Федеральное государственное образовательное бюджетное учреждение
высшего образования
«Финансовый университет при Правительстве Российской Федерации»

На правах рукописи

Ковригин Дмитрий Эльдарович

СОГЛАСОВАНИЕ ИНТЕРЕСОВ ГОСУДАРСТВА И БИЗНЕСА В ОБЕСПЕЧЕНИИ УСТОЙЧИВОСТИ РОССИЙСКОГО СЕГМЕНТА КИБЕРПРОСТРАНСТВА

5.5.2. Политические институты, процессы, технологии

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата политических наук

Научный руководитель — Расторгуев Сергей Викторович,
доктор политических наук, доцент

Москва – 2025

Диссертация представлена к публичному рассмотрению и защите в порядке, установленном ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации» в соответствии с предоставленным правом самостоятельно присуждать ученые степени кандидата наук, ученые степени доктора наук согласно положениям пункта 3.1 статьи 4 Федерального закона от 23 августа 1996 г. № 127-ФЗ «О науке и государственной научно-технической политике».

Публичное рассмотрение и защита диссертации состоятся 5 февраля 2026 г. в 14:00 часов на заседании диссертационного совета Финансового университета Д 505.001.123 по адресу: Москва, Ленинградский проспект, д. 49/2, аудитория 406.

С диссертацией можно ознакомиться в диссертационном зале Библиотечно-информационного комплекса ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации» по адресу: 125167, Москва, Ленинградский проспект, д. 49/2, комн. 100 и на официальном сайте Финансового университета в информационно-телекоммуникационной сети «Интернет» по адресу: www.fa.ru.

Персональный состав диссертационного совета:

председатель – Расторгуев С.В., д.полит.н., доцент;
заместитель председателя – Домбровская А.Ю., д.социол.н.;
ученый секретарь – Данилова Е.А., д.полит.н., доцент;

члены диссертационного совета:

Бродовская Е.В., д.полит.н., профессор;
Володенков С.В., д.полит.н., профессор;
Карсанова Е.С., д.полит.н., доцент;
Манойло А.В., д.полит.н.;
Митрофанова А.В., д.полит.н.;
Пляйс Я.А., д.полит.н., д.ист.н., профессор;
Пушкарева Г.В., д.полит.н., профессор;
Селезнев П.С., д.полит.н., доцент;
Соловьев А.И., д.полит.н., профессор.

Автореферат диссертации разослан 26 ноября 2025 г.

Ученый секретарь диссертационного совета
Финансового университета Д 505.001.123 Е.А. Данилова

I Общая характеристика работы

Актуальность темы исследования. На современном этапе человеческая цивилизация переживает скачок технологического развития в сфере информационно-коммуникационных технологий. Благодаря им люди получили широкие возможности обмена информацией практически в любых точках мира. Данные возможности затрагивают все сферы жизни общества, в связи с этим происходит трансформация и модернизация институтов общества и государства, появляются новые институты. Образованное в процессе развития технологий, коммуникаций киберпространство стало новой площадкой для человеческих взаимодействий. Параллельно с тем, как ИТ-технологии все больше влияют на жизнь общества, происходит трансформация и создание новых политических пространств и экономических рынков в условиях очередного этапа поляризации мира. Внутренняя и внешняя политика крупных геополитических акторов оказывает влияние на стратегию развития ИТ-компаний посредством целеполагания и ресурсного обеспечения в приоритетных направлениях деятельности. Влияние политического фактора на экономику сектора высоких технологий ярко проявилось в условиях санкций после начала специальной военной операции России на Украине (далее – СВО) в 2022 году.

Любое государство стремится обеспечить главенство законодательства на своей территории, в связи с этим киберпространство все более и более подвергается законодательному и технологическому регулированию. Поскольку ни одно государство в силу технических причин не может объявить все интернет-пространство подконтрольной ему зоной, страны стараются обеспечить контроль и безопасность своих национальных сегментов киберпространства. Киберпространство становится все более сегментированным на регуляторные зоны, поскольку государства устанавливают свою юрисдикцию, технические ограничения, информационные фильтры. Необходимость контроля над киберпространством обусловлена стремлением государств предотвратить риски криминала, терроризма, экстремизма, сепаратизма, протестных настроений и угрозы вмешательства во внутренние дела, распространения ценностей, противоречащих официально одобряемым и исторически сложившимся типам ценностных ориентаций. Информационные и гибридные войны в киберпространстве стали реальными формами

противостояния в XXI веке, интенсивность и масштаб данных войн демонстрируют тенденцию к увеличению.

Поэтому вполне естественно, что государства стремятся обеспечить безопасность своего сегмента киберпространства. Для Российской Федерации данная проблема стоит особенно остро. После начала специальной военной операции Россия столкнулась с беспрецедентным уровнем кибератак, пропагандистского давления, а также с санкциями, ставящими под угрозу развитие отечественного сегмента киберпространства и сферы информационно-коммуникационных технологий (далее – ИКТ). Развитие суверенного киберпространства - это необходимый шаг для России в целях достижения стабильности и безопасности. Для этого наряду с законодательным регулированием государства поддерживают свой сегмент киберпространства в информационном и техническом плане. Эффективность взаимодействия государства и бизнеса, максимально удовлетворяющая интересы обеих сторон, играет ключевую роль в том, насколько быстро и результативно будет выстроена система, обеспечивающая устойчивость киберпространства страны.

Исходя из вышесказанного, представляется целесообразным провести анализ взаимодействия государства и ИТ-бизнеса в условиях борьбы со странами коллективного Запада за суверенитет и устойчивость национального сегмента киберпространства, определить наиболее вероятные стратегии деятельности государства и ИТ-бизнеса с учетом сложившихся ресурсных ограничений и интересов.

Степень разработанности темы исследования. Проблематика исследуемой темы нашла отражение в работах, которые можно разделить на следующие группы.

К первой группе относятся труды, в которых раскрыты основные принципы системного подхода, среди них выделяются работы Т. Парсонса, Н. Лумана, Д. Истона, Г. Алмонда, Г.Б. Клейнера. Теоретические основы неоинституционального подхода отражены в работах Д. Норта, Г. О'Доннелла, Р. Коуза, Г. Питерса, Ю.В. Ирхина, Дж. Олсена и Дж. Марча. Концептуальные рамки теории полей разработаны П. Бурдье и нашли свое продолжение в работах Н. Флигстина и Д. Макадама.

Работы второй группы отражают используемый в диссертации методологический инструментарий и понятийный аппарат теории игр, разработанный такими учеными, как Дж.М. Смит, Дж. Нэш, Дж. Нейман, Р. Льюс и Х. Райф, А. Раппопорт, Т. Шеллинг, Л. Шепли.

Третья группа работ состоит из исследований групп интересов, представленных работами А. Бентли, Д. Трумэна, А.В. Павроза и С.В. Расторгуева. Концепция неокорпоративизма на зарубежном материале представлена в работах Ф. Шмиттера, Дж. Лембруха, К. Каусона, Е. Талоса, Г. Кроуча. Среди отечественных авторов проблематика неокорпоративизма отражена в работах А.Ю. Зудина, О.В. Гаман-Голутвиной, С.П. Перегудова, А.В. Павроза, С.Г. Кордонского, О.Э. Бессоновой, О.В. Крыштановской. Теория общественного выбора разработана в трудах Дж. Бьюкенена.

К четвертой группе относится литература, раскрывающая вопросы устойчивого развития систем, в нее входят работы Р.И. Захарченко и И.Д. Королева, О.Ф. Шаброва, С.Э. Хайкина, вопросы киберустойчивости анализируются в работах Ю. Кукола.

В пятую группу входит литература, анализирующая тематику развития киберсреды и киберпространства, представленная работами Д. Кларка, Л.В. Терентьевой, С.В. Петровского, А.А. Максурова, В.М. Розина, Д. Ланира, А.А. Печникова, В.В. Вихмана и М.В. Ромма, Г.В Верховой и С.В. Акимова; сюжетная проблематика информационного пространства отражена в работах С.В. Володенкова, В.Л. Гирич и В.Н. Чуприной, А.В. Манойло, И.А. Добровольской, И.М. Дзялошинского В.А. Филиппова. Вопросы регулирования киберпространства представлены в работах Д. Басселла и Т. Стивенса, К. Флойда и П. Перника, А.А. Данельяна, диссертационных исследованиях А.В. Алагоз, И.А. Бабюк, Д.Р. Мухаметова, Э.Т. Есиева. Цифровые коммуникации и платформы в России, проблемы их развития на современном этапе исследованы в трудах Е.В. Бродовской, А.Ю. Домбровской, Р.В. Пармы, С.Г. Ушкина.

К шестой группе относятся работы А.В. Даниленкова, А. Епифановой, В.Б. Наумова, Д.В. Красикова, Ю. Кол, К. Айкенсера, Н. Цагуриаса, исследующие проблематику суверенитета государства в информационно-телекоммуникационной сфере. Проблема технологического суверенитета представлена в работах В.В. Иванова. Политические конфликты в формате гибридных и информационных войн изучены в работах С.В. Володенкова, Н. Мэттиса и Ф.Г. Хоффмана, В.А. Артамонова и Е.В. Артамоновой, Ю.Ю. Першина, В.Б. Вепринцева, А.В. Манойло, А.И. Петренко, Д.Б. Фролова, В.В. Митевой, Д. Аркилла и Д. Ронфельдта, Р.А. Кларка.

Анализ современных диссертационных исследований по тематике взаимодействия государства и бизнеса в сфере ИКТ, устойчивости киберпространства показал следующее. Основной точкой фокуса являются: проблематика коммуникации политических субъектов в киберпространстве, анализ социальных и политических аспектов цифровизации системы единой публичной власти в Российской Федерации, роль виртуальных технологий в конфликтной мобилизации в интернет-пространстве и противодействие ей, роль государства в трансформации экосистемы цифровой экономики. Меньше внимания уделяется исследованию влияния политического пространства на киберпространство.

В результате анализа вышеуказанных работ российских и зарубежных авторов можно определить поле исследования, недостаточно изученное политической наукой - стратегии взаимодействия российского государства и ИТ-бизнеса в условиях масштабного геополитического противостояния и их влияние на устойчивость национального сегмента киберпространства.

Цель исследования заключается в выявлении особенностей и объяснении стратегий согласования политических интересов российского государства и бизнеса в ИТ-сфере, обеспечивающих устойчивость российского сегмента киберпространства.

Для достижения поставленной цели поставлены следующие **задачи**:

- систематизировать конгруэнтные современным российским условиям теоретические основы исследования взаимодействия государства и бизнеса;

- определить теоретические основы исследования политики по обеспечению устойчивости инфраструктуры национального сегмента киберпространства;

- выявить реакцию политических и экономических акторов, формирующих национальный сегмент киберпространства, на социально-политические вызовы 2020–2024 гг.;

- выявить стратегии государства и бизнеса ИТ-сферы в инфраструктуре национального сегмента киберпространства и их согласованность;

- оценить результативность действующих стратегий согласования интересов при взаимодействии российского государства и компаний ИТ-сферы с точки зрения достижения устойчивости российского сегмента киберпространства;

- определить перспективы конгруэнтности стратегий органов государственной власти и ИТ-бизнеса в условиях внешних вызовов.

Объект исследования – политическое взаимодействие российского государства и бизнеса ИТ-сферы.

Предмет исследования - стратегии согласования политических интересов при взаимодействии государственной власти Российской Федерации с компаниями в ИТ-сфере как ключевых акторов формирования устойчивости инфраструктуры национального сегмента киберпространства.

Гипотеза исследования. Устойчивость российского сегмента киберпространства является результатом согласования политических интересов государственной власти и бизнеса, представленных конгруэнтными стратегиями акторов.

Область исследования диссертации соответствует п. 4. «Механизмы и технологии традиционной и цифровой политики: формы и уровни организации», п. 19. «Глобализация, сетевизация и цифровизация: политические аспекты» Паспорта научной специальности 5.5.2. Политические институты, процессы, технологии (политические науки).

Нормативно-правовая база исследования:

- Нормативно-правовые акты Российской Федерации, информация с сайтов государственных органов власти, касающаяся вопросов регулирования сферы информационных технологий.

- Нормативно-правовые акты зарубежных государств, содержащие информацию по антироссийским санкциям.

Эмпирическая база исследования основана на следующих источниках:

- Данные системы «СПАРК-Интерфакс» по финансовой, налоговой отчетности компаний сферы информационных технологий, структуре собственности, участию в выполнении государственных заказов, арбитражном судопроизводстве, позволяющие проанализировать динамику хозяйственной деятельности в условиях политических вызовов.

- Данные информационных агентств, аналитических центров, связанные с вопросами взаимодействия государства и бизнеса в национальном сегменте киберпространства.

- Официальная информации органов власти, материалы зарубежных исследований по формированию цифрового суверенитета иностранными государствами (КНР, Индия, Австралия, Вьетнам, ЮАР, Великобритания, США, страны Евросоюза).

Хронологические рамки исследования фокусируются на периоде с 2020 г. по 2024 г., что обусловлено необходимостью определения стратегий государства и бизнеса сферы ИТ, способов согласования интересов, оценки устойчивости национального сегмента киберпространства в период до начала СВО и в период СВО.

Ограничения исследования определяются закрытостью части источников, содержащих информацию по ряду аспектов деятельности органов государственной власти и бизнеса, направленных на преодоление последствий антироссийских санкций недружественных государств.

Научная новизна исследования представлена следующими положениями:

1) Обоснована авторская методика исследования взаимодействия поля государства и поля бизнеса на основе конвертации полученных количественных и качественных результатов в матрицу исходов стратегий теории игр и стратегическую матрицу SWOT.

2) Определены рамки реконфигурации основных политических и экономических акторов, обеспечивающих материальную основу национального сегмента киберпространства под влиянием внешнеполитических вызовов, зафиксирован положительный результат (достаточная конгруэнтность) действующих стратегий согласования интересов государства и бизнеса в достижении устойчивости российского сегмента киберпространства текущего периода.

3) Автором предложено сочетание «стратегии развития» со стороны государства и «стратегии развития» со стороны ИТ-бизнеса как оптимальной, Парето-эффективной, равновесной по Нэшу стратегии взаимодействия российского государства и бизнеса в сфере программного обеспечения (далее – ПО) для достижения устойчивости национального сегмента киберпространства.

4) Автором предложено сочетание «стратегии развития» со стороны государства и «стратегии выживания» со стороны ИТ-бизнеса как оптимальной, Парето-эффективной и равновесной по Нэшу стратегии взаимодействия российского государства и бизнеса в сфере аппаратного обеспечения (далее – АО) для достижения устойчивости национального сегмента киберпространства.

5) В условиях среднесрочных внутриполитических и долгосрочных внешнеполитических трендов автором предложено сочетание экспансионистского вида цифрового суверенитета и государственноцентричной стратегии согласования интересов государства и бизнеса ИТ-сферы.

Теоретическая значимость работы заключается в развитии теории о выстраивании адекватных внешним вызовам способов согласования политических интересов государства и бизнеса для устойчивого функционирования инфраструктуры отечественного сегмента киберпространства. Итоги исследования позволяют уточнить научные представления об устойчивости российского сегмента киберпространства как совокупности состояний результирующих векторов политических и экономических взаимодействий. Исследование вносит вклад в развитие понятийно-терминологического аппарата: национальный сегмент киберпространства, устойчивость национального сегмента киберпространства.

Практическая значимость работы заключается в том, что выводы, сделанные в ходе исследования, могут быть использованы акторами политического и экономического поля для оптимизации процессов согласования интересов, способствующих укреплению устойчивости российского сегмента киберпространства.

Методология и методы исследования. Работа строится на постулатах и концептах системного подхода, рассматривающего политическую и экономическую сферы жизни общества как взаимодействующие системы (Т. Парсонс, Н. Луман, Д. Истон, Г. Алмонд, Г.Б. Клейнер, О.Ф. Шабров). Неоинституциональный подход использовался при исследовании развития институтов (правил игры), механизмов соблюдения контрактов при взаимодействии политической власти и бизнеса (Д. Норт, Г. О'Доннелл, Р. Коуз, Г. Питерс, Дж. Олсен и Дж. Марч, Ю.В. Ирхин).

Теоретический фундамент исследования базируется на:

- концепции полей П. Бурдье, новой концепции полей Н. Флигстина и Д. Макадама, анализирующих определенные сферы деятельности как взаимодействия иерархизированных акторов, обменивающихся ресурсами;

- концепции неокорпоративизма Ф. Шмиттера, акцентирующей центральную роль государства в выстраивании иерархически подчиненных полей бизнеса и политики, а также работ отечественных авторов, исследующих неокорпоративистские практики взаимодействия государства и бизнеса в России (А.Ю. Зудин, О.В. Гаман-Голутвина, С.П. Перегудов, А.В. Павроз, С.Г. Кордонский, О.Э. Бессонова, О.В. Крыштановская);

- концепции киберпространства как специфического поля информационной коммуникации в сети интернет, требующего поддержания технологической инфраструктуры, спецификации прав собственности и законодательного регулирования (Дж. Басселл, Д. Кларк, А.В. Манойло).

Эмпирическое исследование проводилось на основе общенаучных и специальных методов. К первой группе относятся: анализ и синтез, индукция и дедукция, исторический и логический методы. Ко второй группе относятся:

- статистический метод расчета среднеарифметической величины, который применялся для анализа экономических показателей компаний сектора ИКТ, баланса импорта и импортозамещения, динамики подготовки кадров и позволил сделать выводы о степени устойчивости инфраструктуры российского сегмента киберпространства;

- теория игр позволила проанализировать кооперативное взаимодействие акторов политической и экономической сферы для максимизации своих выигрышей, что создает разнообразные точки равновесия, определяющие, с одной стороны, удовлетворение интересов акторов, с другой стороны, степень устойчивости национального сегмента киберпространства;

- SWOT-анализ через модель пяти сил Портера применялся в процессе оценки перспектив развития российского сегмента ИТ-сферы, государственной политики по регулированию национального сегмента киберпространства;

- методика ресурсно-акторного анализа использовалась при изучении взаимодействия государственных акторов с акторами бизнеса в вопросах реализации практик, направленных на достижение интересов каждой из сторон интеракций.

Личный вклад автора. Автор участвовал в определении композиции исследования, принял участие в обсуждении результатов диссертации, написании статей, тезисов и докладов. Проводился анализ взаимодействия государственной власти Российской Федерации и бизнеса в сфере ИТ, а также осуществлялась разработка оптимальных сочетаний стратегий их взаимодействия. Все результаты работы получены лично автором.

Положения, выносимые на защиту:

1) Разработанная автором методика исследования, основанная на конвертации полученных количественных и качественных результатов в матрицу исходов стратегий теории игр, является релевантной для изучения особенностей и объяснения стратегий согласования политических интересов государства и бизнеса в современной России. Автором предложено и обосновано определение «киберпространства» как созданной для обмена информацией гибридной площадки (платформы), формируемой из совокупности всех информационных устройств, хранящих, обрабатывающих, передающих информацию и задействованных в

функционировании сети интернет, а также субъектов коммуникационных, технологических, регуляторных процессов (С. 48; 61; 64-70).

2) В условиях геополитического кризиса можно обозначить три варианта стратегии взаимодействия государства и бизнеса: стратегия зависимости; стратегия выживания; стратегия развития. Отечественные компании производители ПО в достаточной степени обладают ресурсами и компетенциями, а с учетом государственной поддержки и ограничительных мер на использование иностранного ПО государственными органами и объектами критической инфраструктуры выступают драйверами роста. Для российского государства и бизнеса в сфере ПО наиболее выгодным будет сочетание стратегий развития, направленных на реализацию имеющегося потенциала. Парето-эффективной стратегией является выбор «стратегия развития – стратегия развития». При этом данная стратегия является равновесием Нэша: односторонняя смена стратегии любым актором только ухудшает положение игрока (С. 52-54; 88-89; 95-96).

3) Отечественные компании производители АО не обладают достаточными ресурсами и компетенциями, что приводит к значительной зависимости от зарубежных компаний или импорта товаров. Несмотря на меры государственной поддержки, производители АО не показывают успехов в импортозамещении. Для устойчивости отечественного сегмента киберпространства оптимальным представляется сочетание стратегии развития со стороны государства и стратегии выживания со стороны российских компаний в сфере АО. Данная конфигурация стратегий обладает характеристиками Парето-эффективности и равновесности по Нэшу (С. 96-98; 107-109).

4) Решающими факторами маркирования границ национального сегмента киберпространства и достижения цифрового суверенитета как составного элемента государственного суверенитета являются политический выбор правящих элит и технологические возможности страны. В свою очередь, технологические возможности определяются, прежде всего, наличием компетентных и ресурсных отечественных фирм по производству ПО, АО, квалифицированных кадров, степенью включенности (исключенности) в глобальные цепочки обмена товарами и услугами. Можно выделить следующие виды цифрового суверенитета: оборонительный; экспансионистский, нормативный, постколониальный, гегемонистский. Можно выделить три стратегии согласования интересов государства и бизнеса ИТ-сектора, обеспечивающих суверенитет и устойчивость национального сегмента киберпространства:

а) максимальный государственный контроль с опорой на отечественные компании ИТ-сектора; б) распределение контроля между интегрированными государствами (одним государством) и западными ТНК; в) сильные отечественные ТНК ИТ-сектора активно участвуют в осуществлении контроля и гарантируют функционирование инфраструктуры киберпространства при умеренном участии государства (С. 134-135).

5) Основными факторами силы российского сегмента киберпространства являются политические факторы, а среди слабостей, прежде всего, доминируют экономические факторы. Также весьма значительна роль внешнеполитического фактора антироссийских санкций. Поле возможностей в равной степени представлено политическими и экономическими факторами, среди угроз доминируют политические факторы. Перспективы развития российского сегмента киберпространства характеризуются как нестрогое неравенство с незначительным преимуществом суммы сил и возможностей над слабостями и угрозами. Результаты SWOT-анализа показывают реальную возможность достижения устойчивости российского сегмента киберпространства на основе конгруэнтности стратегий государства и бизнеса в сфере ПО и АО (С. 145-146).

6) Согласование политических интересов государства и бизнеса в национальном сегменте киберпространства определяется конгруэнтностью стратегий действий органов государственной власти и компаний ИТ-сектора. Современный курс российской политической элиты в сочетании с уровнем развития ИТ-сектора обусловливают выбор экспансионистского вида цифрового суверенитета и первой стратегии (стратегии «а») согласования интересов государства и бизнеса ИТ-сектора. Основным интересом государства является максимальная «национализация» инфраструктуры российского сегмента для обеспечения национальной безопасности. Результатом согласования взаимных интересов органов государственной власти и бизнеса является устойчивость национального сегмента киберпространства (С. 136-138).

Степень достоверности, апробация и внедрение результатов исследования. Результаты и основные положения диссертации обладают подтвержденной степенью достоверности. Использованные методы научного исследования являются объективными и логичными. Корректно использованы исходные данные справочных источников, специальной научной литературы, законодательных баз, эмпирических данных, которые составлены на основе данных наиболее крупных ИТ компаний России.

Основные положения диссертационного исследования были представлены в докладах и выступлениях на следующих конференциях: на XXX Международной конференции студентов, аспирантов и молодых ученых «Ломоносов» в рамках Международного молодежного научного форума «Ломоносов» (Москва, МГУ имени М.В. Ломоносова, 10-21 апреля 2023 г.); на LVIII Международной научно-практической конференции «EURASIASCIENCE» (Москва, Научно-издательский центр «Актуальность.РФ», 30-31 декабря 2023 г.); на XIV Международной научно-практической конференции «Россия и мир: развитие цивилизаций. Мир, страна, университет - 25 лет развития» (Москва, УМЦ имени В.В. Жириновского, 3-4 апреля 2024 г.); на XIX Всероссийской (с международным участием) научной конференции студентов, магистрантов, аспирантов и молодых ученых «Миры прошлого и настоящего на переломе эпох: исследовательские подходы и практики» (г. Томск, Томский государственный университет, 16-18 апреля 2024 г.); на Всероссийском XV молодёжном научном форуме МТУСИ «Телекоммуникации и информационные технологии-реалии, возможности, перспективы» (Москва, МТУСИ, 1-20 апреля 2024 г.).

Результаты диссертационного исследования используются в практической деятельности АО «Микояновская слобода». Ключевые выводы и положения диссертационного исследования стратегий взаимодействия власти и бизнеса, а также обоснованная методика исследования взаимодействия поля государства и поля бизнеса используется в работе организации. По материалам исследования внедрен комплекс количественных и качественных показателей, а также методика их оценки, позволяющая эффективно определять наиболее выгодные стратегии взаимодействия власти и бизнеса в условиях геополитического кризиса. Предложенные системы показателей оценки состояния компаний используются при анализе конкурирующих организаций. Выводы и основные положения диссертации используются в практической работе организации и способствуют повышению эффективности ее деятельности.

Материалы диссертации используются Кафедрой политологии Факультета социальных наук и массовых коммуникаций Финансового университета в преподавании учебных дисциплин «Теория и методология политической науки», «Моделирование и прогнозирование социально-политических процессов по цифровым следам», «Цифровые политические инструменты и технологии».

Публикации. Основные положения диссертации отражены в 5 публикациях общим объемом 2,65 п.л. (весь объем авторский), опубликованных в рецензируемых научных изданиях, определенных ВАК при Минобрнауки России.

Структура и объем диссертации. Диссертация состоит из введения, трех глав, заключения, списка литературы из 242 наименований и 9 приложений. Текст диссертации изложен на 265 страницах, содержит 38 таблиц и 14 рисунков.

II Основное содержание работы

Во введении обоснована актуальность темы исследования, степень разработанности темы исследования, цель и задачи исследования, объект исследования, предмет исследования, проблема исследовании, область исследования, эмпирическая база исследования, степень достоверности, апробация и внедрение результатов исследования.

Первая глава **«Теоретико-методологические основы исследования взаимодействия государства и бизнеса»** содержит обоснование категориального аппарата работы, авторские определения используемых терминов, анализ методологических подходов и релевантных цели исследования концепций, методов исследования, схему структурной операционализации.

В первом параграфе первой главы **«Теоретические основы исследования согласования интересов государства и бизнеса в обеспечении устойчивости российского сегмента киберпространства»** структурирована теоретическая концепция исследования взаимодействия власти и бизнеса на основе концепций полей, групп интересов. Государство является иерархией полей и выполняет функции инициирования появления новых полей, управления всей совокупностью полей, формирования правил игры акторов, обеспечивая тем самым необходимую стабильность.

Описанная М. Портером система кластеров релевантна для представления сегмента производства и разработки аппаратного обеспечения. Концепция групп интересов применяется при рассмотрении государства и бизнеса как совокупности групп давления, что отражается в государственной политике. Группы интересов определяются как объединения по совместной реализации своих интересов.

Определено «киберпространство» как созданное для обмена информацией пространство, обладающее смешанным, гибридным характером. Оно формируется из

совокупности всех информационных устройств, задействованных в передаче, хранении и обработке информации, а также субъектов, задействованных в коммуникационных, технологических, регуляторных процессах. Российский сегмент киберпространства рассматривается как отдельная система, формируемая в результате взаимодействий органов государственной власти и компаний ИТ-сектора.

Определена устойчивость киберпространства как динамичное состояние процессов обмена ресурсами, обеспечиваемое за счет устойчивости подсистем, из которых оно состоит. Баланс взаимодействий государства и бизнеса в области производства аппаратного обеспечения, программного обеспечения, кадрового обеспечения ИТ-сферы (инфраструктура) создает состояние устойчивости национального сегмента киберпространства.

В работе для отечественного сегмента киберпространства применима модель «Патронажа», в которой государство обеспечивает поддержку бизнес-структур, чьи стратегии деятельности сочетаются с политическими целями. Для поддержания состояния устойчивости киберпространства государство обладает властным ресурсом, который используется для регулирования финансовых, технологических, кадровых, внешнеэкономических аспектов деятельности бизнеса.

На современном этапе развития одной из ведущих сфер, определяющих статус державы, стали информационные технологии. Государство как основной институт политической системы на своей территории стремится обеспечить соблюдение законодательства. Поскольку киберпространство является определенным типом пространства, то государство стремится его регулировать, также как и деятельность своих граждан, что необходимо в условиях развития гибридной, информационной и информационно-психологической войны.

Основные угрозы для национального сегмента киберпространства, исследуемые в диссертационном исследовании: санкции в сфере ИКТ, критическая зависимость инфраструктуры от импорта, нехватка квалифицированных кадров в сфере ИКТ.

Во втором параграфе первой главы **«Методология и методика изучения согласования интересов государства и бизнеса в обеспечении устойчивости российского сегмента киберпространства»** систематизирована методологическая основа исследования. Системный подход определен в качестве методологической основы исследования.

Определено, что в настоящем исследовании под государством понимаются органы государственной власти, непосредственно участвующие во взаимодействии с компаниями ИТ-сферы, а под «бизнесом» – наиболее крупные компании в сфере ИТ. Компании отобраны на основе рейтингов Аналитического центра «TAdviser», и данные по ним собраны в системе «Спарк-Интерфакс». Используется концепция неокорпоративизма как наиболее адекватно описывающая взаимодействие российского государства и иерархически подчиненных полей бизнеса. Для анализа взаимодействий используются методы статистического анализа, матриц теории игр (с определением равновесий по Парето и Нэшу), SWOT-анализа, методика ресурсно-акторного анализа.

Для достижения устойчивости киберпространства со стороны государства и бизнеса требуется множество взаимодействий правового, ресурсного, организационного, кадрового характера. Противоречия между государством и бизнесом связаны с фундаментальными проблемами целеполагания и перераспределения ограниченных ресурсов. Бизнес стремится увеличить свою прибыль. Государство как аппарат управления стремится к такому уровню контроля над экономическими субъектами и такому уровню изъятия/распределения ресурсов, которые бы позволили поддерживать и развивать все подсистемы общества.

Стратегии акторов процесса взаимодействия государства и бизнеса выстраиваются исходя из ожидаемых результатов и целей, возможностей/ресурсов актора, а также внешних условий. Выделены три типовые стратегии: стратегия зависимости, стратегия выживания, стратегия развития. Структурная операционализация «Показатель – Переменная – Индикатор» сделана под каждый специальный метод исследования. В ресурсно-акторном анализе в качестве переменных определены конкретные действия органов государственной власти, нацеленные на взаимодействие с бизнесом, а для бизнеса результаты хозяйственной деятельности. В матрице исходов стратегий определены индикаторы выигрышей и проигрышей каждого игрока. В SWOT-анализе в качестве индикаторов переменной представлен баланс сумм сил/возможностей и слабостей/угроз.

Вторая глава **«Взаимодействие государства и бизнеса в области информационных технологий»** содержит анализ взаимодействия органов государственной власти и бизнеса в различных сферах обеспечения российского сегмента киберпространства. Выделяются основные акторы взаимодействия данных групп в условиях геополитического противостояния. Для исследования выделяются

поля производителей программного обеспечения, производителей аппаратного обеспечения, также изучается проблематика подготовки кадров для ИТ-сектора. Каждое из полей обладает своими особыми характеристиками, групповыми интересами и, как следствие, стратегиями взаимодействия с полями государства.

В первом параграфе второй главы «**Ресурсы, акторы, стратегии взаимодействия государства и ИТ-бизнеса в контексте геополитических вызовов 2020–2024 гг.»** анализируются: инфраструктура российского сегмента киберпространства как отдельное поле (система); взаимодействие поля государства с инфраструктурными полями киберпространства; меры воздействия государства на ИТ-компании; лоббирующие интересы ИТ-бизнеса организации; цели и ресурсы акторов государства и бизнеса; показатели развития ИТ-сферы России в период с 2019 г. по 2023 г. в фокусе антикризисных политик органов государственной власти.

В российском ИТ-бизнесе действуют как отечественные частные и государственные компании, так и зарубежные компании. Российское государство является значимым игроком поля, так как формирует правила игры, оказывает поддержку отечественным компаниям, участвует в капитале ИТ-компаний. Внешнеполитические события формируют вызовы для национального сегмента киберпространства, для преодоления которых требуется взаимодействие акторов полей государства и бизнеса. Среди вызовов выделяется санкционное давление коллективного Запада на российский ИТ-сектор, релокация части специалистов в зарубежные юрисдикции.

Несмотря на ряд экономических трудностей, уход с российского рынка иностранных компаний и запрет на поставку в Россию товаров и услуг открыли широкие возможности для роста российских ИТ-компаний. Доля ИТ-сферы в ВВП России активно растет. Отсутствие иностранных конкурентов и государственные меры поддержки вызвали скачкообразный рост прибылей отечественных компаний. Меры поддержки включают в себя государственные заказы, льготные кредиты, отсрочку от армии и льготную ипотеку для специалистов, налоговые льготы и т.д. Важным шагом стала замена иностранного АО и ПО государственных органов и объектов критической инфраструктуры на продукцию отечественных производителей.

Во втором параграфе второй главы **«Взаимодействие государства и бизнеса в поле программного обеспечения»** анализируются наиболее крупные игроки поля ПО, стратегии их взаимодействия с государством.

Несмотря на санкции, рынок ПО продолжил рост, параллельно происходит активное сокращение доли иностранной продукции и, как следствие, увеличение продаж отечественных софтверных компаний. Сфера производства ПО может являться одним из драйверов роста экономики России, особенно с учетом всесторонней государственной поддержки и новых мер, ограничивающих использование государственными органами и объектами критической инфраструктуры иностранного ПО.

Из 100 крупнейших ИТ-компаний России 41 компания занимается разработкой ПО, большинство из которых принадлежат российским физическим и юридическим лицам. На основе использования матрицы теории игр для кооперативной игры определено, что для российского государства и бизнеса в сфере ПО наиболее выгодным будет сочетание стратегий развития со стороны государства и стратегий развития со стороны ИТ-бизнеса. Сочетание указанных стратегий является равновесием Нэша и обладает свойством Парето-эффективности. Данная подсистема национального сегмента киберпространства находится в наиболее выигрышном состоянии в сравнении с остальными подсистемами.

В третьем параграфе второй главы **«Взаимодействие государства и бизнеса в поле аппаратного обеспечения»** рассматривается сфера производства АО, показатели выручки наиболее крупных компаний в сфере АО, а также матрица стратегий взаимодействия государства и бизнеса в данном поле.

Санкции нарушили международные линии поставок компонентов и гарантийной поддержки оборудования, чем нанесли серьезный ущерб российским компаниям-производителям АО. На современном этапе наблюдается серьезная зависимость Российской Федерации от иностранных поставщиков АО, что является угрозой для безопасности государства. Но, несмотря на это, в 2022 г. и 2023 г. произошел значительный скачок продаж отечественного ИТ-оборудования ввиду отсутствия на российском рынке иностранных альтернатив.

Государство активно поддерживает производство и усовершенствование ИТ-оборудования, что необходимо для развития российской экономики и повышения безопасности страны. Значительную долю оборота отечественной ИТ-сферы аппаратного обеспечения составляют государственные закупки.

Одной из особенностей поля АО на современном этапе является легализация параллельного импорта, что временно решает проблему нехватки продукции на российском рынке. Данная стратегия в долгосрочной перспективе несет угрозу для

отечественных производителей, расширяет серую и черную сферу экономики, что, в свою очередь, сказывается негативно на стабильности российского сегмента киберпространства.

Для устойчивости отечественного сегмента киберпространства оптимальным представляется сочетание стратегии развития со стороны государства и стратегии выживания для российских компаний в сфере АО (им необходимы время, ресурсы, компетенции, технологии, чтобы перестроиться под новые экономические условия). Сочетание указанных стратегий является равновесным по Нэшу и Парето-эффективным.

В четвертом параграфе второй главы **«Взаимодействие государства и бизнеса в поле подготовки кадров для ИТ-сферы»** рассматривается подготовка новых кадров для системы государственного управления и бизнес-структур в сфере ИКТ.

В сфере ИТ подготовка новых специалистов и развитие систем фундаментальных научных исследований обладают особенно тесной связью, так как данная сфера относится к высокотехнологичному сектору экономики страны. Одной из наиболее серьезных проблем поддержания устойчивости национального сегмента киберпространства является нехватка квалифицированных специалистов. Данная проблема остро проявилась после введения санкций и активного релоцирования специалистов за рубеж. Данное явление достигло своего пика в начале санкционного противостояния.

Нехватка кадров является системной проблемой российской сферы ИТ. Она вызвана малым интересом общества к отечественной ИТ-сфере до 2020-х годов и активной «утечкой мозгов» за рубеж. Но резкий рост ИТ-компаний, повышение заработной платы и общее внимание к данной области в совокупности с государственной поддержкой способствуют возвращению специалистов из-за рубежа, активному притоку в вузы абитуриентов на ИТ-специальности.

Решение проблемы нехватки кадров требует долгосрочного государственного планирования в сфере высшего образования и поддержки университетов. Акцентируется значимость таких мер, как льготная ипотека, отсрочка от призыва в армию, а для иностранных специалистов трудоустройство и получение ВНЖ. Государство инициирует и поддерживает проекты «Кадры для цифровой экономики», часть национальной программы «Цифровая экономика Российской Федерации».

Третья глава **«Формирование устойчивого сегмента киберпространства Российской Федерации»** содержит анализ подходов различных государств к

выстраиванию системы функционирования и устойчивости национального сегмента киберпространства. Проводится SWOT-анализ российского сегмента киберпространства для определения перспектив его развития с учетом сложившихся сильных и слабых сторон, а также потенциальных возможностей и угроз.

В первом параграфе третьей главы **«Зарубежный опыт и возможности его адаптации в интересах повышения устойчивости российского киберпространства»** рассматривается понятие «цифровой суверенитет» и его связь с различными направлениями государственных политик цифрового суверенитета ряда стран.

Анализ зарубежного опыта форматирования киберпространства в целях маркирования границ национального сегмента и формирования цифрового суверенитета как составного элемента государственного суверенитета показал, что решающими факторами данных процессов являются политический выбор правящих элит и технологические возможности страны. В свою очередь, технологические возможности определяются, прежде всего, наличием компетентных и ресурсных отечественных фирм по производству ПО, АО, квалифицированных кадров, степенью включенности в глобальные цепочки обмена товарами и услугами. Изучение зарубежных кейсов позволило выделить следующие виды цифрового суверенитета, нацеленного на поддержание устойчивости национального сегмента киберпространства: оборонительный, экспансионистский, нормативный, постколониальный и гегемонистский.

На основе анализа зарубежных кейсов выделены три стратегии согласования интересов государства и бизнеса ИТ-сектора, обеспечивающих суверенитет и устойчивость национального сегмента киберпространства:

Максимальный государственный контроль с опорой на отечественные компании ИТ-сектора, а также ИТ-компании дружественных стран как гарантов функционирования инфраструктуры национального сегмента киберпространства (Китай, Россия, Вьетнам, отчасти Австралия);

Контроль распределен между интегрированными государствами (ЕС, отчасти ЮАР) или сосредоточен в одной стране (Индия) с опорой на международные ТНК (либо из США, либо из стран ЕС) как гарантов функционирования инфраструктуры национального сегмента киберпространства.

Государственный контроль формально не является тотально-административным и легализуется формальными институтами (использование неформальных институтов

оправдывается интересами национальной безопасности и защиты прав человека). Сильные отечественные ТНК ИТ-сектора активно участвуют в осуществлении контроля и гарантируют функционирование инфраструктуры национального сегмента киберпространства (США).

Исходя из осуществленной классификации, российской практике соответствует экспансионистский вид цифрового суверенитета и первый тип стратегии обеспечения суверенитета.

Во втором параграфе третьей главы **«Перспективы согласования интересов государства и бизнеса в обеспечении устойчивости российского сегмента киберпространства»** на основе метода SWOT-анализа российского сегмента ИТ-компаний, политики государства в сфере ИТ, а также интегрированного SWOT-анализа российского сегмента киберпространства с использованием модели пяти сил Портера изучены среднесрочные перспективы взаимодействия государства и бизнеса.

Основными факторами поля «Силы» российского сегмента киберпространства являются политические факторы: политический курс на суверенитет национального сегмента киберпространства; финансовое и законодательное обеспечение цифровизации всех сфер общественной жизни; участие в секторе государственных корпораций, квазигосударственных компаний с финансовым и административным ресурсом; политико-экономическое сотрудничество с Китаем как страной производителем дефицитной продукции ИТ-сектора. Среди слабостей, прежде всего, доминируют экономические факторы: высокий уровень серого и черного импорта, использование нелицензионной продукции как результат недостаточного импортозамещения; технологическое отставание российского АО от иностранных аналогов; недостаток ИТ-специалистов. Также весьма значительна роль внешнеполитического фактора антироссийских санкций.

Поле возможностей в равной степени представлено политическими и экономическими факторами. Среди угроз доминируют политические факторы, такие, как расширение пула стран, поддержавших санкции, что затруднит или блокирует получение технологий и дефицитных товаров ИТ-сферы.

Перспективы развития российского сегмента киберпространства как совокупности взаимодействия стратегий политических и экономических акторов в среднесрочном периоде можно представить в качестве нестрогого неравенства, в

котором сумма факторов полей «Силы» и «Возможностей» за счет политической составляющей несколько перевешивает сумму факторов полей «Слабости» и «Угрозы», также состоящую из политических компонентов. Результаты SWOT-анализа показывают реальную возможность достижения устойчивости российского сегмента киберпространства на основе конгруэнтности стратегий государства и бизнеса в сфере ПО и АО.

III Заключение

Согласование политических интересов государства и бизнеса в национальном сегменте киберпространства определяется конгруэнтностью стратегий действий органов государственной власти и компаний ИТ-сектора для достижения целей акторов. Ситуационно складывающие балансы интересов государственных органов и компаний ИТ-сектора в разной степени определяют степень устойчивости российского сегмента киберпространства. Точка согласования политических интересов государства и бизнеса ИТ-индустрии будет находиться в диапазоне экспансионистского вида цифрового суверенитета и первого типа стратегии обеспечения суверенитета национального сегмента киберпространства (максимальный государственный контроль с опорой на отечественные компании ИТ-сектора).

Основным политическим интересом органов государственной власти России в настоящем времени и в среднесрочной перспективе является максимальная «национализация» инфраструктуры российского сегмента киберпространства для решения задачи обеспечения национальной безопасности и стабильного функционирования политического режима. Основным интересом российских ИТ-компаний является увеличение прибыли путем освоения той части российского рынка, которая была ранее занята иностранными компаниями. Результатом согласования интересов, оптимального баланса стратегий действий обеих сторон является состояние устойчивости национального сегмента киберпространства.

IV Список работ, опубликованных по теме диссертации

Публикации в рецензируемых научных изданиях,
определенных ВАК
при Минобрнауки России:

1. Ковригин, Д.Э. Границы государственного суверенитета национального сегмента киберпространства / Д.Э. Ковригин // Общенациональный научно-политический журнал «Власть». – 2023. – № 1. – С. 124-129. – ISSN 2071-5358.

2. Ковригин, Д.Э. Применение теории полей для анализа взаимодействия государства и бизнеса в российском сегменте киберпространства / Д.Э. Ковригин // Вопросы национальных и федеративных отношений. – 2024. – № 1 (106). – С. 223-228. – ISSN 2226-8596.

3. Ковригин, Д.Э. Российский IT-рынок в условиях санкционного давления Запада / Д.Э. Ковригин // Гуманитарные науки. Вестник Финансового университета. – 2024. – № 2. Том 14 – С. 120-125. – ISSN 2226-7867. – Текст : электронный. – DOI 10.26794/2226-7867-2024-14-2-120-125. – URL: https://humanities.fa.ru/jour/issue/viewIssue/58/34 (дата обращения: 08.07.2025).

4. Ковригин, Д.Э. Взаимодействие власти и бизнеса Российской Федерации в поле подготовки кадров для ИТ-отрасли в целях достижения суверенитета российского сегмента киберпространства / Д.Э. Ковригин // Социально-гуманитарные знания. – 2024. – № 5. – С. 149-153. – ISSN 0869-8120. – Текст : электронный. – DOI 10.34823/SGZ.2024.05.00000. – URL: https://socgum-journal.ru/archive/ (дата обращения: 08.07.2025).

5. Ковригин, Д.Э. Политика взаимодействия государственных структур и IT-компаний для достижения суверенитета российского сегмента киберпространства / Д.Э. Ковригин // Вопросы национальных и федеративных отношений. – 2024. – № 12 (117). Том 14. – С. 3773-3780. – ISSN 2226-8596.