global governance // The Annals of the American Academy of Political and Social Science. — 2008. — Vol. 616, no. 1. — P. 78–93.
[30] Sylvester D., McGlynn A. The digital divide, political participation, and place // Social Science Computer Review. — 2010. — Vol. 28, no. 1. — P. 64–74.
[31] Quintelier E., Vissers S. The effect of Internet use on political participation: An analysis of survey results for 16-year-olds in Belgium // Social Science Computer Review. — 2008. — Vol. 26, no. 4. — P. 411–427.
[32] Tolbert C., McNeal R. Unraveling the effects of the Internet on political participation? // Political Research Quarterly. — 2003. — Vol. 56, no. 2. — P. 175–185.c
[33] Hooghe M., Marien S., Quintelier E. Inequalities in non-institutionalized forms of political participation: A multi-level analysis of 25 countries // Political Studies. — 2010. — Vol. 58, no. 1. — P. 87–213.
[34] Bennett S., Maton K., Kervin L. The digital natives debate: A critical review of the evidence // British Journal of Educational Technology. — 2008. — Vol. 39, no. 5. — P. 775–786.
[35] Boulianne S. Does internet use affect engagement?: A meta-analysis of research // Political Communication. — 2009. — Vol. 26, no. 2. — P. 193– 211.
[36] Saebo O., Rose J., Skiftenes Flak L. The shape of e-Participation: Characterizing an emerging research area // Government Information Quarterly. — 2008. — Vol. 25, no. 3. — P. 400–428.
[37] Nam T., Pardo T., Burke G. e-Government interoperability: Interaction of policy, management, and technology dimensions // Social Science Computer Review. — 2012. — Vol. 30, no. 1. — P. 7–23.

для того, чтобы они могли сосредоточиться на задачах, больше соответствующих их набору навыков[38]. В контексте данного исследования значимость имеет еще и тот факт, что цифровые технологии (в частности, технологии искусственного интеллекта) признаются как один из ключевых элементов автоматизации непосредственно в вопросах безопасности[39].

Аналогично, как и с автоматизацией, концептуализация алгоритмизации опирается на социально-технологическую перспективу, а не ограничивается исключительно технологическим процессом. Под алгоритмизацией понимается процесс, в котором организация/институт перестраивает свои рабочие процедуры вокруг использования алгоритмов для принятия решений и совершения соответствующих действий[40]. При этом «реорганизация» процедур происходит при помощи применения алгоритмических систем разной сложности (в т.ч. и с применением технологии искусственного интеллекта). Основной фокус для целей данного исследования делается именно на реорганизации рабочих процессов при помощи использования алгоритмов.

Эволюционное развитие сферы обеспечении безопасности, с одной стороны, и стремительная вовлеченность цифровых технологий (и как следствие – изменения) – с другой, формулируют ***первый уровень проблематизации данного исследования***. На теоретическом уровне проблематизации, мы стремимся заполнить пробелы в академическом знании, связанные с общим контекстом изменений в сфере обеспечения безопасности под влиянием цифровых технологий. Результаты исследований указывают на определенные изменения (а также фиксируют обеспокоенность и неопределенность, связанную с такими изменениями) в сфере безопасности под влиянием цифровых технологий. Однако мало исследований фокусируются на рассмотрении того, **как** именно технологии проникают в сферу обеспечения безопасности, а также **какие** изменения происходят в самой системе обеспечения безопасности государства. Исследования безопасности (security studies) оперируют концепциями угроз и ресурсов/возможностей ликвидации/купирования/преодоления угроз. В данном ключе цифровые технологии могут выступать и в качестве угроз безопасности, и в качестве

[38] Germundsson N. Promoting the digital future: the construction of digital automation in Swedish policy discourse on social assistance // Critical Policy Studies. — 2022. — P. 1–19:9
[39] Sari O., Celik S. Legal evaluation of the attacks caused by artificial intelligence-based lethal weapon systems within the context of Rome statute // Computer Law Security Review. — 2021. — Vol. 42. — P. 105564.
[40] Meijer A., Lorenz L., Wessels M. Algorithmization of Bureaucratic Organizations: Using a Practice Lens to Study How Context Shapes Predictive Policing Systems // Public Administration Review. — 2021. — Vol. 81. — Iss. 5. — P. 837–846:838

инструментов обеспечения безопасности. Возникают вопросы: как государства определяют и воспринимают угрозы в сфере обеспечения безопасности, связанные с цифровыми технологиями? Как государства используют цифровые технологии в качестве инструментов для обеспечения безопасности? Какова динамика применения цифровых технологий?

Пейн[41], проводя параллели между технологией искусственного интеллекта (усложненные алгоритмы прогнозирования и анализа данных) и ядерным оружием, указывает на значительную стратегическую и научную неопределенность в отношении последствий применения данной технологии в военном деле. Происходящие изменения военной деятельности требуют новых стратегических решений: «... Быстрое развитие ИИ, который стремится оптимизировать человеческие цели, *начинает трансформировать* военную деятельность и требует нового стратегического мышления»[42].

Соответственно, на теоретическом уровне, *данное исследование направлено на решение конкретной проблемы – предложить обоснованное понимание (и иллюстрацию динамики) проникновения цифровых технологий в сферу обеспечения безопасности*.

В свою очередь, ***второй уровень проблематизации лежит в инструментальной (методологической) плоскости***. Практически отсутствует понимание того, какой аналитический инструментарий (метод/подход) позволяет проследить такие изменения с возможностью оценки последствий для системы безопасности. Безусловно, экспертные интервью предоставляют некоторую «почву» для исследований, однако попытки «объективного» взгляда на систему безопасности посредством количественной методологии весьма редки. Не преуменьшая значение экспертного знания, мы стремимся его дополнить более верифицируемыми свидетельствами.

Данное исследование стремится предоставить свидетельства того, **как** формируется динамика изменений в сфере обеспечения безопасности при помощи конструирования эмпирической модели изменений и оценки системы безопасности государства под влиянием цифровых технологий (на примере конкретного типа цифровых технологий).

Разработанная эмпирическая модель имеет оценочный характер и направлена на формирование концепции оценки системы безопасности (не только оценка угроз, но и

[41] Payne K. Artificial intelligence: A revolution in strategic affairs? // Survival. — 2018. — Vol. 60. — P. 7–32.
[42] Там же. С. 30 - «...the rapid advances of AI that seeks to optimise human goals is beginning to transform military activity, and demands new strategic thought»

выявление возможностей) и создание эмпирического подхода к измерению такой концепции сферы обеспечения безопасности государства. Таким образом, на теоретическом уровне работа вносит вклад в предметное направление исследований процесса изменений в сфере обеспечения безопасности под влиянием цифровых технологий, а на методологическом – предлагает подход к измерению таких изменений при помощи эмпирической модели.

В основе данного исследования следующее положение: мы рассматриваем цифровые технологии в сфере обеспечения безопасности как (1) инструменты, применяемые для обеспечения безопасности, и как (2) угрозы, определяемые на страновом (национальная безопасность) и международном (международная и глобальная безопасность) уровнях. В данной работе фокус исследования направлен на национальную безопасность страны.

Исследовательский вопрос

Какова динамика применения цифровых технологий правительствами разных стран в сфере обеспечения национальной безопасности?

Исследовательский вопрос подчинен структурной логике исследования. Трансформация как широкое понятие раскрывается посредством существенных изменений и преобразований в политике на теоретическом уровне (Глава 1). Непосредственно эмпирическая часть (Глава 2) сужает рамку до изменений и непосредственных преобразований в сфере безопасности. Исследовательский вопрос направлен на получение содержательных результатов эмпирической части, а именно выявление динамики изменений в сфере обеспечения национальной безопасности. Выявление такой динамики и ее содержательная интерпретация (с опорой как на теоретическую часть, так и на собранные данные) позволит проиллюстрировать и объяснить отдельные элементы трансформации (преобразования и последствия таких изменений).

Дополнительный исследовательский вопрос:

В чем состоят различия и сходства применения цифровых технологий в сфере обеспечения безопасности разных стран?

Ответ на дополнительный исследовательский вопрос позволит наполнить конкретным содержанием выявленные изменения, оказать конкретные содержательные сходства и различия между странами в процессе изменений в национальной безопасности. Таким образом, результаты представят не только фактические

преобразования, но и дополнят фактологию качественным наполнением – демонстрацией практик.

Основной исследовательский вопрос направлен на выявление непосредственной динамики изменений при помощи разработанной эмпирической модели. Дополнительный – на выявление лучших практик (best practices) посредством сравнения моделей различных стран (непосредственно отобранных стран-кейсов).

Цель и задачи исследования

Целью исследования является выявление особенностей применения технологий цифровизации как элемента (фактора) трансформации сферы обеспечения безопасности.

Задачи исследования:

1. Концептуализировать и операционализировать цифровизацию и автоматизацию в сфере обеспечения безопасности;
2. Эмпирически выявить ключевые типы цифровых технологий в концепции цифровизации и перечень стран-лидеров цифровой трансформации;
3. Создать эмпирическую модель для оценки процесса применения цифровых технологий (на примере ключевого типа цифровых технологий) в сфере обеспечения безопасности (на примере выявленных стран);
4. Осуществить сравнительный анализ изменений моделей стран в сфере обеспечения безопасности под влиянием технологий цифровизации;
5. Оценить последствия (риски и выгоды) внедрения технологий цифровизации и автоматизации для государств в сфере национальной безопасности (*дополнительная задача*).

Гипотезы исследования

Исходя из целей и задач исследования, нами сформулированы два набора гипотез.

Первый набор гипотез формулируется относительно моделирования процесса применения цифровых технологий в сфере обеспечения безопасности. Исходя из логики эмпирической модели (соотношения показателя оценки угроз и цифровых возможностей реакции на угрозы), можно предположить, что в моделях стран показатель угроз будет превышать показатель возможностей. Обоснованием служит специфичность цифровых технологий, неоднозначность их применения и стремительность развития. Анализ и оценивание угроз от цифровых технологий (и

анализ и оценивание «традиционных» угроз при помощи цифровых технологий) будет *опережать* имеющиеся решения по противодействию угрозам. Тестирование гипотезы позволит выявить «отношение» правительств к изменениям в сфере безопасности, опосредованным цифровыми технологиями. Объяснительный механизм позволит представить, как государства определяют роль и место технологий (оценка угроз позволит продемонстрировать опасения государств, а потенциал возможностей – то, как государства способны реагировать на угрозы). В случае подтверждения гипотезы мы можем утверждать, что наблюдаем увеличение опасений в вопросах безопасности, т.к. правительства больше внимания обращают на потенциал угроз (как непосредственно со стороны цифровых технологий, так и в вопросах, где технологии должны служить инструментом купирования угроз). В случае опровержения гипотезы, наоборот, правительства успешно интегрируют технологии, сбалансированно оценивая угрозы. В таком случае мы буквально демонстрируем, что государства адаптировались к современным изменениям и сконструировали систему безопасности таким образом, что возможности реагирования превосходят оцениваемые угрозы. Более конкретно, гипотеза сформулирована следующим образом:

H1: *Оценка угроз будет превосходить возможности реагирования на угрозы*

Временной охват эмпирической модели позволяет формулировать гипотезы в терминах динамики изменений. Организационный принцип современных сил обеспечения безопасности (вооруженных сил, правоохранительных органов, специальных служб и пр.) выражается в «максимизации военной мощи за счет использования технологий»[43]. Соответственно, логично предположить, что применение государствами цифровых технологий в сфере обеспечения безопасности будет иметь место *раньше*, чем в обществе начнется содержательная дискуссия об этих типах цифровых технологий. Правительства, если они действительно стремятся к максимизации возможностей, должны начинать принимать политические решения и внедрять технологии быстрее и раньше, чем общество будет включено в указанную дискуссию. Основная публичная дискуссия о применении технологии искусственного интеллекта в сфере обеспечения безопасности началась примерно с 2010 г. в форме обсуждения опасений, связанных с «гонкой вооружений в области искусственного

[43] Farrell T. Constructivist Security Studies: Portrait of a Research Program // International Studies Review. — 2002. — Vol. 4, no. 1. — P. 49– 72:67

интеллекта»[44]. Проверка гипотезы предоставит не только понимание динамики, но и позволит оценить «включенность» правительств в потенциал технологического изменения системы безопасности. Иными словами, мы можем выявить то, насколько проактивно действуют правительства: насколько государство стремится вовлекать и применять технологии (учитывая длительность технологического цикла с момента принятия решений до непосредственной практической реализации) с опережающими темпами до того, как общество обратит внимание на существенные риски и возможности внедрения цифровых технологий. В случае подтверждения гипотезы мы можем утверждать, что государства действительно стремятся к максимизации мощи и безопасности за счет технологий. То есть, наблюдаемые изменения (и, шире, трансформация) должны быть поддержаны и даже инициированы правительствами. Однако, если гипотеза будет опровергнута, может существовать несколько объяснительных механизмов. Основной механизм будет заключаться в том, что государства опасаются угроз и рисков сильнее, чем видят потенциал для применения технологий. Поэтому власти будут стремиться сначала получить доказательную базу условных выгод, а лишь потом начинать внедрять и применять технологии. Альтернативным объяснением может служить перераспределение фокуса правительства, т.е. максимизация может и происходит, но за счет других технологий или за счет иных стратегий и тактик. Таким образом, вторая гипотеза исследования сформулирована следующим образом:

> **H2**: *Динамика применения цифровых технологий в сфере обеспечения безопасности проявиться в промежуток 2008-2010 гг.*

Второй набор гипотез формулируется относительно сравнительного анализа моделей стран. В исследованиях безопасности присутствует консенсус относительно того, что разные государства (правительства) не оценивают угрозы одинаково. Одна и та же угроза может по-разному оцениваться и интерпретироваться государствами[45]. Несмотря на то, что основная работа по данной тематике (исследование Уолферса) относится к «традиционным» подходам к безопасности и может считаться «устаревшей», вопрос неопределенности угроз является весьма актуальным. Несмотря на существующие дискуссии о правильном и должном понимании безопасности,

[44] Artificial Intelligence arms race. Например, см. статью на популярном ресурсе Википедия https://en.wikipedia.org/wiki/Artificial_intelligence_arms_race (дата доступа: 11.09.2021)
[45] Wolfers A. «National Security» as an Ambiguous Symbol // Political Science Quarterly. — 1952. — Vol. 67, no. 4. — P. 481–502:151

восприятие угроз (и его содержание) - и научная, и практическая проблема. Иными словами, в данной гипотезе мы опираемся на содержательную составляющую довода о том, что государства по-разному определяют и оценивают угрозы. Эмпирическая модель данного исследования позволяет анализировать оценку и восприятие угроз каждым государством отдельно и оценить такое восприятие. Однако, несмотря на различия в оценке угроз, вокруг цифровых технологий существует неопределенность в сфере обеспечения безопасности, что формирует излишние опасения. Поэтому мы предполагаем, что в анализируемых странах оценки угроз будут однородными, и этим оценкам будут присущи повышенные опасения. Тестируя данную гипотезу, мы стремимся выявить существование неопределенности в оценке угроз, усложненную спецификой цифровых технологий. С одной стороны, выявление различий в оценке угроз подтвердит эмпирически существующее теоретическое предположение о различиях среди государств в оценке и восприятии угроз. С другой – мы сможем продемонстрировать, существует ли специфика в отношении к цифровым технологиям. В случае подтверждения гипотезы мы опровергнем теоретическое представление о неопределенности в оценке угроз и при этом продемонстрируем уникальное отношение государств к технологии. Указанное значительно расширит дискуссию о трансформационном эффекте технологий. Если же гипотеза будет опровергнута, мы подтвердим существующую теорию о неопределенности оценки угроз, а также продемонстрируем, что отношение правительств к цифровым технологиям не отличается от каких-либо других инструментов, феноменов и пр. Более конкретно, третья гипотеза формулируется следующим образом:

H3: *Восприятие угроз и тип угроз будет достигать максимальных значений во всех анализируемых странах*.

В свою очередь сравнительный анализ также позволит протестировать предположение о высокой готовности государств к рискам и вызовам со стороны цифровых технологий. Мы предполагаем, что к 2018-2019 гг. во всех анализируемых странах, как лидерах в сфере информационных технологий, будут наблюдаться высокие значения показателей эмпирической модели, что будет свидетельствовать о том, что государства (1) высоко оценивают риски и угрозы со стороны цифровых технологий, а также (2) стремительно внедряют цифровые технологии в сферу обеспечения безопасности для противодействия современным вызовам. При тестировании гипотезы мы сможем утверждать не просто о существовании преобразований (и, более широко, трансформации), но и выясним направления таких изменений. Стремительность

внедрения технологий, а также высокая оценка рисков и вызовов продемонстрируют адаптивность и готовность правительств к современным вызовам безопасности, сопряженным с цифровизацией. Более конкретно, четвертая гипотеза сформулирована следующим образом:

> **H4**: *К 2018-2019 гг. показатели эмпирической модели всех анализируемых стран будут приближаться к максимальным значениям, что свидетельствует о высокой готовности государств к рискам и вызовам со стороны цифровых технологий*.

Теоретико-методологические основания и границы исследования

На теоретико-методологическом уровне данное исследование сталкивается с двумя вызовами. Во-первых, распространено мнение, что исследования безопасности возможны сугубо в рамках предметного поля международных исследований. Во-вторых, конструирование единой исследовательской программы для данного исследования будет сталкиваться с дискуссией о возможности реализации количественного эмпирического исследования в теоретической логике Копенгагенской школы исследования безопасности, где подавляющее большинство исследований имеют качественный характер.

Первый вызов можно парировать программной статьей Рональда Кребса о необходимости возвращения политики (и политической науки) в исследования национальной безопасности (возвращение политики в изучение национальной безопасности)[46]. Кребс утверждает, что не все предпочтения в области безопасности в равной степени учитываются в определении «национальных интересов», поскольку политические институты по-разному наделяют акторов полномочиями и направляют агрегацию предпочтений[47]. Политические институты также влияют на то, какие ресурсы доступны лицам, принимающим решения, и какие инструменты политики они считают привлекательными. Лидеры тяготеют к тем инструментам политики, над которыми имеют больший контроль, что объясняет многие решения в области безопасности.

Политика безопасности (security policy) является *политической* на двух уровнях. Первый — это вопросы незащищенности (insecurity), которые обязательно являются

[46] Krebs R. The Politics of National Security // The Oxford Handbook of International Security. — Oxford University Press, 2018. — P. 259–273:2 - «...bringing politics back into the study of national security...»
[47] Там же.

продуктом политических действий[48], так как ни безопасность, ни незащищенность не являются «естественным» положением вещей. Политические акторы продвигают дискурсы безопасности или незащищенности и подпитывают соответствующие общественные эмоции с помощью риторических «речевых актов» (утверждая уязвимость, обещая безопасность) и тем самым формируют политический ландшафт[49]. Второй уровень — это непосредственно разработка и реализация политик безопасности (policy)[50].

Для целей данного исследования опорой будет служить институционализм, который, с одной стороны, позволяет охватить указанные выше уровни *политического* для целей исследований безопасности, с другой – предоставляет возможность для эмпирической анализа.

Реагируя на второй вызов, мы сталкиваемся с «деформацией» в подходах к изучению, выражающуюся в дискуссиях об исследовательских программах в области безопасности[5152]. На протяжении долгого времени изучение безопасности находилось под сильным влиянием реалистского мышления. Многие исследования безопасности были «сосредоточены на четырех S: государствах (states), стратегии (strategy), науке (science) и статусе-кво (the status quo)»[53]. Такой подход к исследованию безопасности основан на понимании субъектов как инструментально рациональных акторов, имеющих дело с внешней реальностью, которая не зависит от их ценностей и представлений и к которой они могут относиться объективно. Точно так же концепция действий государства как инструментально рационального преследования собственных интересов лежит в основе структурно-реалистического анализа международной безопасности[54]. Мы же устанавливаем методологическую рамку исследований безопасности в концепциях теории рационального выбора[55], с одной стороны, а с другой

[48] Cultures of Insecurity: States, Communities, and the Production of Danger / J. Weldes [et al.]. — Minneapolis, MN : University of Minnesota Press, 1999. — 452 p.
[49] Wirls D. Buildup: The Politics of Defense in the Reagan Era. — Ithaca, NY : Cornell University Press, 1992. — 247 p.
[50] Krebs R. The Politics of National Security // The Oxford Handbook of International Security. — Oxford University Press, 2018. — P. 259–273:9
[51] Farrell T. Constructivist Security Studies: Portrait of a Research Program // International Studies Review. — 2002. — Vol. 4, no. 1. — P. 49– 72.
[52] Gheciu A., Wohlforth W. The Oxford Handbook of International Security. — Oxford, UK : Oxford University Press, 2018. — 784 p.
[53] Williams P. D. Security Studies: An Introduction. — 2-nd. — London, UK : Routledge, 2013. — 656:3
[54] Krause K., Williams M. C. Critical Security Studies: Concepts and Cases. — 1-nd. — London, UK : Routledge, 1997. — 404:40
[55] Wittek R., Snijders A., Nee V. The handbook of rational choice social research. — Stanford, California : Stanford University Press, 2013. — 624 p.

- напрямую апеллируем к критическим исследованиям безопасности (Critical Security Studies - CSS). Обоснование предметного поля и границ исследования, а также описание существующих дискуссий о противоречиях в подходах к изучению безопасности представлены в Разделе 1.1 диссертации.

Методологическая рамка теории рационального выбора (ТРВ) базируется на допущении, что все социальные феномены, в том числе политические, можно вывести из поведения отдельных людей. Политические акторы - избиратели, политики, бюрократы - преследуют цель максимизации своих материальных интересов в поисках блага и выгоды в форме голосов, должностей, власти и т.д. С учетом критики ТРВ со стороны академического сообщества[56] в данном исследовании введены институциональные ограничения для изучения оптимального поведения акторов и получения более объективного результата изменений как политической повестки, так и политических институтов.

Применительно к ТРВ отметим, что мы рассматриваем «рациональность» именно в отношении политических акторов, а не в отношении к институтам. Таким образом, мы исключаем рациональный институционализм из рамок данного исследования. Теория рационального институционализма предполагает, что государства являются рациональными, унитарными акторами, чьи действия направлены на максимизацию определенных выгод[57]. Однако данный подход имеет несколько существенных недостатков для исследования безопасности. Во-первых, многие наблюдаемые институты национальной и международной политики в вопросах безопасности оказались неэффективными в выявлении проблем и реакции на новые вызовы. Во-вторых, рациональный институционализм не обладает объяснительной силой в условии, когда более «слабые» акторы начинают подавлять более «сильные» институты (например, когда Индия, Иран и/или Северная Корея начинают переформатировать международные режимы нераспространения и т.п.). В-третьих, рациональный институционализм демонстрирует ограниченность в вопросах взаимосвязи и взаимодействия власти и непосредственно институтов. В связи с чем мы не будем использовать рамку рационального институционализма в данном исследовании. Более

[56] Грин Д., Шапиро И. Объяснение политики с позиции теории рационального выбора: почему так мало удалось узнать? // Полис. Политические исследования. — 1994. — No 3. — с. 59.
[57] Peters, G.B. Institutional Theory in Political Science. The «New Institutionalism» - London: Continuum - 2005 - P. 232: 14, 19

того, содержательно рациональный институционализм сильно противоречит подходам критических исследований безопасности.

Останавливаясь на ТРВ в отношении акторов, мы также обращаем внимание на допущении об «ограниченной рациональности»[58], которая подчеркивает неспособность лиц, принимающих решения, следовать строгой стратегии максимизации полезности в очень сложной среде и в условиях ограниченного времени и информации. Вместо того, чтобы выбирать оптимальный из всех доступных результатов, акторы, используют стратегии поиска наиболее доступного результата, более удовлетворительного, чем статус-кво. Непосредственно в такой рамке ограниченной рациональности мы подходим к анализу в отношении акторов.

Относительно институтов, мы не просто опираемся на классическое «институты имеют значение», а рассматриваем их широко и как правила, и как и нормативные представления политической воли. Оставаясь в предметном поле политической науки, мы подходим к институтам как к содержательным проявлениям политики, но при этом не рационализируя сам институт, давая «возможность» существованию неформальных форм институциональных проявлений и отождествления власти в вопросах безопасности.

Критические исследования безопасности изучают процесс фреймирования безопасности как политического явления[59]. Критические исследования безопасности занимаются анализом политики, лежащей в основе построения знания о безопасности: идеи о безопасности стали рассматриваться как политические, поскольку они были продуктом интерпретации, споров и борьбы между различными политическими акторами. Кроме того, критические исследования безопасности также стремятся пролить свет на связь между теорией безопасности и более широким политическим порядком, исследуя способы, которыми конкретные концепции безопасности не могут быть отделены от более широких представлений о том, как работает или должна работать политика[60]. Ученые, придерживающиеся данного подхода, стремятся привлечь внимание к влиянию идей и практик безопасности на создание определенного политического режима/ политической системы, тем самым *концептуализируя теоретизацию безопасности как самостоятельную политическую деятельность*.

[58] Simon, H. A. Bounded rationality. In Utility and probability // Palgrave Macmillan, London - 1990 - pp. 15-18

[59] Nunes J. Reclaiming the Political: Emancipation and critique in security studies // Security Dialogue. — 2012. — Vol. 43, no. 4. — P. 345–61.

[60] Там же. С. 347

Более того, целью критических исследований безопасности является формирование понимания динамики и последствий построения практики безопасности в конкретном историческом и социальном контексте[61].

Расширение предметных областей сферы обеспечения безопасности потребовало пересмотр того, «кто» и «что» может стать проблемой безопасности. Таким образом, подход критических исследований безопасности может служить оптимальной теоретико-методологической рамкой для данного исследования.

Данное исследование реализовано в теоретико-методологических рамках критических исследований безопасности с учетом концепций институционализма и теории рационального выбора. Это задает логику работы, которая подчинена концептуальному аппарату и секторальному подходу к анализу безопасности, разработанному Барри Бузаном[62], с отдельным фокусом на политический аспект отправления и функционирования сферы обеспечения безопасности. Барри Бузан, как и в целом Копенгагенская школа, являются одними из первых и самых влиятельных представителей критических исследований безопасности[63].

В свою очередь на методологическом уровне данное исследование опирается на концепцию логических моделей Рейна Таагаперы[64] в поисках методологического баланса в исследованиях безопасности. Не преследуя цели критиковать или оспаривать как экспертное мнение (наиболее привычный подход в исследованиях безопасности), так и современные статистические методы анализа, данное исследование стремится использовать рамку логического моделирования Таагаперы для предложения альтернативного и более объективного подхода к анализу безопасности.

Остановимся на том, чего в данном исследовании **нет**. Во-первых, данное исследование не создает и (или) не переосмысливает какую-то теорию в сфере обеспечения безопасности. Задача работы заключается в изучении изменений и их потенциале воздействия, вызванные технологиями цифровизации и автоматизации в

[61] Gheciu A., Wohlforth W. The Future of Security Studies // The Oxford Handbook of International Security. — Oxford University Press, 2018. — P. 1–12.
[62] Buzan B., Waever O., Wilde J. Security: a new framework for analysis. — London : Lynne Rienner, 1998. — 239 p.
[63] Hendershot C., Mutimer D. Critical Security Studies // The Oxford Handbook of International Security. — Oxford University Press, 2018. – P.1-2: «To consider a future for Critical Security Studies (CSS) it bears reiterating that CSS should not be considered a subdiscipline of Security Studies or International Relations….Some of the most influential works produced in the early years include:… and Security: A New Framework for Analysis (Buzan et al. 1998).»
[64] Taagepera R. Making Social Sciences More Scientific: The Need for Predictive Models. — Oxford, UK : Oxford University Press, 2008. — 232 p.

обеспечении безопасности. Дополнительная (но необязательная) задача - проследить и оценить как позитивный потенциал (выгоды) таких изменений, так и негативный (угрозы и риски). Указанное реализуется в рамках существующих теорий и подходов. Во-вторых, исследование не содержит рекомендаций относительно того, какие цифровые решения необходимо принимать к реализации, как именно их реализовывать и т.п. Иными словами, данная работа находится «над феноменами» и оценивает, анализирует и обосновывает фактические аспекты взаимодействия цифровых технологий с областью обеспечения безопасности без предоставления методических рекомендаций построения цифрового «левиафана» в области национальной безопасности. В-третьих, это не работа о единичных событиях (кейсах). Реализация структурного подхода с «реконструкцией» комплексной картины трансформации сферы обеспечения безопасности требует систематического анализа политики каждой страны (с учетом вариаций политических условий, внутренних конфликтов, столкновений технологического детерминизма и политической воли и пр.). В связи этим за единицу анализа берется не конкретный кейс использования цифровой технологии, а взаимосвязь и структура политических институтов исследуемой страны, формирующие политику национальной безопасности.

Дизайн и эмпирическая база исследования

Структура данного исследования подчинена целям и рассматриваемой проблематике. Для раскрытия эффектов «трансформации», которая заявлена в теме, в теоретической части работы (Глава 1) дается содержательный анализ преобразований политики как цифровизации, так и безопасности. На теоретическом уровне мы анализируем различные изменения и их эффекты, благодаря чему можем заявлять о трансформации. В данном контексте трансформация понимается как существенное, значимое изменение с целью улучшения, повышения качества и пр.

Сначала мы представляем преобразования в исследованиях безопасности. Затем, теоретический анализ политики цифровизации. отражая не только значимые изменения, но и сопровождающиеся эффекты цифровизации и ее влияние на политику и государственное управление. Таким образом, на теоретическом уровне мы содержательно раскрываем происходящую трансформацию. Отметим, что несмотря на дискуссионность термина «трансформация», применение его в работе не случайно. Само «понятие безопасности значительно расширилось в результате *преобразований в*

политике — вероятно, на эту *трансформацию* повлияли…»[65] различные факторы, в том числе и технологического характера. Более того, сама среда может приводить «к трансформации того, что означает безопасность»[66]. При этом «существует связь между трансформацией политик безопасности и развитием исследований в области безопасности»[67]. Таким образом, **осознание расширения содержания «безопасности» и наличие значительных преобразований – «трансформации» - в политике служит отправной точкой данного исследования.**

Эмпирическая часть исследования (Глава 2) сужает изучаемую трансформацию до ее отдельных элементов – динамики изменений и последствий таких изменений. Указанное обусловлено как теоретическими рамками, так и методологическими ограничениями. Именно поэтому исследовательский вопрос сужен до оценки динамики (подчинен, таким образом, эмпирической части исследования). Такое разведение теоретической и эмпирической части не является случайным. *Демонстрация динамики изменений позволит выделить содержательные элементы того, как такая трансформация отразилась на сфере национальной безопасности стран*. Таким образом, соблюдается единая структурная логика исследования, где трансформация представляется как более широкий концепт, но с измеримыми элементами изменений и эффектов.

Эмпирический дизайн исследования реализовывался поэтапно. **На первом этапе** был проведено предварительно исследование: два независимых сетевых анализа, по результатам которых определен пул стран, на которых будет сфокусировано исследование. Отдельно была выявлена «ключевая» цифровая технология, как фокус исследования – технология искусственного интеллекта (ИИ). Для целей исследования определены страны, демонстрирующие лидирующие позиции по итогам двух сетевых анализов: *США, Швеция, Германия, Финляндия и Франция*.

В связи с эмпирическим установлением конкретной цифровой технологии была реализована концептуализация искусственного интеллекта. В рамках данного исследования *под технологией искусственного интеллекта будут пониматься алгоритмические и компьютерные системы (в том числе программное обеспечение и/или оборудование), которые, обучаясь, могут решать сложные проблемы, делать*

[65] Schlag G., Junk J., Daase C. Transformations of security studies: dialogues, diversity and discipline. - Routledge. 2015. - P.250:12 -
[66] Там же. С. 152
[67] Там же. С. 233

прогнозы или выполнять задачи, требующие человеческого восприятия, познавать, планировать, обучаться, общаться или совершать физическое действие, обязательно, в сфере обеспечения безопасности или непосредственно в военной сфере.

Вторым этапом было формирование эмпирической модели. Формируя эмпирическую модель, наш выбор индикаторов и параметров определяется акцентом на то, что поддается измерению[68]. Работа с индикаторами и показателями, в свою очередь, подчинена необходимостью соблюдать баланс между полнотой и доступностью данных[69].

Показатель согласованности (консистентности) безопасности (security consistency) формируется посредством разницы показателей угроз (threats) и возможностей технологий ИИ (AI capability) реагировать на такие угрозы. Методологически, влияние алгоритмов (ИИ, как отдельного типа цифровых технологий) в национальной безопасности представляется в виде процесса принятия решений в сфере обеспечения безопасности при помощи блок схем с определением математических параметров. *Показатель согласованности (консистентности)* безопасности отражает как государство способно оценивать угрозы (*показатель угроз*) и обладает ли государство необходимым уровнем возможностей для их отражения (*показатель возможностей*).

Индикатор возможностей ИИ рассчитывается в логике композитных индексов. Исходя из концептуальной рамки понимания Искусственного интеллекта и целей создания индикатора было выделено четыре области/ сферы (технологическая сфера; экономическая сфера; управление; социальная сфера) с распределением весов.

Формирование индикатора оценки угроз опирается на подходы узкоспециализированного предметного поля исследований военного вооружения и военных угроз - Оценка угрозы и назначение оружия (Threat Evaluation and Weapon

[68] Fioramonti L., Kononykhina O. Measuring the Enabling Environment of Civil Society: A Global Capability Index // Voluntas. — 2015. — Vol. 26. — P. 466–487.
[69] Там же. С. 467

Assignment – TEWA)[70][71][72][73][74]. В данном исследовании основная логика представляет собой оценку угрозы и соотношение этих угроз с защищаемыми объектами и секторами безопасности.

Дополнительно была **произведена верификация и тестирование модели** при помощи ее численного исследования (simulation analysis[75]). Логика численного исследования направлена на проверку чувствительности модели[76]. Что если какая часть данных не соответствует реальности, является ложной или совсем отсутствует? На сколько сильно это повлияет на результаты? Тестирование модели при помощи симуляции направлена на получение ответов на эти вопросы.

По итогу симуляций и тестирования, модель демонстрирует устойчивость по отношению к большинству показателей. Однако следует обращать особое внимание на источники данных к показателю Факторы угроз (Threat factors – TF) из индикатора Оценка угроз, показателям Технологической и Социальной сферы из индикатора Возможностей ИИ. К данным показателям дополнительно проверялось завышение (преувеличения) в данных из доступных источников.

Следующим этапом было применение эмпирической модели для каждой страны-кейса и сравнение полученных моделей стран.

Непосредственная реализация эмпирической модели для каждой выбранной страны проходила по единому протоколу. На первом этапе определялся временной охват, релевантный для каждой страны. При определении временного охвата в учет были взяты:

1. основные нормативно правовые акты (НПА) в сфере обеспечения безопасности (стратегии национальной безопасности, законы, декреты, доктрины и т.п., определяющие систему безопасности государства);

[70] Cocelli M., Arkin E. A threat evaluation model for small-scale naval platforms with limited capability // EEE Symposium Series on Computational Intelligence. — 2017. — P. 1–8.
[71] Johansson F., Falkman G. Comparison between two approaches to threat evaluation in an air defense scenario // Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics). — 2008. — Vol. 5285. — P. 110–121.
[72] Naeem H., Masood A. An optimal dynamic threat evaluation and weapon scheduling technique // Knowledge-Based Systems. — 2010. — Vol. 23, no. 1. — P. 337–342.
[73] Decision support system for optimum decision making process in threat evaluation and weapon assignment: Current status, challenges and future directions / A. Naseem [et al.] // Annual Reviews in Control. — 2017. — Vol. 43. — P. 169–187.
[74] Kumar S., Tripathi B. Modelling of Threat Evaluation for Dynamic Targets Using Bayesian Network Approach // Procedia Technology. — 2016. — Vol. 24. — P. 1268–1275.
[75] Marquardt K. L. How and how much does expert error matter? Implications for quantitative peace research // Journal of Peace Research. — 2020. — Vol. 57, no. 6. — P. 692–700.
[76] Gelman A., Hill J., Vehtari A. Regression and Other Stories (Analytical Methods for Social Research). — Cambridge University Press, 2020. — 552 p

2. основные нормативные документы информационно-технической сферы, с фокусом на цифровизацию, алгоритмизацию, автоматизацию политики и государственного управления (с учетом концепции электронного правительства, вплоть до регулирования конкретных типов цифровых технологий);
3. временной охват с учетом нескольких правительств/ администраций для динамики изменений.

После формирования временной таблицы начинался непосредственно сбор данных по каждому показателю модели. Обязательным условием сбора данных был учет как национальных НПА и официальных статистик, так и международных отчетов, баз данных и пр. по анализируемой стране. В итоге по каждой стране был сформирован дата-сет, где к каждому значению показателя делалась пометка об источнике данных (для верификации). Данные доступны в открытом репозитории GitHub по стабильной ссылке отдельными файлами по каждой стране[77].

При построении дата-сета по каждой стране была проведена более расширенная работа с национальными НПА и официальными данными статистики. Если для обоснования дат учитывались только основополагающие акты стран, то данные для модели насыщались в результате анализа всех публичных документов. В случае отсутствия данных на национальном уровне или существования единообразной базы по всем странам – учитывались данные международных организаций.

Указанное разграничение в работе с НПА, а также расширенная работа с национальными актами, подчинена единой логике исследования: мы стремимся выявить и проследить изменения, происходящие непосредственно на национальном (внутреннем) уровне страны. Использование общих (наднациональных) документов востребовано только в случае отсутствия (или не публичности) внутренних источников.

Научный вклад исследования в развитие предметного поля

Современные исследования сферы безопасности испытывают значительное влияние парадигм международных отношений и, зачастую, опираются на качественную методологию с опорой на экспертные интервью. Не исключая ценность существующих подходов, данное исследование стремится преодолеть оба ограничения: во-первых, исследование «возвращает» институциональные основы политической науки в

[77] Репозиторий с данными по каждой стране: https://github.com/AlTurobov/PhD_SecurityConsistency (стабильная ссылка). Каждой стране корреспондирует отдельный файл, также к каждой стране указана дополнительная ссылка с комментариями и описанием источников.

исследования сферы обеспечения безопасности, а во-вторых, предлагает количественный подход к оценке динамики при помощи разработки эмпирической модели, которая позволяет оценить трансформационный эффект цифровых технологий на системы национальной безопасности стран.

На теоретическом уровне исследование предоставляет описание процесса проникновения цифровых технологий (на примере технологии ИИ) в сферу обеспечения безопасности с оценкой вызываемых изменений в системах безопасности государств. Результаты демонстрируют как происходит адаптация систем национальной безопасности посредством внедрения передовых цифровых технологий. Косвенно результаты демонстрируют то, что государства активно применяют наработки больших (в контексте национального и международного рынков) технологических компаний для нужд обеспечения безопасности. Таким образом, продолжается тенденция подчинения и секьюритизации развития (development) сфере обеспечения безопасности. Оценка и восприятие угроз в контексте цифровых технологий со стороны государств нелинейная, а обладает волнообразным характером. Динамика изменений во всех анализируемых моделях стран не является единообразной, хотя и имеет несколько схожих этапов.

Положения выносимые на защиту

1. Исследования безопасности, как и сам конструкт «безопасность», развиваются эволюционно, как расширяясь в вопросах понимания угроз (и возможностей их купирования), так и наполняясь новыми феноменами. Предлагается рассматривать эволюцию предметной области безопасности как связный процесс. Мы предлагаем рассматривать содержательные изменения в исследованиях безопасности вне дискуссии о школах, опираясь на анализ изменения концептов (угроз, безопасности и пр.), расширением секторов безопасности и т.д. Цифровые технологии, по своему влиянию и проникновению, пронизывают все сектора безопасности, значимо их преобразовывая.
2. Феномен цифровизации является политическим, напрямую зависящим от функционирования институтов. Качество цифровизации зависит от совместных действий политических институтов и технологических компаний. Процесс цифровизации подчинен принимаемым политическим решениям (дискуссия возможна об уровне таких решений). При этом сам процесс напрямую сопряжен и зависит от применения конкретных типов цифровых технологий.

3. Сетевой анализ[78] торговых (ИКТ и цифровыми товарами и услугами) связей стран выделяет страны-лидеры (например, Финляндия, Германия и Швеция) и демонстрирует международную конкуренцию в области цифровизации. В сетевой структуре можно наблюдать страны, которые являются ключевым звеном связности международной торговли. Такие страны выступают своего рода «мостом» глобального обмена опытом, диффузии технологий и, потенциально, ключевыми акторами глобальной институционализации цифровизации.
4. Концептуальное понимание технологии искусственного интеллекта, разработанное для целей данного исследования, является «зонтичным», охватывая совокупность подходов, инструментов и алгоритмов. Под технологией искусственного интеллекта понимаются алгоритмические и компьютерные системы (в том числе программное обеспечение и/или оборудование), которые, обучаясь, могут решать сложные проблемы, делать прогнозы или выполнять задачи, требующие человеческого восприятия; познавать, планировать, обучаться, общаться или совершать физическое действие (обязательно в сфере обеспечения безопасности и (или) непосредственно в военной сфере).
5. Разработана, протестирована и валидизирована эмпирическая модель изучения изменений и оценки системы безопасности государства под влиянием цифровых технологий. Эмпирическая модель имеет оценочный характер. Влияние технологии в сфере национальной безопасности представляется в виде процесса принятия решений в сфере обеспечения безопасности. Показатель согласованности (консистентности) безопасности отражает то, как государство оценивает угрозы (показатель угроз), а также то, обладает ли государство необходимым уровнем возможностей для их отражения (показатель возможностей). Предлагаемый подход подразумевается, как дополнение к существующим и позволяет оценивать динамику развития системы безопасности конкретного государства под влиянием технологии искусственного интеллекта.
6. Сравнительный анализ моделей стран позволяет утверждать, что (1) у правительств единообразный подход к определению возможностей технологии ИИ в вопросах

[78] Результаты второго сетевого анализа (в рамках предварительного исследования проведено два сетевых анализа для выявления стран, которые будут включены в анализ, и выявления конкретного типа цифровых технология как фокуса эмпирического части исследования) представлены в публикации: Туробов А.В. Возможности трансплантации политических институтов при торговле технологиями: результаты сетевого анализа в сравнительной перспективе // Вестник Томского государственного университета. Философия. Социология. Политология – 2022–№65 - С. 310-327.

безопасности; (2) наблюдается постоянное накопление знаний и опыта о потенциале технологии, поэтому во всех моделях присутствует постоянный рост показателя возможностей; (3) существует международное единообразие и конкуренция, когда страны в приблизительно одинаковый промежуток времени начинают обращать внимание на влияние цифровых технологий в области безопасности; (4) регламентация технологии искусственного интеллекта происходит единообразно и в схожие временные промежутки (все анализируемые страны приняли соответствующие стратегии в период двух лет: 2017-2019 гг.).

7. Динамика изменений систем национальной безопасности нелинейна. Волнообразный характер динамики отражает различия в адаптивности политических институтов и разнообразие политических решений в вопросах применения технологий в сфере безопасности. Несмотря на то, что все анализируемые страны максимизируют возможности применения цифровых технологий в безопасности, оценка угроз неоднородна и может меняться в каждой стране. Указанное, с одной стороны, иллюстрирует специфику самих цифровых технологий – сложности с оценкой угроз, технические вызовы и пр. С другой – позволяет утверждать, что само понимание угроз от страны к стране может сильно меняться, как и конкретная угроза может пересматриваться даже в рамках одного государства с течением времени.
8. Государства определяют роль и место технологий соразмерно их потенциалу возможностей, т.е. правительства адаптируются к современным вызовам и преобразуют сферу национальную безопасность, интегрируя технологии. Государства сконструировали систему безопасности таким образом, что возможности реагирования превосходят оцениваемые угрозы. Более широкая интерпретация результатов позволяет предположить, что изменения и преобразования в системах безопасности полностью контролируются государствами.

Апробация результатов

Список публикаций

1. Туробов А.В., Миронюк М.Г. Эмпирическая модель анализа динамики алгоритмизации (технологии искусственного интеллекта) в сфере обеспечения безопасности на примере США // Политическая наука. 2021. No 3. С. 72-111.
2. Туробов А.В. Возможности трансплантации политических институтов при торговле технологиями: результаты сетевого анализа в сравнительной перспективе // Вестник

Томского государственного университета. Философия. Социология. Политология. 2022. № 65. С. 310-327.

3. Туробов А. В., Чумакова М. А., Вечерин А. В. Международный опыт применения математико-статистических алгоритмов прогнозирования преступности // Международные процессы. 2019. Т. 17. № 4. С. 153-177.
4. Антонова А. В., Туробов А. В. Мишени цифровых технологий через призму образования // Образовательная политика. 2020. № 2 (82). С. 42-55.

Представление результатов исследования на конференциях

1. 9th International Conference on Information Law and Ethics. Psychological and socio-political dynamics within the Web: New and old challenges to Information Law and Ethics. 11-13 July 2019 Rome, Italy. Доклад: Data for Public Policy in the Web Era: A Call for Systemic and Ethical View.
2. 11 Российский форум по управлению Интернетом. Молодежный семинар по управлению интернетом. 4-8 апреля 2020, Москва, Россия. Выступающий, приглашенный эксперт. Доклад: Выступающий, приглашенный эксперт: Государство, этика и искусственный интеллект: гуманитарные и законодательные проблемы разработки и внедрения алгоритмов в повседневную жизнь.

Представление результатов исследования в реализуемых дисциплинах

1. «От больших данных к принятию политических решений», ОП «Прикладная политология» (2019/2020 - н.в.);
2. «Правительство и государственная политика в эпоху цифровых технологий», ОП «Прикладная политология» (2019/2020 - н.в.);
3. «Актуальные проблемы современной политики», Майнор (2019/2020 - н.в.).

Апробация результатов исследования на грантовой основе

В рамках аспирантского исследования был выигран и реализован (финальный отчет высоко оценен комиссией) грант РФФИ №20–011–31658 «Анализ динамики алгоритмизации (технологии искусственного интеллекта) в сфере национальной безопасности: эмпирическая модель стабильности безопасности на примере США.» (рук. - Миронюк М.Г., исп - Туробов А.В.)

Основное содержание работы

Теоретическая часть исследования посвящена установлению и обоснованию сопряжения предметной области безопасности и политики цифровизации. Продемонстрировано широкое понимание концепта трансформации. Первый уровень

теоретического анализа направлен на выявление эволюционного развития как понимания концепта «безопасности», так и предметного поля исследований безопасности. Теоретический анализ направлен на демаркацию области исследования безопасности (security studies), выявление ключевых преобразований понимания и подходов безопасности, а также формулирует взгляд на современные изменения, сопряженные с применением цифровых технологий. Указанный раздел одновременно выполняет функцию концептуализации понимания безопасности, а также демонстрации исторического развития подходов к такому пониманию. В итоге предлагается рассматривать проникновение цифровых технологий в вопросы безопасности не как формирование самостоятельно сектора безопасности (в логике Копенгагенской школы), а как процесс, пронизывающий все сектора (схоже со спецификой информационной безопасности). Предлагаемая теоретическая рамка направлена на изучение взаимосвязи цифровых технологий в сфере обеспечения безопасности.

Принимая существующие противоречия на уровне подходов, мы стремимся продемонстрировать связность развития сферы безопасности. Угрозы действительно наполняются иным содержанием, расширяются, их концептуализация содержательно меняется, однако это происходит с учетом предыдущих работ и в опоре на них. Таким образом, мы предлагаем рассматривать содержательные изменения в исследованиях безопасности вне дискуссии о школах, но с опорой на анализ содержательных аспектов наполняемости концептов, расширения секторов и т.д. Отметим, что такой взгляд на безопасность не является новым или уникальным. Книга «Трансформации исследований безопасности: диалоги, разнообразие и дисциплина» вся посвящена «…наведению мостов между различными «лагерями», инициируя диалог…исследований в области безопасности»[79], по сути, предлагая схожий взгляд на связность существующих подходов.

Краткое представление эволюции сферы обеспечения безопасности необходимо для фокусировки понимания безопасности данного исследования. Мы не отождествляем военную безопасность (отсутствие угроз и вызовов военного свойства) с безопасностью государства как таковой. Соответственно, данное исследование находится в предметном поле исследований безопасности (security studies) и подчинено его логике.

[79] Schlag G., Junk J., Daase C. Transformations of security studies: dialogues, diversity and discipline. - Routledge. 2015. - P.250:2

Второй теоретический уровень направлен на анализ политики цифровой трансформации. Сначала мы концептуализируем цифровизацию, демонстрируя значимую роль политических институтов. Более того, концептуализация цифровизации позволяет считать данный феномен как политический процесс. Понимая, что цифровизация это не «процесс в вакууме», а напрямую реализуется за счет и посредством цифровых технологий, предлагается различная типологизация цифровых технологий. Выявление и анализ типов цифровых технологий не подчинен логике технологического детерминизма, а неразрывно связан с институциональным базисом. Демонстрируя последствия применения цифровых технологий и сопутствующих преобразований, мы представляем непосредственно «процессуальные» политические изменения. Указанные особенности нашего подхода позволяют расширенно рассматривать трансформацию. Объединяя оба теоретических уровня, мы формулируем и демонстрируем как происходит сопряжение сферы безопасности и цифровизации.

Эмпирическая часть исследования сужает теоретическую рамку трансформации до ее измеримых элементов изменений и последствий. Представлено предварительное исследование, направленное на выявление основных стран, подлежащих анализу, при помощи методологии сетевого анализа. Мы стремимся не просто проанализировать страны с высоким «инновационным потенциалом», а непосредственно страны, занимающие лидирующие позиции в вопросах цифровизации. Также предварительный анализ позволит сфокусировать исследование на одном конкретном типе цифровых технологий – искусственном интеллекте.

Предложена эмпирическая модель с обоснованием. Также демонстрируются результаты верификации модели – проверки ее на устойчивость при помощи численного исследования модели (simulation analysis). По результатам мы с определенной уверенностью утверждаем, что модель действительно позволяет измерять и анализировать динамику проникновения цифровых технологий в систему обеспечения безопасности современных государств.

Построение эмпирической модели по пяти странам - США, Швеции, Германии, Финляндии и Франции - позволяет продемонстрировать проникновение технологии в систему национальной безопасности, а также выявить динамику такого процесса. По каждой стране работа с данными и построение модели реализовывалось по единому протоколу. Сама модель и работа с данными является рассмотрением институциональных последствий и результатов политического процесса. Результаты

моделей представляются с качественным описанием и интерпретацией конкретных случаев.

Сравнительный анализ моделей стран по трем показателям (возможности ИИ, оценка угроз, согласованность (консистентность) системы безопасности) позволяют выявить различные подходы правительств к вопросам применения цифровых технологий в безопасности, а также дают основу для определения лучших практик, заявленных в дополнительном исследовательском вопросе.

Сравнение моделей стран по показателю *возможностей технологии искусственного интеллекта* позволяет проследить динамику того, как правительства оценивают возможности технологии относительно сферы обеспечения безопасности. Графическое сравнение моделей представлено ниже на Рисунке 1.

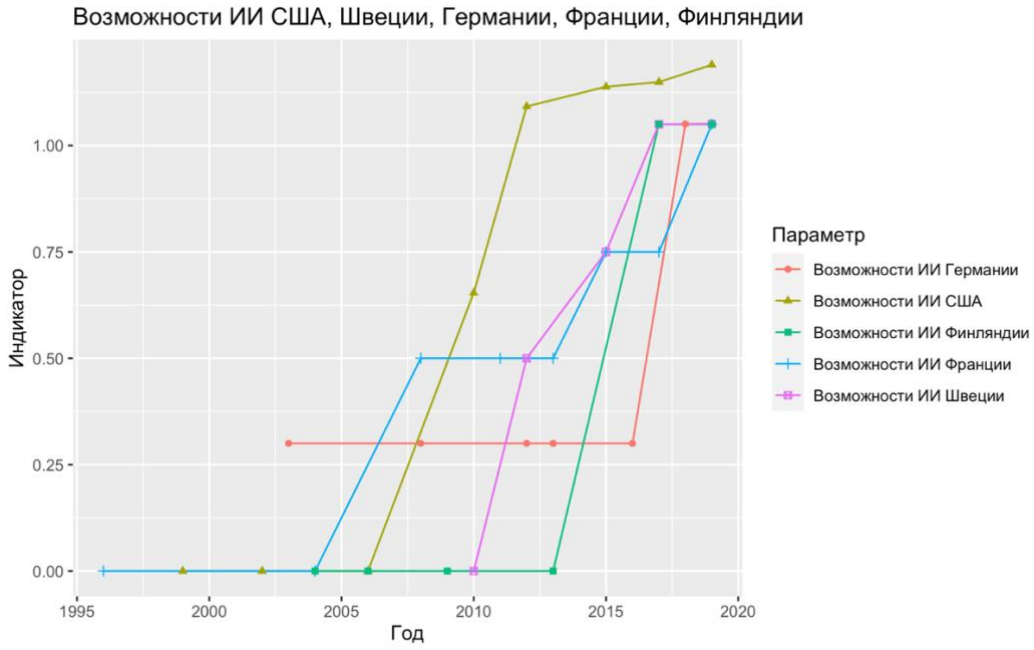

Рисунок 1: График сравнения моделей стран по показателю возможностей технологий искусственного интеллекта

Сравнительный анализ моделей стран по *показателю оценки угроз* позволяет отследить как правительства стран определяют угрозы, сопряженные с технологическим фактором, в сфере обеспечения безопасности. Графическое сравнение моделей представлено ниже на Рисунке 2.

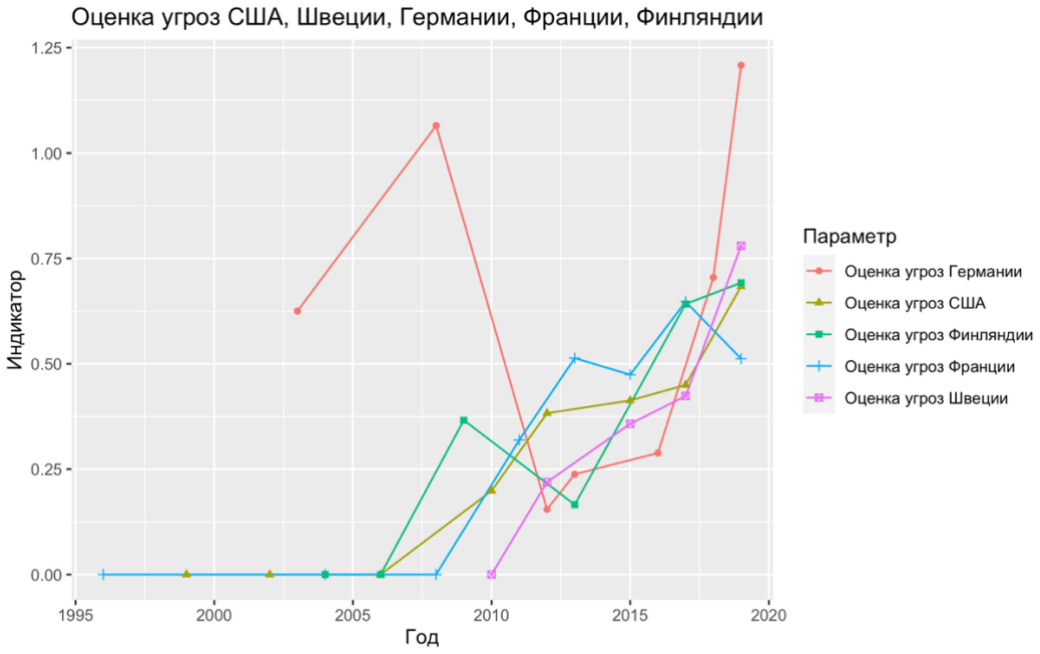

Рисунок 2: График сравнения моделей стран по показателю оценки угроз

Логика *показателя согласованности системы безопасности* отражает готовность государства реагировать на угрозы. Готовность проявляется за счет учета того, как государство оценивает грозы (показатель оценки угроз) и как государство определяет возможности купирования/преодоления угроз (показатель возможностей технологии ИИ). Данный показатель сфокусирован на конкретном типе цифровой технологии, а именно технологии искусственного интеллекта. Таким образом, высокий показатель согласованности безопасности означает, что система безопасности государства готова соразмерно отвечать на определяемые (выявляемые) правительством угрозы.

Непосредственно сравнительный анализ моделей стран по разработанному показателю согласованности (консистентности) системы безопасности представлен ниже на Рисунке 3.

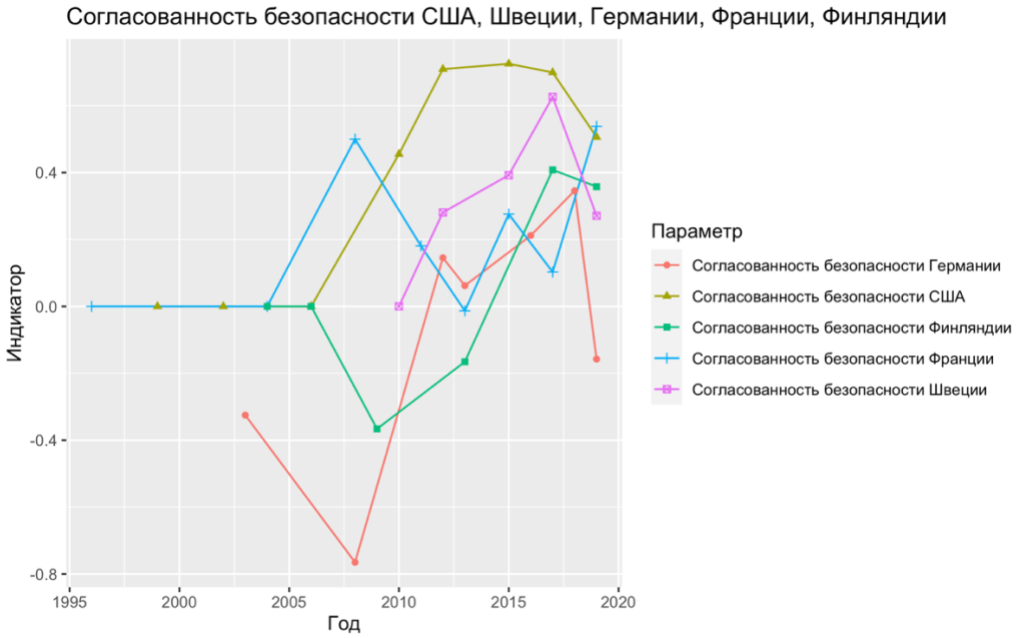

Рисунок 3: График моделей стран по показателю согласованности (консистентности) системы безопасности

В моделях анализируемых стран присутствуют схожие тренды. Во-первых, это единообразный подход правительств к определению возможностей технологии, который проявляется в постоянном росте этого показателя. Ни в одной модели стран не было случая, чтобы данный показатель демонстрировал отрицательную динамику. Во-вторых, анализируемые модели стран демонстрируют в целом сходную временную динамику. Внимание к оценке угроз технологического характера проявляется в период 2006-2008 гг., а максимальные значения по всем показателям достигаются в 2017-2019 гг. Иными словами, мы можем наблюдать определенное единообразие (или конкуренцию), когда страны в приблизительно одинаковый промежуток времени начинают обращать внимание на цифровые технологии в области безопасности.

В-третьих, интересно единообразие в части регламентации технологии искусственного интеллекта. В 2017 г. Финляндия и Франция принимают национальную стратегию по развитию данной технологии, в 2018 г. – Швеция и Германия, а в 2019 г. – США. Указанное также может объясняться как конкурентной борьбой вокруг технологии, так и определенным единообразием процессов развития инновационно-технологичных стран.

Основные результаты исследования

Опираясь на заявленную проблематизацию, данное исследование на теоретическом уровне представляет описание процесса того, **как** цифровые технологии

(на примере технологии ИИ) проникают в сферу обеспечения безопасности, а также **какие** изменения происходят в самой системе безопасности государства. Результаты показывают, что происходит максимизация возможностей систем национальной безопасности за счет внедрения передовых цифровых технологий (однако не равномерно, с учетом институциональных особенностей государств). Косвенный образом результаты демонстрируют, что государства активно применяют наработки больших (в контексте национального и международного рынков) технологических компаний в сфере обеспечения безопасности. Таким образом, продолжается тенденция подчинения и секьюритизации развития (development) сфере обеспечения безопасности.

Динамика изменений во всех анализируемых моделях стран не единообразна, однако имеет несколько схожих этапов. Так, к 2018-2019 гг. стабилизируется показатель возможностей ИИ, а показатель оценки угроз к данному периоду демонстрирует стремительный рост. При этом показатель согласованности (консистентности) безопасности демонстрирует различия среди государств относительно начала проникновения цифровых технологий в сферу обеспечения безопасности (рост с колеблется от 2003 до 2006 гг.), а также общей динамикой. Пока одни страны активно наращивают потенциал трансформации систем национальной безопасности (например, США и Швеция), другие страны демонстрируют обратный тренд – усиление опасений и рисков таких изменений (например, Германия и Финляндия).

На втором уровне проблематизации – в инструментальной (методологической) плоскости – разработана, протестирована и валидизирована эмпирическая модель изменений и оценки системы безопасности государства под влиянием цифровых технологий (на примере технологии ИИ). Эмпирическая модель имеет оценочный характер и направлена на формирование концепции оценки системы безопасности (не только оценка угроз, но и выявление возможностей) и создание эмпирического подхода к измерению сферы обеспечения безопасности государства.

Попытка «объективного» анализа динамики демонстрируют некоторые преимущества. Во-первых, мы можем отдельно наблюдать изменения как в официальных оценках угроз (то **как** и на **что** государство обращает внимание и определяет в качестве угрозы), а также в определении возможностей технологии (в контексте публичного восприятия реализуемых исследований, апробации и внедрения различных алгоритмических систем искусственного интеллекта). Во-вторых, мы можем с учетом временных отрезков анализировать то, как развивалась технология, как она «проникала» в систему безопасности. Например, стремительное развитие технологии

ИИ в период с 2006 по 2012 гг. в США позволило этому государству инициировать и возглавить технологическую гонку, последствия которой выходят за научно-исследовательские и технологические рамки. В-третьих, отдельный акцент на оценке угроз позволяет анализировать политическое внимание (отношение) к технологии, что расширяет существующую дискуссию в предметном поле политизации и секьюритизации технологий. В-четвертых, представленная модель обладает интерпретационной гибкостью, учитывая, что собранные данные представляют разные области (социальная, экономическая, политическая) и с большим временных охватом. В-пятых, модель может быть полезна для проведения сравнительных исследований стран. Последующие исследования будут направлены на усиление кросстранового сравнительного анализа как по единому показателю согласованности безопасности, так и по отдельным индикаторам возможностей ИИ и оценки соответствующих угроз.

Особо отметим масштабируемость модели: потенциально можно заменить технологию ИИ любой другой цифровой технологией (например, облачные вычисления, технологии связи пятого поколения и т.д.) и строить эмпирическую модель согласованности (консистентности) безопасности с учетом конкретной технологии. Подразумевается, что сферы, веса и коэффициенты будут сохранены и для другого типа цифровой технологии, однако указанное будет проверено в последующих исследованиях. В результате можно проследить динамику изменений системы безопасности государства, но уже относительно конкретного типа технологии, и также проводить сравнительный анализ стран. Последующие исследования будут сфокусированы на тестировании возможностей модели и проверке ее интерпретационных возможностей (особенно в сравнительной перспективе).

Результаты тестирования гипотез

Первая гипотеза относительно оценки угроз, которая должна опережать имеющиеся решения по противодействию угрозам во всех анализируемых странах, **частично опровергнута**. Несмотря на специфичность, неоднозначность и стремительность развития цифровых технологий, в частности технологии искусственного интеллекта, большинство государств успевают как минимум на институциональном уровне определять и закреплять возможности реагирования на такие угрозы. Иными словами, мы наблюдаем феномен, когда государства в сфере обеспечения безопасности на первоначальном этапе определяют возможности реагирования на угрозы более емко (полно и вариативно), чем характеризуют саму угрозу. Однако указанное распространяется не на все государства. В анализируемых

моделях стран подобное наблюдается во всех странах, кроме Германии. Модель Германия является единственной, где к 2019 г. показатель оценки угроз превосходит показатель определения возможностей. Именно поэтому мы можем лишь частично опровергнуть первую гипотезу.

Содержательная интерпретация результата тестирования первой гипотезы позволила определить «отношение» правительств к изменениям в сфере безопасности, опосредованным цифровыми технологиями. Государства определяют роль и место технологий соразмерно их потенциалу возможностей. Правительства успешно интегрируют технологии, сбалансированно оценивая угрозы. Мы демонстрируем то, что государства адаптировались к современным изменениями и сконструировали систему безопасности таким образом, что возможности реагирования превосходят оцениваемые угрозы. При более широкой интерпретации результатов можно предположить, что изменения и преобразования в системах безопасности полностью контролируются государствами. Иными словами, это не «спонтанная трансформация», не простая реакция на возникающие вызовы, а планомерная и стратегическая политическая деятельность по оценке потенциала возможностей в соотношении с угрозами. Указанный выше подход присущ не всем государствам. Можно утверждать, что в некоторых государствах (например, Германии) наблюдается увеличение опасений в вопросах безопасности, т.к. правительства больше внимания обращают на потенциал угроз.

Вторая гипотеза относительно проявления динамики применения цифровых технологий в сфере обеспечения безопасности в промежутке 2008-2010 гг. опиралась на организационный принцип современных сил обеспечения безопасности - «максимизация военной мощи за счет использования технологий»[80]. Результаты моделей **частично опровергают** предположение о том, что применение государствами цифровых технологий в сфере обеспечения безопасности будет происходить раньше, чем в обществе появится дискуссия об этих типах цифровых технологий. Несмотря на схожую динамику, модель Германии демонстрирует проявление применения цифровых технологий лишь к 2016 г., а модели Франции и Финляндии – в 2013 г. Таким образом, мы не можем однозначно утверждать, что во всех странах проявления применения цифровых технологий в сфере обеспечения безопасности обнаружились раньше

[80] Farrell T. Constructivist Security Studies: Portrait of a Research Program // International Studies Review. — 2002. — Vol. 4, no. 1. — P. 49– 72:67

общественной/ публичной дискуссии. Несмотря на то, что модели США и Швеции подтверждают данный тезис, такие результаты не распространяются на все страны. Возможный объяснительный механизм столь неожиданного результата скрывается в специфике технологии искусственного интеллекта, которая не является изначально военной технологией, а разрабатывалась как гражданские/коммерческие решения.

К сожалению, неоднозначность результата (в отношении моделей двух стран гипотеза подтверждается, в отношении трех – опровергается) не позволяет нам однозначно утверждать, что государства стремятся к максимизации мощи и безопасности за счет технологий. Потенциальным объяснением такого разнообразия в моделях стран может служить то обстоятельство, что часть государств опасаются угроз и рисков сильнее, чем видят потенциал для применения технологий. Поэтому они будут стараться сначала получить доказательную базу выгод, а лишь потом начинать внедрять и применять технологии. Также разнообразие может объясняться существующими возможностями технологического развития (development) и потенциалом человеческого капитала (наличием или отсутствием высококвалифицированных кадров для внедрения технологий).

Третья гипотеза относительно сравнительного анализа показателей восприятия угроз и типа угроз конструировалась вокруг консенсуса о том, что одна и та же угроза может по-разному восприниматься государствами. Мы хотели проверить, действительно ли относительно цифровых технологий существует сильная неопределенность, которая формирует излишние опасения, в связи с чем восприятие и тип угроз будут достигать максимальных значений во всех анализируемых странах. Результаты анализа демонстрируют, что гипотеза **подтверждается.** *Однако с позиции эмпирической точности - частично.* В разные периоды даже в рамках одной страны данный показатель может колебаться. Таким образом, *восприятие угроз государствами не является линейным*. Вполне возможно достижение максимальных показателей в середине 2010-х гг. с последующем снижением данного показателя. Указанное подтверждает существующее ограничение сферы обеспечения безопасности, что каждое государство по-разному определяет и оценивает угрозы. Мы не просто подтверждаем существующий консенсус о различиях в определении и оценки угроз, но и уточняем его непосредственно контекстом цифровых технологий. Более того, мы наблюдаем, что по-разному определяются и оцениваются одни и те же угрозы относительно разных временных периодов. Причем указанное не означает, что с течением времени восприятие одной и той же угрозы должно «снижаться».

Мы обнаруживаем существенную специфику в отношении к цифровым технологиям, что расширяет дискуссию о трансформационном эффекте технологий. Более того, мы демонстрируем, что такие преобразования не являются линейными. Государства адаптируются к угрозам, а также стараются соразмерно оценивать возникающий потенциал их купирования. В свою очередь, цифровые технологии выступают и как инструмент (укрепляющий изменения), и как сам фактор, повышающий опасения. Это важный результат, который позволяет, при расширенной интерпретации, утверждать, что трансформация может быть сопряжена не только с позитивными изменениями, но и с появлением обоснованных опасений.

Четвертая гипотеза относительно достижения к 2018-2019 гг. максимальных показателей эмпирической модели всех анализируемых стран формулировалась в логике готовности государств к рискам и вызовам со стороны цифровых технологий. По результатам анализа гипотеза **подтвердилась частично**. Мы ожидали, что будем наблюдать во всех моделях анализируемых странах примерно единообразный тренд к 2018-2019 гг.: показатель возможностей ИИ выравнивается и стабилизируется на одном уровне в течении нескольких лет, что означает что государства начинают практическое применение технологии с соразмерным пониманием возможностей и пределов применимости. В свою очередь показатель оценки угроз должен был получить стремительный рост к 2018-2019 гг., что должно было свидетельствовать о высокой оценке рисков и угроз со стороны государства именно в последние годы, когда мы стали получать все больше информации и знаний о влиянии технологий, а также сопутствующих рисках. Сам же показатель согласованности безопасности должен был демонстрировать рост с 2006-2010 гг. с примерно схожей поступательной динамикой роста и резким скачком в периоды 2016-2017 гг. т.к. в этот временной период, во-первых, государства могли наблюдать, по сути, первые реальные последствие применения технологий, а во-вторых, реализовывалось усиление политизации и секьюритизации цифровых технологий.

Однако наши результаты не всегда отражают указанные ожидания. Они верны для стран США и Швеции, соответственно для этих стран продемонстрированная логика укладывается в подход правительства к изменениям систем национальной безопасности под влиянием цифровых технологий, но не распространяется в полной мере на Германию, Францию и Финляндию. Действительно, во всех анализируемых странах показатель возможностей технологии искусственного интеллекта достигает схожего максимального значения к 2019 г., а вот по остальным показателям и их динамике

различия между моделями странам существенны. Во-первых, оценка угроз не во всех моделях стран линейна с достижением высоких показателей к 2019 г. Так, модель Франции, например, наоборот, демонстрирует спад в оценке угроз с 2017 к 2019 г. Во-вторых, разработанный показатель согласованности безопасности не обязательно демонстрирует постепенный планомерный рост. Его динамика волнообразна и довольно уникальна для каждой страны, за исключением США и Швеции. Указанное подкрепляет существующие дискуссии о неоднородности систем национальной безопасности стран, а также демонстрирует новые результаты о разнообразии реакции правительств на технологические вызовы в сфере безопасности. В-третьих, вопреки теоретическим ожиданиям, резкий скачок показателя согласованности безопасности в 2016-2017г. наблюдается только у модели Франции, тогда как в остальных моделях наблюдается спад. Указанное может объясняться как сложностью технологии искусственного интеллекта, где в более ранее время было больше обнадеживающей информации о пользе и потенциале, а с течением времени потенциальные ожидания сменились прагматическим пониманием ограниченности технологии и возрастанием рисков относительно применения. Альтернативное объяснение может скрываться в усилении секьюритизации технологии и смещении отношения к ИИ с публичного обсуждения в сторону информационного ограничения (секретности).

Теперь мы **можем ответить на заявленный основной исследовательский вопрос** о динамике применения цифровых технологий правительствами разных стран в сфере обеспечения национальной безопасности двумя основными тезисами. Во-первых, динамика применения нелинейная, а волнообразная и отражает как национальные особенности концептуализации национальной безопасности, так и внутреннюю специфику отношений государств к конкретному типу цифровых технологий. Несмотря на теоретические опасения, правительства стран успевают соразмерно внутренним особенностям системы безопасности оценивать риски и выгоды от технологий и на основании такой оценки работать над их внедрением. Иными словами, результаты демонстрируют, что в странах отсутствуют как «алармистские» и завышенные опасения, так и снисходительность к вопросам технологических изменений систем национальной безопасности. Во-вторых, в странах присутствуют общие тренды как во временной плоскости (например, схожие сроки принятия национальных стратегий и программ по искусственному интеллекту), так и по конечной динамике определения возможностей технологии искусственного интеллекта – приближение к максимальным значениям к 2019 г. Указанное может свидетельствовать или о функционировании системы

международного сотрудничества как в области безопасности, так и в сфере цифровых технологий, или о развитии и усилении конкуренции между странами относительно технологии искусственного интеллекта. Понимание реального механизма, скорее всего, требует объединения указанных объяснений: страны продолжают наращивать международное сотрудничество, но при этом усиливается конкуренция между ними.

В свою очередь, сравнительный анализ позволяет выявить как сходства применения и сходства временной динамики, так и уникальные страновые различия для ответа на дополнительный исследовательский вопрос.

Заключение

Современные исследования сферы обеспечения безопасности отражают практическую и теоретическую обеспокоенность развитием и применением современных цифровых технологий в системах национальной безопасности. Несмотря на увеличение интереса, а также публичную заинтересованность в вопросах технологических изменений систем национальной безопасности практически отсутствовало понимание того, как именно происходят указанные изменения.

Основной результат настоящего исследования –теоретическое рассмотрение трансформации безопасности, опосредованной политикой цифровизации, и эмпирическое измерение элементов такой трансформации с реконструкцией динамики изменений и их последствий.

На теоретическом уровне:

1. Предложен содержательный анализ преобразований политики цифровизации и области безопасности. Мы представляем углубленный и широкий анализ изменений и эффектов, которые формируют указанную трансформацию. Так, безопасность наполняется и насыщается новыми феноменами (начиная от конкретных направлений, например, кибербезопасность, заканчивая процессами, которые пронизывают всю систему безопасности, такими как цифровизация). Расширяются область безопасности и концептуализация угроз.
2. Проблемы безопасности являются политическими проблемами, т.к. (1) происходит содержательное наполнение того *как* и *что* понимается под безопасностью; а также самой концептуализации угроз как продукта деятельности политических акторов; (2) безопасность функционирует за счет политических институтов, а качество и «условия» безопасности зависят от качества и взаимодействия институтов.

3. Феномен цифровизации является политическим процессом. Такой процесс подчинен принимаемым политическим решениям, и сопряжен (и зависит) от применения конкретных типов цифровых технологий.
4. В социальных и политических исследованиях допустимо рассмотрение «зонтичных» понятий, определяющих совокупность подходов, инструментов, факторов и функций феномена. Работа основана на понимании технологии искусственного интеллекта как алгоритмических и компьютерных систем (в том числе программное обеспечение и/или оборудование), которые, обучаясь, могут решать сложные проблемы, делать прогнозы или выполнять задачи, требующие человеческого восприятия, познавать, планировать, обучаться, общаться или совершать физическое действие, причем обязательно в сфере обеспечения безопасности или непосредственно в военной сфере.

На эмпирическом уровне:

1. Выделены страны-лидеры цифровизации (например, Финляндия, Германия и Швеция) и демонстрируется международная конкуренция в области цифровизации (при помощи сетевого анализа). Сетевая структура позволяет выделять страны, которые являются ключевыми звеньями международной торговли ИКТ и цифровыми технологиями и услугами.
2. Предлагается валидизированная эмпирическая модель изучения изменений и оценки системы безопасности государств под влиянием цифровых технологий. Влияние технологии в сфере национальной безопасности представляется в виде процесса принятия решений в сфере обеспечения безопасности. Показатель согласованности (консистентности) безопасности отражает то, как государство оценивает угрозы (показатель угроз), а также то, обладает ли государство необходимым уровнем возможностей для их отражения (показатель возможностей). Предлагаемый подход подразумевается, как дополнение к существующим и позволяет взглянуть на динамику развития системы безопасности конкретного государства под влиянием технологий.
3. Сравнительный анализ моделей стран показывает, что:

   3.1 правительства в целом единообразно подходят к определению возможностей технологии ИИ в вопросах безопасности (как на уровне политического процесса и принимаемых решений, так и на уровне институционального закрепления);

   3.2 постоянное накопление знаний и опыта о потенциале технологии приводит к систематическому увеличению возможностей технологий в вопросах безопасности;

3.3 развивается конкуренция между странами, а также наблюдается единообразие подходов к политическому контролю и нормативному закреплению технологий в области безопасности (на выборке пяти стран);

3.4 политические решения по регламентации технологии ИИ происходит единообразно и в сходные временные промежутки (все анализируемые страны приняли соответствующие стратегии в период двух лет: 2017–2019 гг.). Указанное может свидетельствовать о единообразии в политизации и секьюритизации технологий.

4. Динамика изменений систем национальных безопасности нелинейна. Волнообразный характер динамики отражает различия в адаптивности политических институтов и разнообразие политических решений в вопросах применения технологий в сфере безопасности. Несмотря на то, что все анализируемые страны максимизируют возможности применения цифровых технологий в сферах национальной безопасности, оценка угроз неоднородна и может меняться в каждой стране. Указанное, с одной стороны, иллюстрирует специфику самих цифровых технологий, – сложности с оценкой потенциала угроз и возможностей, технические вызовы и пр. С другой – позволяет утверждать, что само понимание угроз от страны к стране может сильно меняться, как и конкретная угроза может пересматриваться даже в рамках одного государства с течением времени.
5. Государства (правительства) адаптируются к современным технологическим вызовами в сфере безопасности. Государства определяют роль и место технологий соразмерно потенциалу возможностей, т.е. адаптируются к современным вызовам и преобразовывают национальную безопасность, интегрируя технологии. Государства сконструировали систему безопасности таким образом, что возможности реагирования превосходят оцениваемые угрозы. Более широкая интерпретация результатов позволяет предположить, что преобразования в системах безопасности полностью контролируются государствами.

В нашем исследовании мы продемонстрировали непосредственную динамику изменений сферы обеспечения безопасности под влиянием технологий цифровизации и автоматизации на примере конкретного типа цифровых технологий – искусственного интеллекта. С методологической точки зрения, нами предпринята попытка выстроить единую системную работу, привлекая методологические основы теории рационального

выбора (по отношению к политическим акторам), институционализма[81], современные подходы школы критического исследования безопасности и общие подходы логического моделирования Таагеперы. При этом мы стремимся расширить методологические возможности, поэтому не отрицаем ценность экспертного знания, а дополняем его количественным подходом.

Результатом работы стала демонстрация динамики изменений сферы безопасности под влиянием технологии цифровизации и автоматизации при помощи разработанной и апробированной эмпирической модели. Таким образом, на теоретическом уровне мы продемонстрировали непосредственные изменения и эффекты трансформации. Результаты подкрепляют существующую литературу о политизации и секьюритизации технологий в сфере безопасности, неоднородном восприятии угроз правительствами разных стран, частично подтверждают существование милитаризации технологий и, косвенно, иллюстрируют подчинение развития (development) сфере обеспечения безопасности. При этом мы фиксируем и уникальные результаты, в числе которых тезис о нелинейности динамики систем национальной безопасности правительств разных стран, а также выделение конкретных особенностей национальных политик в области безопасности и отношений политической воли к технологическим изменениям.

Результаты сравнительного анализа позволяют выявить лучшие практики адаптации правительств и изменений системы безопасности к изменениям, сопряженным с цифровыми технологиями. Во-первых, страны с более развитым государственно-частным партнерством демонстрируют лучшие результаты. Политические и институциональные возможности привлечения технологических наработок от частных компаний и стартапов позволяют лучше адаптироваться к изменениям и демонстрировать более согласованную систему безопасности. Подтверждением этого является опыт разных стран в применении технологий двойного назначения (первоначально технологические разработки ориентированы на гражданское применение и развиваются частными компаниями, в последующем эти разработки получают применение в сфере безопасности). Во-вторых, сбалансированный подход к приобретению технологий и национальной разработке позволяет достигать более качественных результатов в сфере безопасности. Так, адаптация Швецией лучших

[81] Повторимся, мы не просто опираемся на классическое «институты имеют значение», а рассматриваем их широко, как правила и нормативные представления политической воли. Оставаясь в предметном поле политической науки, мы подходим к институтам как содержательным проявлениям политики. При этом, не рационализируя сам институт, давая «возможность» существованию неформальных форм институционального проявления и отождествления власти в вопросах безопасности

практик и технологических процессов за счет сети торговых связей, а также самостоятельное стимулирование и поддержка национальных разработок позволяют ей демонстрировать лидирующие позиции по результатам сетевого анализа, а также высокие показатели эмпирической модели. Таким образом, исключительная политика импортозамещения или «слепая вера» в приобретение технологий за рубежом не позволит сбалансировать и адаптировать систему безопасности страны. В-третьих, страны, активно вовлеченные в международные связи (как на уровне торговых операций, продемонстрированных сетевым анализом, так и на уровне блоков и наднациональных организаций, и широкой сети вовлекаемых экспертов) и демонстрирующие политическую волю институциональной и политической унификации правил и норм, достигают более высоких результатов. Сотрудничество в рамках блока (НАТО, ЕС) позволяет более системно и широко рассмотреть потенциал возможностей и риски, связанные с технологиями. В свою очередь, вовлечение экспертов и сильные торговые связи позволяют на практике оценивать эффекты цифровизации в вопросах безопасности. При этом если качество и взаимодействие институтов в государстве позволяет адаптироваться к таким изменениям, сфера национальной безопасности соразмерно и сбалансированно меняется, применяя цифровые технологии.

На инструментальном (методологическом) уровне разработана, протестирована и валидизирована эмпирическая модель изменений и оценки системы безопасности государства под влиянием цифровых технологий (на примере технологии ИИ). Разработанная модель позволяет оценивать системы безопасности как по показателю угроз (как правительства определяют и оценивают угрозы), так и по показателю возможностей технологии (как правительства определяют потенциал и возможности применения).

Применение разработанной модели позволяет не только расширить существующие дискуссии, но и заполнить некоторые лакуны. Так, анализ динамики изменений позволяет утверждать, что правительства относятся к технологиям более прагматично, поэтому большинство академических опасений скорее излишни. Несмотря на различия среди государств в понимании и применении технологий, а также волнообразную динамику, это не влечет за собой существенных проблем в системах национальной безопасности стран. Другой важный результат отражает не просто возникновение, а активное развитие конкуренции среди государств в вопросах технологии искусственного интеллекта. Причем, такая конкуренция проявляется не

просто в «привычных» сферах международной торговли, геополитики и пр., а напрямую в вопросах безопасности. В свою очередь, масштабированность разработанной модели позволяет в будущем оценивать системы национальной безопасности стран относительно любого иного типа цифровых технологий.

Дальнейшие направления исследований с применением теоретических и инструментальных (методологических) наработок данного исследования могут касаться как тематики data-driven, а именно включение новых данных (относительно различных типов цифровых технологий) в предметное поле исследований безопасности, так и в рамках сравнительной парадигмы политической науки. Во-первых, можно расширить границы исследования и посмотреть на связи динамики систем национальной безопасности относительно цифровых технологий с режимными вариациями. Иными словами, одним из последующих направлений может стать сравнительный анализ моделей стран с разными режимными маркерами. Речь идет не просто о сравнении «автократии» против «демократий», а учет большего режимного спектра, как минимум на основе типологии V-Dem рассмотреть четыре страны с разными режимными характеристиками (либеральная демократия, электоральная демократия, электоральная автократия, закрытая автократия). Во-вторых, применение модели с различными типами цифровых технологий потребует разработки системной модели, которая будет оценивать систему безопасности не относительно одного типа технологий, а в общности различных типов. Такая модель позволит посмотреть на динамику систем безопасности стран более комплексно и в общей увязке с реализацией стратегий цифровизации и автоматизации. В-третьих, со временем потребуется дополнительное построение модели, чтобы отследить изменения последующие после 2019 г. Также интересным направлении может стать построение уже прогностических моделей, на основе имеющейся оценочной. Прогностические модели расширят наше понимание трансформационного эффекта технологий, а также позволят более обоснованно подходить как к практическому планированию технологического воздействия, так и к улучшению политического воздействия.

В качестве самостоятельно задела для будущих исследований возможно расширить концептуализацию технологии ИИ. Для этого возможно произвести анализ научных публикаций (с ключевыми словами тематики ИИ) с вычленением аннотаций и ключевых слов из каждой статьи. На созданном массиве текстов далее можно произвести количественный тематический анализ (topic modelling), параллельно проведя страновую аффилиацию авторов статей. Такой анализ позволит выявить как

конкретные темы (топики) современного понимания технологии, так и установить страны (через аффилиацию авторов), имеющие наибольший интеллектуальный и научный потенциал для развития технологии ИИ. В совокупности это позволит дополнительно проверить и выявить пул стран, занимающих лидирующие позиции в вопросах развития технологии ИИ. Более того, результаты моделирования позволят соотнести и сравнить условные «позиции» стран с имеющимися результатами сетевого анализа. Самостоятельным результатом такого исследований будет выступать более широкая концептуализация понимания технологии искусственного интеллекта.