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

ДИССЕРТАЦИЯ
на соискание ученой степени
кандидата политических наук

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

Москва - 2025

Оглавление

Введение 4

Глава 1 Теоретико-методологические основы исследования взаимодействия государства и бизнеса 19

1.1 Теоретические основы исследования согласования интересов государства и бизнеса в обеспечении устойчивости российского сегмента киберпространства 19

1.2 Методология и методика изучения согласования интересов государства и бизнеса в обеспечении устойчивости российского сегмента киберпространства 46

Глава 2 Взаимодействие государства и бизнеса в области информационных технологий 74

2.1 Ресурсы, акторы, стратегии взаимодействия государства и ИТ-бизнеса в контексте геополитических вызовов 2020–2024 гг. 74

2.2 Взаимодействие государства и бизнеса в поле программного обеспечения 88

2.3 Взаимодействие государства и бизнеса в поле аппаратного обеспечения 96

2.4 Взаимодействие государства и бизнеса в поле подготовки кадров для ИТ-сферы 110

Глава 3 Формирование устойчивого сегмента киберпространства Российской Федерации 124

3.1 Зарубежный опыт и возможности его адаптации в интересах повышения устойчивости российского киберпространства 124

3.2 Перспективы согласования интересов государства и бизнеса в обеспечении устойчивости российского сегмента киберпространства 135

Заключение 151

Список литературы 160

Приложение А Российский сегмент ИТ-компаний 193

Приложение Б Финансовая деятельность крупнейших компаний ИТ-сферы 2020–2023 гг. 194

Приложение В Данные крупнейших компаний ИТ-сферы 206

Приложение Г Законодательные акты Российской Федерации в сфере ИТ, принятые в 2020–2023 гг. 231

Приложение Д Данные SWOT-анализа российского сегмента ИТ-компаний..... 249

Приложение Е Данные SWOT-анализа российской политики в сфере ИТ 253

Приложение Ж Данные SWOT-анализа российского сегмента киберпространства 257

Приложение И Данные матрицы исходов стратегий взаимодействия государства и бизнеса сегмента ПО 261

Приложение К Данные матрицы исходов взаимодействия государства и бизнеса сегмента АО 264

Введение

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 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 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 [29], Н. Лумана [17], Д. Истона [229], Г. Алмонда [223], Г.Б. Клейнера [176]. Теоретические основы неоинституционального подхода отражены в работах Д. Норта [23], Г. О'Доннелла [194], Р. Коуза [13], Г. Питерса [202], Ю.В. Ирхина [174], Дж. Олсена и Дж. Марча [234]. Концептуальные рамки теории полей разработаны П. Бурдье [5] и нашли свое продолжение в работах Н. Флигстина и Д. Макадама [37].

Работы второй группы отражают используемый в диссертации методологический инструментарий и понятийный аппарат теории игр: Дж.М. Смита [56], Дж. Нэша [234], Дж. Неймана [235], Р. Льюса и Х. Райфа [18], А. Раппопорта [53], Т. Шеллинга [41], Л. Шепли [239].

Третья группа работ состоит из исследований групп интересов: А. Бентли [43], Д. Трумэна [58], А.В. Павроза [196] и С.В. Расторгуева [204]. Концепция неокорпоративизма на зарубежном материале представлена в работах Ф. Шмиттера [221], Дж. Лембруха [231], К. Каусона [46], Е. Талоса [241], Г. Кроуча [183]. Среди отечественных авторов проблематика неокорпоративизма отражена в работах А.Ю. Зудина [170], О.В. Гаман-Голутвиной [6], С.П. Перегудова [199], А.В. Павроза [28], С.Г. Кордонского [11], О.Э. Бессоновой [2], О.В. Крыштановской [15]. Теория общественного выбора разработана в трудах Дж. Бьюкенена [224].

К четвертой группе относится литература, раскрывающая вопросы устойчивого развития систем, в нее входят работы Р.И. Захарченко и И.Д. Королева [168], О.Ф. Шаброва [218], С.Э. Хайкина [214], вопросы киберустойчивости анализируются в работах Ю. Кукола [49].

В пятую группу входит литература, анализирующая тематику развития киберсреды и киберпространства: Д. Кларк [225], Л.В. Терентьева [210],

С.В. Петровский [89], А.А. Максуров [186], В.М. Розин [206], Д. Ланир [16], А.А. Печников [201], В.В. Вихман и М.В. Ромм [154], Г.В Верхова и С.В. Акимов [153]; сюжетная проблематика информационного пространства отражена в работах В.Л. Гирич и В.Н. Чуприной [162], А.В. Манойло [19], И.А. Добровольской [165], И.М. Дзялошинского [8], В.А. Филиппова [85]. Вопросы регулирования киберпространства представлены в работах Д. Басселл и Т. Стивенса [44], К. Флойда и П. Перника [57], А.А. Данельяна [163], диссертационных исследованиях А.В. Алагоз [86], И.А. Бабюк [81], Д.Р. Мухаметова [88], Э.Т. Есиева [82]. Цифровые коммуникации и платформы в России, проблемы их развития на современном этапе исследованы в трудах Е.В. Бродовской [152], А.Ю. Домбровской [166], Р.В. Пармы [198], С.Г. Ушкина [211].

К шестой группе относятся работы, исследующие проблематику суверенитета государства в информационно-телекоммуникационной сфере: А.В. Даниленков [164], А. Епифанова [228], В.Б. Наумов [192], Д.В. Красиков [182], Ю. Кол [230], К. Айкенсер [227], Н. Цагуриас [242], проблема технологического суверенитета представлена в работах В.В. Иванова [171]. Политические конфликты в формате гибридных и информационных войн изучены в работах С.В. Володенкова [159], Н. Мэттиса и Ф.Г. Хоффмана [48], В.А. Артамонова и Е.В. Артамоновой [146], Ю.Ю. Першина [200], В.Б. Вепринцева [25], А.В. Манойло [188], А.И. Петренко [25], Д.Б. Фролова [25], В.В. Митевой [159], Д. Аркилла и Д. Ронфельдта [42], Р.А. Кларка [47].

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 [86], анализ социальных и политических аспектов цифровизации системы единой публичной власти в Российской Федерации [81], роль виртуальных технологий в конфликтной мобилизации в интернет-пространстве и

противодействие ей [82], роль государства в трансформации экосистемы цифровой экономики [84]. Меньше внимания уделяется исследованию влияния политического пространства на киберпространство, среди имеющихся работ следует упомянуть диссертацию Д.Р. Мухаметова, рассматривающую процесс формирования и различные направления развития «умного» государства в качестве новой модели политического управления в контексте цифровой трансформации [88].

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 и объяснении стратегий согласования 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 устойчивости инфраструктуры национального сегмента киберпространства с учетом особенностей внешних вызовов;

- выявить структуру и динамику ИТ-сферы Российской Федерации в 2020–2024 гг. как материальной основы национального сегмента киберпространства;

- определить особенности стратегий 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 диссертации - взаимодействие российского государства и бизнеса ИТ-сферы.

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

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).

Эмпирическая база исследования основана на следующих источниках:

- 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.

- 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 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) 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 для достижения устойчивости национального сегмента киберпространства.

4) 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 для достижения устойчивости национального сегмента киберпространства.

5) В условиях среднесрочных внутриполитических и долгосрочных внешнеполитических трендов 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 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. Данное 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 данного 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 [29], Н. Луман [17], Д. Истон [229], Г. Алмонд [223], Г.Б. Клейнер [176], О.Ф. Шабров [218]). Неоинституциональный подход использовался при исследовании развития институтов (правил игры), механизмов соблюдения контрактов при взаимодействии политической власти и бизнеса (Д. Норт [23], Г. О'Доннелл [194], Р. Коуз [13], Г. Питерс [202], Дж. Олсен и Дж. Марч [232], Ю.В. Ирхин [174]).

Теоретический фундамент исследования базируется на:

- концепции полей П. Бурдье [5], новой концепции полей Н. Флигстина и Д. Макадама [37], анализирующих определенные сферы деятельности как взаимодействия иерархизированных акторов, обменивающихся ресурсами;

- концепции неокорпоративизма Ф. Шмиттера [221], 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 [170], О.В. Гаман-Голутвина [6], С.П. Перегудов [199], А.В. Павроз [28], С.Г. Кордонский [11], О.Э. Бессонова [3], О.В. Крыштановская [15]);

- концепции киберпространства как специфического поля информационной коммуникации в сети интернет, требующего поддержания технологической инфраструктуры, спецификации прав собственности и законодательного регулирования (Дж. Басселл [44], Д. Кларк [225], А.В. Манойло [19]).

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.

Положения, выносимые на защиту:

Разработанная автором методика исследования основывается на принципах системного и неоинституционального подхода, постулатах концепций полей и неокорпоративизма, конвертации полученных количественных и качественных результатов в матрицу исходов стратегий теории игр (с фиксацией состояний Парето-эффективности и равновесия Нэша). 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; 64-70; 61).

В условиях геополитического кризиса можно обозначить три варианта стратегии взаимодействия государства и бизнеса: стратегия зависимости;

стратегия выживания; стратегия развития. Отечественные компании производители программного обеспечения 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).

Отечественные компании производители аппаратного обеспечения 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).

Анализ мирового 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 (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).

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 неравновесное 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).

Согласование 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 киберпространства для решения задачи обеспечения национальной безопасности. Основным интересом российских ИТ-компаний является увеличение прибыли путем освоения той части российского рынка, которая ранее была занята иностранными компаниями. Результатом согласования интересов, оптимального баланса стратегий действий для обеих сторон 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 им методы научного исследования являются объективными и логичными. Автором корректно использованы исходные данные справочных источников, специальной научной литературы, законодательных баз, эмпирических данных, которые составлены на основе данных наиболее крупных ИТ компаний России.

Апробация результатов исследования. Основные положения диссертационного исследования были представлены автором в докладах и выступлениях на следующих конференциях: на XXX Международной конференции студентов, аспирантов и молодых ученых «Ломономов» в рамках Международного молодежного научного форума «Ломоносов» (Москва, МГУ имени М.В. Ломоносова, 10-21 апреля 2023); на LVIII Международной научно-практической конференции «EURASIASENCE» (Москва, Научно-издательский центр ООО «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 Государтственный Университет, 16-18 апреля 2024 г.); на Всероссийском XV молодёжном научном форуме МТУСИ «Телекоммуникации и информационные технологии-реалии, возможности, перспективы» (Москва, МТУСИ, 01-20 апреля 2024 г.).

Внедрение результатов исследования. Результаты диссертационного исследования используются в практической деятельности АО «Микояновская слобода». Ключевые выводы и положения диссертационного исследования стратегий взаимодействия власти и бизнеса, а также обоснованная автором 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 автором системы показателей оценки состояния компаний используются при анализе конкурирующих организаций. Выводы и основные положения диссертации используются в практической работе АО «Микояновская слобода» и способствуют повышению эффективности деятельности организации.

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».

Апробация и внедерение результатов исследования подтверждены соответствующими документами.

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. Диссератция 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.

Глава 1
Теоретико-методологические основы исследования взаимодействия государства и бизнеса

1.1 Теоретические основы исследования согласования интересов государства и бизнеса в обеспечении устойчивости российского сегмента киберпространства

В данном параграфе структурирована теоретическая основа исследования согласования интересов государства и бизнеса: теория полей, теория общественного выбора, концепция групп интересов, концепция неокорпоративизма, концепции кластеров и цепочки создания стоимости. Далее рассматриваются теоретические основы исследования национального сегмента киберпространства: терминология, связанная с киберпространством, кибербезопасность, устойчивость киберпространства, границы государства в киберпространстве.

Для анализа концепций согласования интересов государства и бизнеса представляется перспективным использовать теорию полей П. Бурдье [5]. В трудах П. Бурдье поле политики рассматривается как рынок, на котором, как и на экономическом рынке, существуют производство, спрос и предложение. На данном рынке циркулируют особые политические продукты, такие как политические программы, анализы, события, позиции и партии. Политическое поле понимается как место сил и борьбы агентов политического процесса. Данное поле формируется в процессе взаимного позиционирования акторов, чей властный капитал различается по структуре и объёму. Качество имеющегося капитала определяет способность актора войти в поле, повлиять на структуру поля, на других участников и, в конечном счете, на извлечение прибыли.

Борьба между агентами направлена на изменение соотношения данных сил, определяющих, в свою очередь, структуру поля политики. По Бурдье политическая жизнь следует логике спроса и предложения, где граждане представлены потребителями политической продукции. Чем меньше они могут влиять на производство политических продуктов, тем выше вероятность, что граждане получат не то, на что надеялись.

Под политическим агентом П. Бурдье понимает активного, самостоятельного, действующего исключительно внутри социальных отношений участника процесса, который своими действиями репродуцирует или трансформирует данные отношения. Поскольку все характеристики агента формируются за счет его перемещений в социальном пространстве, агент не является универсальным. Все агенты индивидуальны и являются продуктами коллективной и индивидуальной истории. Здесь П. Бурдье вводит еще одно ключевое понятие: «габитус». Под ним понимается система схем восприятия и оценки социальной реальности. Данная система формируется в процессе человеческой социализации и выполняет роль посредника между агентом и социальными отношениями. П. Бурдье говорит о том, что оценка общества и процессов в нем зависит от точки расположения в нем оценивающего субъекта.

Главное противостояние во властном поле происходит между доминирующими игроками, стремящимися сохранить свое положение, и претендентами, стремящимися его занять, изменив тем самым структуру и логику системы. П. Бурдье под доминантным игроком понимал актора, обладающего явным превосходством в ресурсном плане перед своими конкурентами. Они конкурируют в одной и той же сфере деятельности. Но при этом П. Бурдье отмечал взаимосвязанность разных полей. Из этого следует, что игроки, находящиеся в различных полях, всё же могут оказывать влияние друг на друга.

Концепция П. Бурдье легла в основу работ Н. Флигстина и Д. Макадама [37]. Данные авторы предложили ввести нового игрока поля,

которого они назвали «внутренние управленческие единицы», следящие за соблюдением норм остальными игроками. Государство в лице своих органов власти представлено самостоятельными полями, активно воздействующими на негосударственные или квазигосударственные поля. Данная концепция использована в диссертации для анализа взаимодействия полей государства и бизнеса.

Необходимо отметить, что для Н. Флигстина и Д. Макадама поля – это пространство постоянного соперничества участников, стремящихся достичь вершины иерархии. Они борются не только за материальные ресурсы и различные привилегии, но и за исходящие из них интерпретационные рамки понимания реальной ситуации. Поля постоянно меняются, так как сложившееся положение дел постоянно оспаривается. Стабилизация поля происходит в момент формирования общепризнанной игроками иерархии, которая фиксирует ресурсный потенциал на определенный момент времени. Выделяются три стратегии игроков: принуждение, соперничество, кооперация. Реализация трех вышеуказанных стратегий создает социальные миры, отражающие временный консенсус разновекторных и не равных по ресурсам акторов поля.

Для создания консенсусной коалиции необходим определенный «социальный навык», под которым понимается способность актора обеспечивать кооперацию посредством создания разделяемых группой смыслов и коллективной идентичности. Благодаря этому группы с разными установками начинают сотрудничество для достижения общей цели.

На основе этого Н. Флигстин и Д. Макадам выстраивают систему взаимосвязанных полей (макрооснования теории), в которой ключевую роль играет внешняя среда. Вокруг поля сосредоточены соседние поля, которые могут как взаимодействовать с исследуемым полем, так и не взаимодействовать. В случае взаимодействия поля могут находиться в состоянии доминации-подчинения или равноправного обмена. Связи между

полями поддерживаются их акторами, поэтому степень их близости определяется за счет количества акторов и качества их связей.

Масштаб полей колеблется в зависимости от входящих в него элементов, которыми могут быть индивиды, группы, организации, компании, государства. Несмотря на разницу в масштабе поля, его структура одинакова, и крупный элемент поля может выступать как самостоятельное поле для более мелких элементов. По сути, полем может быть названа любая площадка, занятая двумя и более игроками, чьи действия ориентированы друг на друга.

Государство само, будучи иерархией полей, выполняет функции инициирования появления новых полей и управления всей совокупностью полей. Государство формирует правила игры акторов, обеспечивая тем самым необходимую стабильность. Правила игры эффективны, когда они прописаны максимально полно, четко и всесторонне. Государственное поле характеризуется стремлением к расширению, степень его разрастания ограничивается идеологическими особенностями государства и наличием или отсутствием в конкретный промежуток времени кризисных явлений, требующих усиления государственного контроля за ситуацией. Изменения внутри поля могут проистекать из внешних и внутренних для данного поля причин.

Поля возникают, когда в какой-то новой сфере деятельности еще не возникли правила деятельности, и акторы стремятся их туда привнести. В современном мире в качестве основных причин возникновения полей выделяются такие факторы, как рост численности населения, технологический прогресс (что особенно важно для исследования), процессы социальной организации и влияние государства.

Институционализация поля проходит в процессе выработки условий регулирования и иерархии деятельности акторов поля при содействии со стороны государства. При этом институционализация поля стимулирует появление и трансформацию других полей. Источниками дестабилизации

поля служат вторжение акторов из другого поля, трансформация взаимосвязанного или контролирующего поля и критические макрособытия, такие, как война. Стабильность в поле восстанавливается, когда достаточно влиятельные группы объединяются в коалицию, чаще всего это достигается при поддержке государства.

Рассматривая в данной работе различные формы объединения акторов в различные системы, следует отдельно разобрать теории кластеров и цепочки создания стоимости М. Портера [53]. Под кластером М. Портер подразумевает взаимосвязанные и взаимодополняющие компании в определенной сфере, которые соседствуют друг с другом в географическом пространстве. Компании географически концентрированы. Данные компании можно разбить на три категории: поставщики, производители и посредники. Помимо них в кластер входят связанные с данными компаниями организации, к которым относятся образовательные заведения, где обучаются новые специалисты для компаний. Далее идут инфраструктурные компании, предоставляющие услуги, позволяющие компаниям функционировать. Третьим типом взаимосвязанных организаций являются органы государственного управления, обеспечивающие законность и стабильность функционирования кластера. Поскольку компания существует в своем кластере, М. Портер указывает на то, что конкурентоспособность стран на мировой арене надо оценивать именно через конкурентоспособность кластеров этих стран, а не отдельных фирм. Устанавливается причинно-следственная связь: субъекты кластера наиболее эффективно используют ограниченные ресурсы, что позволяет им быть максимально конкурентоспособным и, как следствие, максимально устойчивыми (готовыми справляться с внутренними и внешними шоками). Описанная М. Портером система кластеров наиболее актуальна для представления сегмента производства и разработки аппаратного обеспечения, так как требует взаимосвязи как на региональном, так и на международном уровне.

Добившаяся успеха фирма распространяет свое положительное влияние на свое ближайшее окружение, повышая его успешность. В основе формирования кластеров лежит процесс обмена информацией между сферами экономики по поводу потребностей, техники и технологий. В данной системе конкуренция способна нанести вред процессу обмена информацией и, как следствие, понизить эффективность использования ресурсов кластером. В рамках кластерного подхода, в соответствии с М. Портером, устойчивого развития на практике можно достичь только посредством создания кластеров, ведь основной целью кластера является повышение конкурентоспособности входящих в него предприятий. При этом происходит распространение выгоды на всех стейкхолдеров. Развитие кластера также способствует повышению уровня жизни местного сообщества.

Концепция «цепочки создания стоимости» М. Портера позволяет анализировать процесс производства товаров и услуг внутри компании с фиксацией всех видов издержек на каждом этапе. Политологический аспект «цепочки создания стоимости» состоит в том, что в качестве сквозных бизнес-процессов, влияющих на все этапы создания продукта, М. Портером указаны практики связей с государственными органами (Government relations) и кадровый рекрутинг компании (который напрямую связан с подготовкой абитуриентов в системе государственного образования и нормами трудового законодательства). Анализ данных элементов позволяет исследовать взаимодействия полей государственных органов и кластеров ИТ-компаний.

Концепция групп интересов разрабатывалась в работах зарубежных и отечественных политологов. А. Бентли указывает, что группы интересов в обществе оказывают давление как друг на друга, так и на государство, что является определяющим фактором политики государства. А. Бэнтли определяет группу индивидов, объединившихся из-за общих интересов и взаимодействующих с государством, как единицу политического процесса.

Общество является совокупностью групп интересов, а их количество ограничивается лишь количеством интересов. Понятия «группа» и «интерес» в данной концепции являются строго взаимосвязанными, без интереса не происходит объединение людей в группу [43].

В свою очередь, Д. Трумэн определяет «политические группы интересов» как группы, которые взаимодействует с институтами государства. Политический процесс представляется как групповая конкуренция за контроль над механизмами распределения ресурсов [58]. Конкурирующие группы интересов ищут доступ к ключевым центрам принятия политических решений. Групповая конкуренция способствует общественному равновесию и стабильности политических систем. Группы интересов действуют через политико-административные институты. Государственная политика по производству и распределению общественных благ, законодательному регулированию общества, в конечном счете, определяется балансом воздействий конкурирующих групп интересов. Д. Трумэн полагал, что невозможно установление монополии одной группы интересов, поскольку индивиды одновременно участвуют в разных группах.

Отечественный политолог А.В. Павроз определяет группы интересов как объединения по совместной реализации своих интересов. Он отмечает, что на современном этапе партийная демократия постепенно уступает место демократии групп интересов. Формирование политических решений постепенно переходит в область взаимодействия групп интересов и лоббистов [196]. Это связанно с тем, что группы интересов стали осуществлять функцию посредничества между институтом государства и гражданским обществом. Причинами усиления влияния групп интересов послужили: увеличение социальной дифференциации, размывание прежних социальных расколов, а также усложнение процессов политико-административного управления. В современном обществе необходим прямой диалог между государством и различными социальными интересами. На современном этапе происходит становление новой партисипаторной модели

взаимодействия между государством и группами интересов. Данная модель базируется на том, что достижение наибольшей эффективности выработки политико-административных решений возможно только при максимально интенсивном взаимодействии государства и групп интересов.

Для анализа взаимодействия государства и бизнеса в современной России целесообразно применить концепцию неокорпоративизма, которая разрабатывалась в трудах таких зарубежных авторов как Ф. Шмиттер [221], Дж. Лембрух [231], Э.Талос [241], Г. Штрек [240], К. Кроуч [183], К. Коусон [46], Л. Панич [236]. Концепция неокорпоративизма предполагает наличие двух центральных групп интересов, а именно власти и бизнеса. Государство представлено как самостоятельная и наиболее ресурсная группа интересов, которая выстраивает вокруг себя подчиненные группы интересов. Государство обладает первенством в выработке политических решений, но при этом оно допускает различные группы интересов к подготовке и реализации решений.

Ф. Шмиттеру принадлежит классическое определение неокорпоративизма как системы представительства интересов, в которой государство предопределило место и функции специально отобранных (лицензированных) монопольных групп в политико-административном процессе в обмен на контроль над кадровой политикой и программными требованиями данных групп. Г. Лембрух определил неокорпоративизм как форму выработки политики, в центре которой находится социальное сближение. Публичная политика как в форме распределения ресурсов, так и артикулируемых дискурсов, определяется коалицией наиболее крупных групп интересов и государства [231].

Среди отечественных авторов, развивающих концепцию неокорпоративизма, автором выделяются: А.Ю. Зудин [170], О.В. Гаман-Голутвина [6], С.П. Перегудов [199], А.В. Павроз [28], С.Г. Кордонский [11], О.Э. Бессонова [3], О.В. Крыштановская [15] и др. С.П. Перегудов на основе анализа российских практик 1990-х начала 2000-х

годов выявил тенденцию корпоративно-бюрократического симбиоза [237]. А.В. Павроз доказывал, что в России нацеленные на поиск ренты группы интересов встраиваются в систему принятия государственных решений через механизм административного торга, а наиболее ресурсные акторы бизнеса встраиваются в вертикаль власти [197]. Концепция С.Г. Кордонского указывает на административный рынок, где чиновники ведут своеобразный торг за распределение ресурсов, как на основной механизм взаимоотношений государства и бизнеса. В современном российском обществе группы интересов иерархически ранжируются в зависимости от объема осваиваемых ими ресурсов и их корпоративного статуса [12].

О.Э. Бессонова указывает на то, что в мировой истории можно выделить два основных типа экономических механизмов: рыночный механизм и раздаточный механизм. Раздаточный механизм базируется на принудительной мобилизации ресурсов [150]. Данный тип организации был свойственен СССР и другим странам с плановой экономикой и давал возможность концентрировать экономические ресурсы на решении первостепенных задач в обход потребностей рынка. Несмотря на то, что на современном этапе в Российской Федерации официально функционирует рыночная экономика, элементы раздаточных механизмов продолжают функционировать как определенный элемент культурного кода, оставшегося в политических и экономических элитах от периода Советского Союза [149]. О.В. Крыштановская также выделяет два типа организации общества: экономическое общество (частная собственность, рыночные отношения, принципы модернизации, стратификация основана на экономическом принципе), политическое общество (значительная роль государственной собственности, распределительные отношения, стратификация основана на месте индивида во властной иерархии). Российская Федерация характеризуется как симбиоз экономического и политического общества, с доминированием последнего типа [15].

С.В. Расторгуев, анализируя взаимоотношения политической власти и бизнеса как разноуровневые сетевые обмены ресурсами с использованием концепции коммуникационных кодов систем общества Н. Лумана, пришел к выводу о возможности зафиксировать состояния баланса и дисбаланса обменных операций экономической и политической сферы. В случае, если код политической системы «политическая власть» приобретает значительное доминирование над кодом экономической системы «экономический капитал», формируется классическая неокорпоративистская модель [204].

В ходе анализа взаимоотношений российского государства и бизнеса исследователи выделяли типовые модели взаимодействий. Модель – это искусственный, созданный в исследовательских целях объект, который в упрощенном виде воспроизводит существенные характеристики и процессы действительности. На основе российской практики начала XXI века были выделены четыре модели взаимодействия органов государственной власти и бизнес-структур в зависимости от того, какая сторона и в какой степени доминирует в данном процессе [35].

- «Невмешательство», в данной модели органы государственной власти не принимают активного участия в проводимой бизнесом политике [40].

- «Партнерство», в данной модели субъекты взаимодействия достигли взаимовыгодного компромисса.

- «Патронаж», в данной модели органы власти предоставляют бизнес-структурам доступ к ресурсам в качестве компенсации за их участие в социально ориентированных проектах.

- «Подавление и принуждение», в данной модели превалирует административное давление государства на бизнес-структуры.

Для отечественного сегмента киберпространства применима модель «Патронаж», в которой государство обеспечивает поддержку бизнес-структурам, чьи стратегии деятельности сочетаются с политическими целями.

Можно выделить три основных режима функционирования взаимодействия органов государственной власти и бизнеса [144]:

- «директивный», в данном режиме доминирующим агентом является государство за счет ресурсов, которыми оно обладает. Стратегическое управление целиком подчинено государству. Бизнес подчиняется и не стремится получить рычаги влияния на формирование политического курса;

- «функциональный», в данном режиме государство стремится реализовать управление над бизнесом, который является социально-политическим актором. Права собственности четко не определены и не защищены, активы находятся под контролем собственников, пока они лояльны существующей власти. Конфликтные ситуации чаще всего решаются при помощи административных методов;

- «коммуникативный», в данном режиме взаимоотношения акторов регулируются законами рынка. Распределение ресурсов подчинено экономическим и юридическим механизмам. Права собственности четко определены. Влияние бизнеса на выработку политических решений осуществляется посредством официально закрепленных механизмов лоббирования.

Эффективным способом управления взаимодействием является институционализация, поскольку прописанные процедуры взаимодействия и формальное структурирование поля акторов повышает предсказуемость поведения, уменьшает транзакционные издержки. Не потеряла актуальности классификация взаимоотношений государства и бизнеса Е. Ясина: а) «белая зона» – только формальные практики регулируемых законодательством взаимодействий; б) «серая зона» – практики неформального взаимодействия; в) «черная зона» – неформальные и противозаконные практики взаимодействия [222].

На современном этапе в сфере ИТ-бизнеса преобладают белые и серые зоны взаимодействия, что связанно с необходимостью обхода зарубежных

санкций, отставанием законодательного регулирования от технологического прогресса.

Теория общественного выбора Дж. Бьюкенена представляет собой применение экономического подхода к изучению нерыночных механизмов принятия решений [45]. Она является дополнением к теории рыночного обмена, объясняющей функционирование политических рынков. Теория общественного выбора базируется на трех принципах: индивидуализме (в политической сфере люди действуют, как и в бизнесе, исходя из своих интересов), концепции экономического человека (каждый человек руководствуется единым принципом рациональности, сравнение предельных выгод и предельных издержек) и на представлении политики как процесса обмена. Политическое решение представляет собой выбор альтернативных вариантов подобный рыночному механизму. В политике происходит обмен налогов на общественные блага.

Государство представляет собой арену конкуренции за влияние на принятие решений, а также за доступ к иерархической лестнице принятия решений. Дж. Бьюкенен проводит аналогию политики с игрой, в которой конституция – это правила игры, в рамках которой действуют участники политики. Текущая политика – это результат игры, а ее эффективность зависит от того, насколько всесторонне были проработаны правила игры, конституция, основной закон не только государства, но гражданского общества.

Дж. Бьюкенен указывает, что может возникнуть ситуация, когда государство не способно обеспечить эффективное распределение и использование общественных ресурсов. Причинами неэффективности являются: ограниченность информации для принятия решений, несовершенство политического процесса, неспособность государства предугадать долгосрочные последствия принятых решений. Также Дж. Бьюкенен разделяет две отдельные функции государства: государство

как гарант (гарант соблюдения конституционного договора) и государство как производитель (производитель общественных благ) [224].

Далее рассматриваются теоретические и концептуальные основы исследования национального сегмента киберпространства. Технологический прогресс на протяжении всей истории человечества определял, какое государство будет доминировать над своими конкурентами на том или ином этапе. На современном этапе развития одной из ведущих сфер, определяющих статус державы, стали информационно-коммуникационные технологии. От того, кто контролирует новейшие разработки в области микрочипов и программного обеспечения (далее – ПО) и кто владеет системами регулирования потоков информации, зависит экономическая, социальная, технологическая и во многом политическая картина мира. Современный мир является глобальным и взаимосвязанным в производственном плане. Это дает возможность странам не производить определенные технические элементы оборудования или программного обеспечения у себя, а импортировать необходимое извне. Однако, как показал пример России, попавшей под санкции стран глобального Запада с 2014 г., а особенно после начала СВО на Украине в 2022 г., такой подход к развитию экономики опасен. Если Российская Федерация намерена проводить самостоятельную политику на международной арене, необходимо обладать технологическим суверенитетом, распространяющимся на киберпространство.

Рассматривая регулирование национального сегмента киберпространства, необходимо дать определение самому термину «киберпространство» и связанным с ним концептам. Данный термин пришел в современную науку из научной фантастики. Термин «киберпространство» впервые появился в рассказе «Сожжение Хром» (Burning Chrom) У. Гибсона в 1982 году [163].

При появлении интернета под киберпространством стали понимать место обмена сообщениями. С развитием новых медиа киберпространство

включило в себя значительную часть общества. Как отмечает В.М. Розин, интернет оказывает огромное влияние на развитие цивилизации, виртуальное пространство фактически становится новой средой существования человека [206]. Сейчас киберпространство это многоаспектное понятие, для которого существует большое количество различных определений в зависимости от подхода.

Помимо термина «киберпространство» в научных работах используются термины: «киберсреда», «медиасфера», «сеть интернет», «интернет-среда», «веб-пространство», «медиапространство», «информационная реальность/ пространство-сфера», «виртуальная реальность/пространство/сфера». Следует отметить, что в западном научном дискурсе термины «киберсреда» и «киберпространство» более популярны. В свою очередь, в российском дискурсе более популярны термины «информационное пространство» и «интернет». Хотя все вышеперечисленные термины активно используются для обозначения виртуальной среды, некоторые из них являются взаимоисключающими. Вопросы регулирования киберпространства представлены в работах Дж. Басселл, Т. Стивенса [44], К. Флойда и П. Перника [57]. В своих трудах Дж. Басселл, определяет термин «киберпространство» как «аморфный и, предположительно, «виртуальный» мир, который образован связями между устройствами, обладающими поддержкой, а также компонентами самой инфраструктуры Интернета» [129]. Основываясь на данном определении, делается вывод, что определение киберпространства и интернета не релевантны друг другу.

В первую очередь, следует рассмотреть понятие «информационное пространство», так как оно затрагивает наиболее широкую сферу человеческих взаимоотношений, связанных с производством и обменом информацией. Под информацией, в данном случае, понимаются любые данные вне зависимости от их формы. В свою очередь, понятие «пространство» предполагает, что у сосуществующих субъектов, в данном

случае это распространители и получатели информации, есть взаимное расположение. Так, можно дать определение, в соответствии с которым, «информационное пространство» это система взаимодействия субъектов по производству, обмену и потреблению информации.

В.Л. Гирич и В.Н. Чуприна в своих трудах определяют «глобальное информационное пространство» как совокупность информационных ресурсов и инфраструктур, которые составляют компьютерные сети [162]. Данное определение действует как на уровне отдельного государства, так и на межгосударственном уровне. Также в систему «информационного пространства», в соответствии с В.Л. Гирич и В.Н. Чуприной, включены телекоммуникационные системы, сети общего пользования, а также другие каналы трансграничной передачи данных.

Определение термина «информационное пространство» присутствует в Указе Президента Российской Федерации от 9 мая 2017 года №203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы». В документе представлено следующее определение информационного пространства: «…совокупность информационных ресурсов, созданных субъектами информационной сферы, средств взаимодействия таких субъектов, их информационных систем и необходимой информационной инфраструктуры» [63].

В своих работах, А.В. Манойло определяет три составные элемента киберпространства, а именно: информационное поле, информационные потоки и каналы коммуникации средств массовой информации, в том числе, и массовой коммуникации [19]. В данном определении как производители, так и потребители информации являются одновременно и объектами, и субъектами информационного пространства. На основе вышеуказанных определений в исследовании сделан вывод, что информационное пространство – это многокомпонентная структура, базирующаяся на совокупности различных каналов коммуникации [165].

Можно сделать вывод, что термин «информационное пространство» значительно шире термина «киберпространство», так как охватывает потоки информации, передаваемые без помощи ИКТ.

Термины «медиасфера» и «медиапространство» имеют большое количество трактовок и часто считаются синонимичными с термином «информационное пространство». И.М. Дзялошинский под медиапространством понимает две сферы: первая – это информационное поле, которое находится внутри системы СМИ, акторами в котором выступают журналисты; вторая – это «ирреальное информационное пространство», в котором акторами являются производители информации и их целевая аудитория [8]. В.А. Филиппова определяет медиасферу как сферу общественных отношений по производству, обмену и потреблению продуктов медиа [85].

Интернет можно определить как информационно-телекоммуникационную сеть. С.В. Петровский определяет интернет как предназначенную для обмена данными международную сеть электросвязи общего пользования [89]. В свою очередь, А.А. Максуров определяет интернет как вид человеческой коммуникации [186]. Веб-пространство появилось позже интернета и на его основе. Под данным понятием понимается глобальное информационное пространство, которое основано на физической инфраструктуре интернета, специальном протоколе передачи данных, а также на особом языке [201].

Д. Ланир определяет «виртуальную реальность» как искусственно созданную при помощи информационных технологий среду, в которую человек при помощи специальных устройств (например, VR-очки) может погрузиться, изменять ее, испытывая при этом ощущения, схожие с восприятием реального мира. Д. Ланир рассматривает, как данный тип технологий влияет на государство, общество и человека. Указывается на опасность обретения монопольными ИТ-корпорациями сверхвласти над обществом [16].

Основной функцией киберсреды является обеспечение сквозного инфокоммуникационного взаимодействия между субъектами. Киберсреда базируется на трех принципах. Первый – это принцип агентности, который подразумевает под собой возможность свободной регистрации агента в киберсреде. Это происходит посредством создания (формирования) цифрового двойника. Под цифровым двойником понимается программный (виртуальный) аналог физического устройства [154], а в отношении человека – это виртуальная личность. В обоих вариантах осуществляется процесс создания и накопления в киберпространстве данных о физическом субъекте (устройстве, человеке, компании, организации, государстве). Вторым принципом является информационное самообслуживание. Этот принцип означает, что правообладатели информации сами вносят ее в киберсреду для ее распространения (контролируемого или неконтролируемого). Третий принцип: управляемая информационная открытость. В данный принцип входит лицензирование распространяемой информации, что накладывает определенные ограничения на ее распространение, а также ее изменение и удаление. В данный пункт входит все законодательное регулирование информации в киберсреде [153].

В соответствии с Глоссариием терминов НАТО киберпространство определяется как глобальная область, состоящая из всей совокупности взаимосвязанных коммуникационных и информационных технологий [138]. В данную совокупность входят другие электронные сети, системы и данные. Отмечается, что разделенные и независимые системы, которые отвечают за хранение, обработку и передачу данных, также входят в киберпространство. Киберпространство – это совокупность взаимосвязанных подсистем. С другой стороны, киберпространство в трактовке Европейской комиссии – это виртуальное пространство, в котором осуществляется циркулирование электронных данных между компьютерами во всем мире [129]. Проблемами для формирования единого подхода являются такие свойства киберпространства, как глобальный, трансграничный характер пространства.

В киберпространстве происходит агрегация данных из большого количества источников, находящихся в разных странах, что обуславливается архитектурной сосредоточенностью сети коммуникаций.

Киберпространство обладает смешанным, гибридным характером. Оно обладает как физическими, так и информационными уровнями. Д. Кларк в своих работах выделяет в системе киберпространства четыре уровня: 1) физический уровень; 2) логический уровень; 3) уровень контента (информационный уровень); 4) социальный уровень [225]. Первый уровень включает все оборудование, принимающее участие в функционировании киберпространства. Второй включает все программы, ответственные за функционирование оборудования и потоков информации. Третий содержит всю циркулирующую в киберпространстве информацию. Четвёртый уровень представляют люди, задействованные в процессах производства и распространения информации, разработки программ и производства техники, то есть люди, влияющие на первые три уровня.

Термин «киберпространство» имеет несколько определений, формулируемых авторами в зависимости от целей работы [210]. Несмотря на различие в подходах, на современном этапе киберпространство является концептом, который активно используется в международном дискурсе, в правительственных инициативах и в военных доктринах [226]. Несмотря на различия в определениях, в них можно выделить общие элементы. Первое, киберпространство зависит от интернета и без него не могло появиться и существовать. Второе, киберпространство обладает пространственными характеристиками.

Государство как основной институт политической системы на своей территории стремится обеспечить соблюдение законодательства. Проведение границ государственной территории в физическом мире не составляет особой сложности. Поскольку киберпространство является определенным типом пространства, то государство стремится регулировать его и деятельность своих граждан на его территории. Но из-за гибридного характера в

киберпространстве невозможно провести четкие границы. На современном этапе государственное законодательство в основном направлено на регулирование физической составляющей киберпространства. Так, сюда входят все технические средства обеспечения функционирования киберпространства, находящиеся на территории государства или под его юрисдикцией. Также сюда входят физические и юридические лица, подпадающие под юрисдикцию государства. Но тут уже возникают определенные вопросы. Многие компании, отвечающие за функционирование киберпространства определенного государства, не зарегистрированы в данном государстве, крайне слабо им контролируются и могут по тем или иным причинам его покинуть. Также крайне затруднительно регулировать деятельность граждан государства в киберпространстве, когда они находятся на территории другой страны. В ситуации с кибератаками, производимыми из-за рубежа, из-за неопределенности государственных компетенций крайне сложно найти и почти невозможно привлечь виновных к ответственности. В этом и заключается проблема контроля киберпространства. Нелегальный или нежелательный для государства и общества контент циркулирует внутри страны и между странами, технически поддерживаемый инфраструктурой киберпространства. Под юрисдикцию государства подпадают распространители недопустимого контента, находящиеся на территории данной страны, но при этом граждане страны могут легко получить доступ к сайтам иностранных распространителей.

Традиционно выделяют четыре стратегические области: суша, море, воздух и космическое пространство [130]. Но на современном этапе киберпространство также следует рассматривать как стратегическую область, обладающую при этом рядом уникальных свойств. Так, киберпространство пронизывает всю стратегическую среду, так как у него нет границ, из чего следует, что оно охватывает остальные стратегические среды.

Традиционным центром внимания при решении проблем безопасности является физическая сфера, последствия киберугроз обычно ограничиваются киберпространством, но они могут распространяться и на физическую сферу. Киберпространство и материальный мир тесно взаимосвязаны. Киберпространство может быть использовано для усиления реагирования систем безопасности в физической сфере.

Рассматривая различные виды угроз в киберпространстве, следует обратить особое внимание на концепцию гибридной войны. Данная тематика была рассмотрена в работах Н. Мэттиса и Ф.Г. Хоффмана [48]. Они выделяют четыре типа вызовов для государства, а именно: 1) традиционные вызовы, 2) нетрадиционные вызовы, 3) катастрофические вызовы, 4) разрушительные вызовы. Война может вестись в разных измерениях, в своей работе Н. Мэттис и Ф.Г. Хоффман вводят в научный оборот проблематику ведения войны «четвертого измерения». Под «четвертым измерением» понимается пространство, в котором противники не находятся физически, но при этом способны оказывать информационное влияние [200]. Политические конфликты в формате гибридных и информационных войн также представлены у Д. Аркилла [42] и Д. Ронфельдта.

В соответствии с работами А.В. Манойло можно дать определение информационной и информационно-психологической войны как противоборства в мировом и локальном информационном пространстве [25]. Данное противоборство осуществляется посредством насильственных и манипуляторных методов и приемов воздействия на информационно-психологическую сферу вражеской стороны с целью достижения поставленных стратегических задач.

Взломы правительственных сайтов и учреждений, кибератаки на элементы критической инфраструктуры представляют собой элементы кибервойны. Поскольку кибервойна более новое явление, чем информационная война, данное понятие определено менее четко. Наиболее просто можно определить кибервойну как вид военных действий,

проводимых посредством компьютеров, интернета [146]. Это использование интернета (электронные способы воздействия) и связанных с ним технологий одним государством с целью причинить ущерб безопасности и суверенитету другого государства. По Р.А. Кларку кибервойна – это действия одного национального государства против другого посредством проникновения в компьютеры или сети атакуемого государства для нанесения ущерба [47].

Военные теоретики Н. Мэттис и Ф.Г. Хоффман [48] указывают на то, что физические атаки, информационные и кибератаки наиболее эффективны при их совмещении. Гибридная война есть синтез различных типов скрытых операций. В данном случае, информационные и кибератаки усиливают влияние от санкционного давления и военных операций.

С.В. Володенков указывает на то, что интернет-коммуникации влияют на политические процессы в обществе [155], при этом через системы ИКТ во время конфликтов производится воздействие на информационное пространство стран-мишеней. К данным воздействиям относятся разрушение ценностных ориентиров и традиций общества, подрыв доверия народа к правительству, разжигание внутригосударственных конфликтов. Сетевая информационная война стала неотъемлемым элементом современной политики на всех уровнях ее организации. Следовательно, конкуренция в мировом информационном пространстве для государства невозможна без системной работы по развитию арсенала онлайн-инструментов влияния на данное пространство. Для стабильности функционирования национального сегмента киберпространства, а как следствие для минимизации рисков для государства в целом, необходимо наличие управленческой и аналитической инфраструктуры по противодействию внешним агрессорам, использующим ИКТ как инструменты коммуникационной агрессии [159].

Развитие цифровых коммуникаций и платформ в России, а также их влияние на политической процесс на современном этапе, рассматриваются на основе работ Е.В. Бродовской [152], А.Ю. Домбровской [166], Р.В. Пармы [198], С.Г. Ушкина [211]. Государству на современном этапе необходимо

урегулировать недовольство граждан не только в физическом пространстве, но и реагировать на виртуальное отображение социального недовольства, которое потенциально может перерасти в народные волнения в физическом пространстве.

Для ведения как оборонительных, так и наступательных действий в информационной войне государству необходимо обладать инфраструктурой и кадрами. Эффективность гибридной войны напрямую зависит от разнообразия привлекаемых для ее ведения сил и средств, а также от качества организации и координации действий.

Основные угрозы для национального сегмента киберпространства, изучаемые в диссертационном исследовании:

- Санкции в сфере ИКТ. Запрет на поставку в Россию новейшего оборудования, программного обеспечения и аппаратного обеспечения (далее – АО) с целью подорвать экономическое и техническое развитие Российской Федерации;

- Критическая зависимость инфраструктуры российского сегмента киберпространства от импорта, в том числе, и из дружественных стран, ставящая государство и общество в неравноправное положение по отношению к внешним акторам;

- Нехватка квалифицированных кадров в сфере ИКТ как следствие ускоренных темпов развития данной области экономики и оттока специалистов за рубеж.

В своих рекомендациях Международный союз электросвязи определяет кибербезопасность как совокупность инструментов, политик, концепций безопасности, практик управления рисками, гарантий и технологий, которые могут быть использованы для защиты киберсреды. Также в данную совокупность входят активы организаций и пользователей [74]. К активам относятся вычислительные устройства, инфраструктура, сервисы и приложения, телекоммуникационные системы, обслуживающий их персонал. Всю совокупность передаваемой и/или хранимой в киберпространстве

информации можно относить к активам. Кибербезопасность в данной работе определяется как состояние защищенности системы ИКТ от кибератак [188].

Как отмечалось, политическая система подвержена внешним влияниям других систем общества, других государств. Степень воздействия на политическую систему других общественных систем и других стран зависит от степени открытости государства (как ядра политической системы). Открытость политической системы создает условия для дестабилизирующих воздействий. О.Ф. Шабров выделяет три фактора, повышающих устойчивость системы [218]. Сюда входят внутренние механизмы адаптации и защиты от сигналов, которые система не способна обработать, а также внешняя среда, поставляющая необходимые компоненты для функционирования системы.

В данном исследовании используется позиция О.Ф. Шаброва, в соответствии с которой между стабильностью и развитием общества постоянно возникают противоречия, разрешаемые посредством меры воздействия государства на систему. Для развития системы необходимо, чтобы она обладала достаточной устойчивостью, чтобы не разрушиться, но при этом она не должна утрачивать способность к качественным изменениям. Под нестабильностью в работах О.Ф. Шаброва понимается состояние, при котором политическая система в функционировании нарушает собственную идентичность и вступает в противоречие со своей сущностью [217]. Вопросы устойчивого развития систем также рассматриваются в работах С.Э. Хайкина [214].

Необходимо рассмотреть понятия «устойчивость» и «устойчивость киберпространства». Устойчивость в системе управления характеризует ее способность выполнять свои функции не только в спокойной, но и в резко меняющейся и кризисной обстановке, а также при деструктивном влиянии среды и противоборствующих сторон [168]. Устойчивость определяется такими свойствами системы, как живучесть, помехоустойчивость, надежность. Сам термин «устойчивость» можно определить, как способность

системы при малых изменениях начальных условий оставаться в положении равновесия.

Сохранение значений показателей управления в установленных пределах в условиях различных кризисных явлений есть необходимый элемент для институтов, отвечающих за функционирование киберпространства страны. Разработка мер повышения устойчивости системы стала очевидной необходимостью после введения санкций против России.

Рассматривая понятие «киберустойчивость» (cyberstability), следует обратиться к результатам исследований Глобальной комиссии по стабильности киберпространства (далее – GCSC) [139]. В их публикациях киберустойчивость определяется как состояние киберпространства, при котором каждый его пользователь может быть обоснованно уверен, что он обладает возможностью безопасно пользоваться данными ресурсами. Для достижения киберустойчивости в соответствии с GCSC следует, в частности, наращивать потенциал киберпространства [121].

Для поддержания состояния устойчивости киберпространства государство должно обладать в нем определенными ресурсами и стать значимым субъектом кибервласти, контролировать и формировать само киберпространство в соответствии со своими целями [49]. Ресурсами государственной власти в киберпространстве являются:

- человеческие ресурсы (наличие специалистов, работников, а также учебных заведений для их подготовки);

- технологии (наличие возможности производить на территории государства все необходимое для поддержания и развития киберпространства на конкурентном международном уровне);

- нормативные и правовые акты, регулирующие развитие и деятельность акторов в национальном сегменте киберпространства;

- организации (подконтрольные государству коммерческие и некоммерческие организации, а также участие государства в международных союзах).

В работах Г.Ю. Никипорец-Такигавы [193], Л.Н Гарас [151], А. Епифановой [228] отмечается, что Российская Федерация активно развивает свои институты по регулированию и совершенствованию интернет-пространства страны. Ярким подтверждением данного факта является принятие закона «О суверенном Рунете» и развитие на его основе новых систем поддержки и регулирования киберпространства. Активное обсуждение данных мер властями России, а также активная реализация данных постановлений в жизнь демонстрирует курс Российской Федерации на укрепление своего положения в киберпространстве. Но при этом на официальном уровне не существует определения термина «суверенный интернет», это, как и многие другие пробелы российского законодательства, осложняет развитие институтов регулирования информационного и киберпространства страны. В рамках проблематики исследования суверенитета государства в информационно-телекоммуникационной сфере также рассматриваются работы А.В. Даниленкова [164], В.Б. Наумова [192], К. Айкенсер [227] и Н. Цагуриаса [242], проблематика технологического суверенитета государства представлена в работах В.В. Иванова [171].

Рассматривая определение границ государства в киберпрострастве, следует обратиться к международным актам, в частности к Таллиннскому руководству 2.0. В соответствии с 8 правилом данного документа государство обладает правом осуществлять территориальную и экстратерриториальную юрисдикцию в отношении данного типа пространства [55] с учетом ограничений, обозначенных в международном праве. Лица и осуществляемая ими деятельность в киберпространстве подчинены юрисдикционным прерогативам (законодательным, судебным и исполнительным) и ограничениям [182], действующим в отношении других форм их деятельности. Таким образом, территориальная юрисдикция

государства распространяется на киберинфраструктуру при наличии определенных факторов. Во-первых, если данная инфраструктура расположена в переделах границ государства. То же относится к лицам, осуществляющим киберактивность на ее территории. Также под юрисдикцию государства подпадает такая деятельность в киберпространстве, которая проводится, завершается или имеет значительное воздействие в пределах государственной территории. Таким образом, суверенитет государства распространяется не только на его физические аспекты, находящиеся на его территории, но и на отношения, затрагивающие национальный сегмент киберпространства.

Ю. Кол при определении того, какую деятельность в интернет-пространстве вправе регулировать конкретное государство, выделяет три подхода [230]:

- «грубый целевой» подход. Если с территории государства можно получить доступ к информации, то законодательство государства распространяется на данную информацию.

- «умеренный целевой» подход. Юрисдикция распространяется, если активность в киберпространстве была непосредственно направлена на данное государство.

- «происхожденческий» подход. Деятельность в киберпространстве подпадает под юрисдикцию только того государства, с территории которого она осуществляется.

На современном этапе в киберпространстве идут процессы «территориализации». Но при этом параллельно идет развитие экстратерриториальных юрисдикционных подходов [242]. К. Айкенсер отмечает, что международно-правовые юрисдикционные правила базируются на суверенитете государств в отношении конкретной территории.

Для целей данного исследования необходимо дать определение термину «взаимодействие». В словаре Т.Ф. Ефремовой значение слова «взаимодействие» определяется как воздействие предметов, явлений

действительности друг на друга, обусловливающее изменения в них [21]. Термин «взаимодействие» можно определить как взаимообусловленный процесс воздействия двух и более субъектов друг на друга, и в зависимости от конкретных обстоятельств достижение целей субъектов может носить как сильную, так и слабую корреляцию, она также может быть положительной, отрицательной или нейтральной.

Под взаимодействием понимается взаимная связь, обусловленность, а также взаимодействие общественных явлений [14]. Взаимодействие – это воздействие вещей друг на друга для отображения взаимосвязей между различными объектами [34]. На современном этапе перед социальными, экономическими и политическими субъектами стоит задача сформировать систему взаимодействия власти и бизнеса, отвечающую как принципам государственного регулирования экономики в общественных интересах, так и мотивационным установкам бизнеса.

В работах В.В. Радаева под взаимодействием понимается экономические сделки, которые являются обменом благами. Данное взаимодействие является конституирующим для рыночного обмена. Но взаимодействия между акторами не сводятся только к обмену ресурсами, они также пронизаны властными отношениями, которые формируются за счет неравенства способностей игроков в реализации своих интересов. Любые экономические сделки также проходят в рамках реализации властных взаимодействий. Рассматривая конкуренцию как отдельный тип взаимодействия, В.В. Радаев определяет ее как соперничество двух и более участников рынка за внимание третьего игрока или соперничество за ограниченные ресурсы. Следующим типом взаимодействия участников рынка является установка и поддержание социальных связей между собой как устойчивых непосредственных взаимодействий. Этот тип отношений формируется во внеконтрактной зоне конкурентных отношений. Причем данный тип связей формируется даже между конкурентами [31].

1.2 Методология и методика изучения согласования интересов государства и бизнеса в обеспечении устойчивости российского сегмента киберпространства

В данном параграфе систематизирована методологическая основа исследования. Обосновывается применимость к предмету исследования системного и неоинституционального подходов, валидность статистических методов, теории игр и SWOT-анализа, модели «пяти сил Портера». Дается определение базовым понятиям – «киберпространство», «стратегия», «интерес»; обосновываются перечни акторов, формирующие множества «государство» и «бизнес». Конечным этапом является процедура структурной операционализации для проведения эмпирического исследования.

Для поддержания устойчивости киберпространства требуется множество взаимосвязанных мер правового, ресурсного, организационного, кадрового и иного характера, которые раскрыты в данной работе в рамках взаимодействия власти и бизнеса.

Для проведения исследования согласования интересов государства и бизнеса в сфере-ИТ по обеспечению устойчивости национального сегмента киберпространства, необходимо рассмотреть их взаимодействия как систему. Системный подход является методологической основой исследования. В основе данного подхода лежит анализ объекта как системы, состоящей из взаимодействующих элементов, функционально сопряженных сетью интеракций, обратных связей, ресурсных обменов. Подход ориентирован на определение многообразия типов связей объекта и на сведение их в единую теоретическую картину [20].

Системный анализ в узком смысле – это совокупность методологических средств для подготовки и обоснования решений по сложным проблемам [7]. Как указывает Г.Б. Клейнер, основными принципами системной парадигмы являются: изучение системы в целом, но

при учете взаимосвязи с ее элементами; комплексный характер исследования, не ограниченный одной дисциплиной; основное внимание в исследовании уделяется постоянно действующим институтам; устанавливаются исторические причинно-следственные связи процессов и событий; индивидуальные предпочтения субъектов диктуются системой, в которой они функционируют; упор на исследование процессов трансформации систем; каждая система обладает специфичными свойствами; свойства системы объясняются исследователями путем их сравнения с аналогичным свойствами другой системы. Объединение систем само является системой, объектом, процессом, средой [176].

В свою очередь, Т. Парсонс стал одним из первых, кто применил системный подход в сфере политики. В его подходе политическая система общества представляется в виде «черного ящика», обладающего входами, выходами, а также обратной связью. Первичная необходимость общества – это мотивация человека к внесению вклада в поддержание общественной системы, участию, а также согласие индивида с нормативными порядками. Механизмы воздействия общества на поведение человека проявляются в трех взаимосвязанных системах разного уровня: в социальном действии, социальной системе и социетарной общности. Социальная система состоит из взаимоотношений и ролей индивидов в определенной физической среде [29].

Д. Истоном создана модель взаимодействия политической системы с внешней средой. Политическая система – динамическое явление, обладающее способностью к саморегуляции и к адаптации к внешним изменениям. Происходит непрерывное взаимодействие политической системы с окружающей средой. Политическая система, откликаясь на «требования» и «поддержку» внешней среды, воздействует на нее посредством политических решений – «выход». В свою очередь, внешняя среда порождает реакцию на данное воздействие, выражающееся в новых

требованиях к политической системе – «вход», на что политическая система реагирует новыми актами [229].

В своих работах Г. Алмонд дополняет Д. Истона и определяет политическую систему как упорядоченную совокупность взаимодействий внутри системы и с окружающей средой. Она выполняет функции интеграции и адаптации к окружающей среде посредством применения или угрозы применения принуждения. Так же осуществляется взаимодействие с другими обществами. Г. Алмонд отмечает, что, несмотря на различие политических систем в разных государствах, системы везде выполняют практически одинаковые функции [223].

Н. Луман называет свой подход функциональным структурализмом. Соотнесение элементов во времени уточняется понятием структуры. На первый план выходит проблематика структуры и изменения. Изменения происходят в отношении структур, но не событий. В свою очередь, процессы не могут завершаться сами и зависят от внешней интерференции, а также от недостатков возможностей новых структурных образований, процессы развиваются скачкообразно. В трактовке Н. Лумана основной ролью политической подсистемы общества является осуществление коммуникации общественных подсистем. Н. Луман отмечает, что у систем есть границы, выполняющие функцию разделения и связывания системы и окружающего ее мира. При наличии четких границ элементы причисляются либо к системе, либо к окружающему миру [17].

В данной работе российский сегмент киберпространства рассматривается как отдельная система, материальным ядром которой являются подсистемы органов государственной власти и компаний ИТ-сектора. Пользователями и поставщиками ресурсов системы становятся физические и юридические лица в различных организационно-правовых формах.

Неоинституциональный подход анализирует влияние институтов, понимаемых как правила игры, на экономические, политические,

культурные, социальные практики, при этом исторические, культурные, идеологические особенности общества и государства оказывают влияние на институты [23]. Акторы политической сферы обладают полномочиями создавать официальные (формальные) институты и контролировать легальные механизмы исполнения контрактов. При этом сами акторы ограничены своими стратегиями и ресурсным потенциалом [194]. От баланса формальных и неформальных институтов зависят характеристики и результаты деятельности различных сфер общественной жизни. Р. Коуз определяет институты общества как инструменты сдерживания оппортунистического поведения людей, а также минимизации транзакционных издержек [13]. В своих работах Р. Коуз вводит понятие «транзакционные издержки», которые определяет как издержки, возникающие в процессе сбора и обработки информации, а также в процессе принятия решений и проведения переговоров. Среди зарубежных представителей неоинституционального подхода также следует указать Дж. Олсена [232] и Дж. Марча, а среди российских Ю.В. Ирхина [174].

Существуют два направления неоинституционализма: нормативный и исторический. В случае нормативного неоинституционализма центральным объектом исследования является набор норм и ценностей, определяющих поведение членов общества [202]. В больших группах людей организованное поведение основывается на существовании функциональных кодов, ведь человеческая организация невозможна без понимания большинством членов правил группы. Необходимо, чтобы при разработке новых законов они не противоречили устоявшимся понятиям в обществе. В свою очередь, исторический институционализм исследует трансформации институтов общества, причем в исследовании учитываются как исторические события, так и их исторический контекст [189].

Одновременно с развитием информационно-коммуникационных технологий происходит изменение формальных и неформальных институтов. Учитывая контекст санкций и проведения специальной военной операции,

представляет исследовательский интерес вопрос о балансе формальных и неформальных институтов и влиянии этого баланса на устойчивость национального сегмента киберпространства.

В рамках исследования целесообразно использовать в качестве методологического инструмента элементы теории игр, рассматривающей поведение акторов, стремящихся достичь своих интересов. Среди классиков теории игр следует выделить работы таких исследователей как: Д. Розенау [54], Дж.М. Смит [56], Дж. Нэш [234], Дж. Нейман [235], А. Раппопорт [53], Т. Шеллинг [41], Л. Шепли [239], Р. Льюс и Х. Райф [18].

Понятие «игра» определяется как процесс, в котором два и более игроков за счет применения различных стратегий ведут борьбу за реализацию своих интересов. Каждая сторона использует определенные стратегии, которые могут привести как к успеху (игра с положительной сумой), так и к неудаче (игра с отрицательной суммой) в зависимости от стратегий других сторон. Теория игр базируется на постулате, что поведение индивидов рационально, что позволяет выбрать наилучшие стратегии для конкретных акторов игры [38].

Для целей данного исследования представляют интерес концепты «игра с нулевой/положительной/отрицательной суммой», «равновесие Нэша» «Парето-эффективность» [234]. Три возможных исхода: нулевая, положительная, отрицательная сумма могут быть интерпретированы как результаты взаимодействия акторов как внутри одного поля, так и акторов из разных полей. Исследовательский вопрос заключается в сравнении указанных результатов и применении предложенных Н. Флигстином и Д. Макадамом стратегий принуждения, соперничества, кооперации [213]. Равновесие Нэша, понимаемое как невозможность в одностороннем порядке улучшить свое положение в игре (получить б*о*льшую выгоду), показывает баланс ресурсов акторов и степень прочности сложившейся иерархии внутри поля и между различными полями. Концепт «Парето-эффективность», понимаемый как максимизация общей выгоды игроков, гипотетически может

быть рассмотрен в качестве индикатора устойчивости национального сегмента киберпространства как системы.

В экономике термин «интерес» можно определить как «предмет заинтересованности, желания и побудительных мотивов действий экономических субъектов» [4]. В социологии и политологии «интерес» – это реальная причина деятельности субъектов [32]. Данная причина направлена на удовлетворение потребностей субъектов. Она определяется ролью субъекта в системе общественных отношений. По И. Канту интерес - это причина, определяющая волю разумного существа [10]. В данной работе под термином «интерес» понимается желаемый результат, на достижение которого направлена деятельность.

Для проведения анализа стратегий акторов необходимо проанализировать подходы к определению понятия «стратегия». И. Ансофф под понятием «стратегия» понимает набор правил по принятию решений, которыми организация руководствуется в своей деятельности [1]. В соответствии с определением Л. Фридмана, стратегия – это наука о поддержании баланса между целями, способами, средствами, которая направлена на определение целей, ресурсов и методов достижения данных целей [39].

В данной работе под стратегиями акторов политики и экономики понимаются «обобщенные планы действий на основе ресурсного потенциала, формальных и неформальных институтов, властных позиций внутри поля для достижения определенных целей». Под целью в данной работе понимается предвидимый и желаемый результат, на достижение которого направлены действия актора. В свою очередь, под «оптимальной целью» понимается «предвидимый максимально-достижимый результат в рамках принятых политик» [167].

Противоречия между государством и бизнесом связаны с фундаментальной проблемой перераспределения ресурсов. Бизнес стремится увеличить свою прибыль, программы социальной ответственности и

налогообложение для каждой конкретной фирмы означают уменьшение прибыли. Государство как аппарат управления стремится к такому уровню контроля над экономическими субъектами и такому уровню изъятия ресурсов, которые бы позволили достичь двух целей, с одной стороны, максимизации власти и доходов самого аппарата, с другой стороны, поддержания и развития всех систем общества [9].

Необходимо отметить, что универсального подхода к разработке стратегии не существует. В качестве лидеров разработки процедур формирования стратегий можно выделить представителей Гарвардской школы бизнеса, в частности, в данном исследовании используется подход «пяти сил» М. Портера.

Модель «пяти сил» М. Портера позволяет проанализировать взаимное влияние внешнего окружения и изучаемого субъекта (организации, фирмы). Устанавливается степень зависимости (властного контроля над ресурсом) по отношению к клиентам, поставщикам, конкурентам [51]. В своих работах М. Портер проводил исследование экономических структур различных сфер экономики [30]. Сила, обладающая наибольшим влияниям на систему конкуренции, должна являться основой для формулирования стратегии развития субъекта. Хотя концепция М. Портера изначально разрабатывалась для бизнес-субъектов, она может быть применена для анализа органов государственной власти, некоммерческих организаций.

Выбор экономической стратегии в период кризиса представлен тремя вариантами: стратегия закрытия (ликвидации); стратегия развития; стратегия выживания [20]. Ж. Сапир указывает на необходимость четкого разграничения стратегии государства и стратегии компании [238].

Стратегия выстраивается исходя из ожидаемых результатов и целей, возможностей/ресурсов актора, внешних условий. Следует выделить три типовые стратегии.

- Стратегия зависимости характеризуется наличием агрессивной окружающей среды, а также нехваткой ресурсов для поддержания

функционирования актора. В данных условиях основной целью актора становится сохранение своего существования, чего можно добиться посредством попадания в зависимость от других акторов, обладающих необходимыми ресурсами. Стратегия зависимости ведет к потере самостоятельности.

- Стратегия выживания характеризуется негативной окружающей средой и/или нехваткой ресурсов, не позволяющей поддерживать стабильное развитие актора. Целью данной стратегии является минимизация получаемого ущерба в краткосрочной перспективе для возобновления активного роста в будущем.

- Стратегия развития характеризуется наличием благоприятной окружающей среды и/или достаточным количеством ресурсов для поддержания стабильного развития актора. Целью в данной стратегии является максимизация получаемой выгоды, основываясь на имеющихся преимуществах актора.

Специфика применения стратегий зависимости, выживания, развития по отношении к ИТ-бизнесу и государству рассмотрено в таблице 1.

Таблица 1 – Стратегии поведения государства и ИТ-бизнеса

Стратегия	ИТ-Бизнес	Государство
1	2	3
Стратегия зависимости / возвращение к старому	Попытки наладить старые связи и/или заменить их новыми аналогичными отношениями, встраивание в глобальные производственные цепочки, максимальный импорт дефицитных товаров	Действия для восстановления старого международного статус-кво/ воссоздание старых отношений с новыми государствами. Открытие сектора для зарубежных акторов, готовых инвестировать ресурсы
Стратегия выживания	Сохранение и консервация технологий, компетенций, минимизация потерь с опорой на получение дефицитных ресурсов от фирм дружественных стран	Направление усилий на недопущение падения секторов экономики, легализация и содействие в получение дефицитных ресурсов из дружественных стран, приоритет государственного

Продолжение таблицы 1

1	2	3
		финансирования сферы Открытие сектора для зарубежных инвесторов дружественных стран
Стратегия развития	Максимальное импортозамещение, укрепление отечественной производственной базы с установлением сбалансированных отношений с фирмами разных стран с минимальным встраиванием в глобальные цепочки и максимальной диверсификацией дефицитного импорта	Сочетание административных и рыночных стимулов для развития сферы; выстраивание прагматичных и взаимовыгодных отношений с различными странами, корпорациями для получения отечественными фирмами максимально возможного доступа к дефицитным ресурсам при реализации максимального импортозамещения

Источник: составлено автором.

Под государством в настоящем исследовании понимаются следующие органы государственной власти, непосредственно участвующие во взаимодействии с компаниями ИКТ-сферы: Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации; Министерство экономического развития Российской Федерации; Правительство Российской Федерации; Президент Российской Федерации; Федеральная служба безопасности Российской Федерации; Федеральная служба по техническому и экспортному контролю Российской Федерации; Министерство труда и социальной защиты Российской Федерации; Министерство финансов Российской Федерации; Федеральная налоговая служба Российской Федерации; Государственная Дума Федерального Собрания Российской Федерации, Министерство науки и высшего образования Российской Федерации.

Рассматривая понятие «бизнес», необходимо обратиться как к научным работам, так и к законодательным документам. Бизнес можно определить, как инициативную экономическую деятельность [3]. Данная деятельность

осуществляется за счет собственных или заемных средств, на свой риск и под свою ответственность. Цель данной деятельности заключается в получении прибыли и развитии собственного дела. А.Н. Асаул указывает в своих работах, что предпринимательство отличается от бизнеса наличием новаторства, которое становится причиной нарушения рыночного равновесия [26]. Бизнес может определяться как «деловая активность, направленная, в конечном счете, на совершение коммерческих операций по обмену товарами или услугами, результатом которых может быть получение прибыли или несение убытков» [33]. В данное определение входят как деятельность на постоянной основе, так и разовые коммерческие сделки. Бизнес может определяться как «экономическая деятельность субъекта в условиях рыночной экономики, нацеленная на получение прибыли путем создания, реализации определенной продукции или услуг…» [22]. Бизнес понимается как стабильная экономическая деятельность, нацеленная на получение прибыли и удовлетворение потребностей общества [173]. Если рассмотреть Гражданский кодекс Российской Федерации, то под бизнесом (предпринимательская деятельность) понимается самостоятельная профессиональная деятельность. Данная деятельность осуществляется на свой риск. Ее целью является систематическое получение прибыли посредством использования имущества, продаж товаров, а также осуществления работ или оказания услуг [59].

В данном исследовании используются понятия «бизнес» и «предпринимательская деятельность» как синонимы, так как, несмотря на их особенности, они являются взаимосвязанными элементами современной экономики, в Российском законодательстве данные понятия также являются синонимами. Понятие «бизнес» предполагает совокупность деловых, инициативных отношений по оказанию услуг в конкретном виде экономической деятельности. Данные отношения осуществляются посредством обмена в условиях рынка, на свой риск для получения прибыли. Данное определение позволяет наиболее полно охватить сферу бизнеса

Российской Федерации в сфере информационно-коммуникационных технологий, так как оно включает как систематическое производство и предоставление услуг, так и деятельность по разработке новых товаров и услуг, что особенно важно в сфере высоких технологий.

Конкретизируя вышесказанное, необходимо определить критерии выделения компаний ИТ-сферы, которые в процессе эмпирического исследования представляют непосредственный предмет анализа. В качестве «бизнеса» в данной работе рассматриваются наиболее крупные компании в сфере ИТ.

Для определения пула наиболее крупных компаний на российском рынке ИТ использовался рейтинг Аналитического центра «TAdviser» за 2023 год, из которого для анализа было взято 100 наиболее крупных компаний [180]. Данный рейтинг выбран из-за того, что «TAdviser» является российским интернет-порталом и аналитическим агентством, одним из основных направлений специализации которого являются информационные технологии. Был взят рейтинг за 2023 год, так как в нем учитываются результаты деятельности компаний за 2022 год. На основе представленных в рейтинге данных можно сделать выводы о перечне наиболее крупных игроков российского сегмента ИТ-компаний после начала специальной военной операции. Данные о компаниях для исследования их состояния в период с 2020 г. по 2023 г. были собраны посредством использования системы СПАРК-Интерфакс. Полный перечень компаний представлен в приложении Б.

А.В. Манойло, рассматривая кибербезопасность и кибероборону на примере НАТО и БРИКС, отмечает, что данные организации выстраивают стратегии обороны и защиты с применением понятия «киберпространство» [187]. Так, НАТО рассматривает киберпространство как пятую сферу ведения современной войны [188]. В работах С.В. Володенкова указывается необходимость изучения опыта ведения операций в киберпространстве, развития систем кибербезопасности и регулирования отношений государств

в данной области [156]. Таким образом, термин «киберпространство» представлен в зарубежных правовых документах. В Белой книге «Военная стратегия Китая» 2015 года отмечается, что киберпространство является одной из четырех сфер безопасности, наравне с морской, космической и ядерной безопасностью [70].

С.В. Володенков анализирует влияние киберпространства на общество и индивида, а также развитие процессов репрезентации граждан в киберпространстве [160]. Отмечается тенденция активной политизации киберпространства [157] . С.Ив Лоран в своих работах указывает на то, что киберпространство оказывает стратегическое влияние как на социальные процессы общества, так и на политический контекст. Оно обладает сложной архитектурой и является новой социально-технической реальностью [190].

С. Кутюр и С. Тоупин подразделяют цифровой суверенитет на пять подкатегорий, среди которых выделяется «суверенитет киберпространства» [158]. В исследованиях ставится проблема правового регулирования киберпространства [203]. Обсуждается возможность применимости к новому типу пространства существующих норм международного права [172].

Таким образом, термин «киберпространство» представлен в российской и зарубежной науке, а также в законодательных актах зарубежных государств и международных союзов. Основные направления исследования киберпространства посвящены: ведению боевых действий в киберпространстве; вопросам международного права (границы государств и их взаимоотношения в киберпространстве); киберпреступность и кибербезопасность.

Ж. Липтон обозначил основные черты киберпространства: глобальное распространение сети «интернет»; особые нормы поведения в киберпространстве в отличие от норм в «физическом» мире; виды ущерба от недобросовестного поведения в киберпространстве [50]. Понятие киберпространства раскрывается в трех аспектах: физическом, информационном, социальном [210]. Оно охватывает все компьютерные сети

мира как изолированные, так и подключенные к интернету. Киберпространство включает в себя все множество взаимосвязанных систем и структур. При подключении устройства к киберпространству оно становится его частью, его ресурсы становятся частью общей совокупности ресурсов киберпространства. На раннем этапе формирования киберпространства человек являлся исключительно его разработчиком, но на современном этапе в определенных сферах жизнедеятельности человек сам стал элементом киберпространства, продолжая его развивать [208]. Н. Цагориас отмечает, что киберпространство состоит из физической инфраструктуры пользующихся компьютерами людей и не обладает определенной территорией [242]. Результатом объединения функциональных элементов киберпространства (средства каналообразования, средства хранения информации) является реализация процессов по обеспечению информационного обмена и формированию информационных услуг. Основной функцией киберпространства является интерактивная и виртуальная среда для большого количества участников [175].

В своих работах А.В. Курилкин рассматривает различные подходы к термину «киберпространство» [83]. В частности, им выделяется определение М. Майера: киберпространство это глобальная, изменчивая динамическая область, характеризующаяся использованием электричества и электромагнитного спектра. Киберпространство включает в себя: физическую инфраструктуру и телекоммуникационные устройства; компьютерные системы и сети; узлы доступа пользователей и промежуточные узлы; «сети сетей» – сети, связывающие отдельные компьютерные сети, а также составные данные и данные пользователей. Киберпространство не является иерархической сетью [233]. А. Стрельцов определяет понятия «киберпространство» и «ИКТ-инфраструктура» как идентичные: «совокупность средств, систем и сетей, используемых для оказания услуг телекоммуникационной связи и автоматизированной обработки информации, а также организационной инфраструктуры,

предназначенной для создания и эксплуатации соответствующих средств, систем и сетей, включающее в себя две основные составляющие – телекоммуникационную среду и информационную среду» [209]. В монографии Г.Ю. Филимонова, О.Г. Карповича и А.В. Манойло киберпространство определяется как «метафорическая абстракция, используемая в философии и в компьютерах, виртуальная реальность, которая представляет ноосферу, второй мир как «внутри» компьютеров, так и «внутри» компьютерных сетей» [36]. Ю.И. Стародубцев, П.В. Закалкин, С.А. Иванов определяют киберпространство как «искусственное неоднородное технологическое пространство с множеством разноуровневых органов оперативного и технологического управления, процесс создания и эксплуатации которого не предопределяется требованиями одной системы управления, а функционирует в интересах множества разнородных, в том числе, антагонистических систем управления, при этом свойства киберпространства зависят как от характеристик собственных элементов, так и от объема и свойств реализуемых процессов в интересах внутренних и внешних потребителей» [208].

«Киберпространство» не синонимично понятию «цифровое пространство», которое является более широким [161]. Цифровое пространство включает в себя «киберпространство», «интернет-пространство», «онлайн-пространство» или «виртуальное пространство». Цифровое пространство – это, скорее, вид перцептуального или концептуального пространства, нежели реального. Цифровое пространство включает в себя цифровую инфраструктуру (аппаратные средства, программное обеспечение) и цифровые ресурсы (базы данных, оцифрованные образы физических объектов), средства цифрового взаимодействия (процессы, технологии, методы управления) [207]. Можно выделить социологический, классический экономический, технико-технологический подходы к определению цифрового пространства [220]. В рамках технико-технологического подхода можно определить

цифровое пространство, как «набор систем, подсистем, сгруппированных по областям и сферам и взаимодействующих между собой на базе единой платформы с интерфейсами для заинтересованных пользователей. Цифровое пространство – это информационная проекция реального пространства, искусственно созданная, поддерживаемая и развиваемая человеком» [215]. С другой стороны, «цифровое пространство» можно определить как систему идей, ожиданий, практик и операций, являющихся продуктом не только технологий, но в большей степени создавших и пользующихся ими людей [161]. А.П. Сидорова указывает на то, что «цифровое пространство» виртуально включает в себя разноплановую информацию, а также объединяет разносторонние действия, путем использования персонализированных автоматических средств, что позволяет эффективно обрабатывать и передавать информацию [207]. Цифровое пространство можно определить как «пространство, интегрирующее цифровые процессы, средства цифрового взаимодействия, информационные ресурсы, а также совокупность цифровых инфраструктур, на основе норм регулирования, механизмов организации, управления и использования» [65].

В работе В.Л. Гирича и В.Н. Чуприной информационное пространство определяется как «совокупность информационных ресурсов и инфраструктур, которые составляют государственные и межгосударственные компьютерные сети, телекоммуникационные системы и сети общего пользования, иные трансграничные каналы передачи информации» [162]. А.В. Манойло предлагает универсальную модель информационного пространства, включающего информационное поле, информационные потоки, каналы коммуникации СМИ и МК [19]. Таким образом, информационное пространство - это совокупность общественных отношений по хранению, обработке, передаче, обмену, распространению и созданию информации [87]. Данная информация может быть представлена в электронном, компьютерном, телевизионном, радио, бумажном и иных форматах.

В данном исследовании используется следующее определение киберпространства. **Киберпространство** – это созданная для обмена информацией гибридная площадка (платформа), формируемая из совокупности всех информационных устройств, хранящих, обрабатывающих, передающих информацию и задействованных в функционировании сети интернет, а также субъектов коммуникационных, технологических, регуляторных процессов [177]. В документах Российской Федерации не используется термин «киберпространство». Вместо него был выбран термин «информационное пространство», что является более широким понятием.

В настоящем исследовании дается следующее определение понятию «устойчивость политической системы» – это динамическое состояние политической системы, позволяющее ей в условиях меняющейся реальности как сохранять свое равновесие, противостоя внутренним и внешним угрозам, так и производить необходимые и допустимые изменения внутри себя.

Устойчивость киберпространства – это динамическое состояние процессов обмена информацией в гибридном пространстве, обеспечиваемое за счет индивидуальной устойчивости подсистем, из которых оно состоит, а именно: обеспечения стабильной передачи данных, оперативной ликвидации нарушений, а также постоянного развития и обновления технологических, кадровых и регуляционных систем.

Существуют различные подходы к определению национального сегмента киберпространства. Можно проводить его разграничение по Национальной системе доменных имен или по доминирующему языку коммуникации. Но наиболее четким определением границ государства в киберпространстве является зона распространения государственной юрисдикции киберпространства.

Исходя из этого, определяется, что границы государственного суверенитета в национальном сегменте киберпространства определяются системой подчиненных юрисдикции государства взаимоотношений

участников коммуникационных, технологических, регуляторных процессов киберпространства.

Следует определить составные элементы национального сегмента киберпространства Российской Федерации [58]:

- научно-производственная база государства;

- государственная система аутентификации и шифрования;

- аминистративные и технологические процессы по удалению противоправного контента и внесению в черный список сайтов распространителей;

- проводимая интернет-провайдерами по заказу государства политика по развитию целевых систем наблюдения, массовой локализации и хранение данных интернет-трафика;

- критические информационные инфраструктуры и связанная с ними законодательная база;

- системы осуществления информационно-технологических и информационно-психологических контрмер;

- системы обратной связи, мониторинга, контроля и управления.

В данной работе исследуется взаимодействие органов государственной власти и бизнеса, занимающегося техническим обеспечением функционирования инфраструктуры киберпространства, а также взаимодействие по вопросам удовлетворения спроса на подготовку кадров для ИТ-сектора. Баланс взаимодействий государства и бизнеса в области производства материальной части, программного обеспечения, кадровой подготовки как раз и создает состояния устойчивости национального сегмента киберпространства. Обеспечивает технологический суверенитет государства как способность экономики страны самостоятельно производить высокотехнологичную продукцию, которая необходима для решения стратегических задач государственного развития. Суверенитет российского государства в информационно-телекоммуникационной сфере основывается на замещении продукции недружественных стран отечественными аналогами

или продукцией из дружественных стран, а также полученной через схемы параллельного импорта. В настоящей работе под взаимодействием понимается взаимное влияние двух и более субъектов, оказываемое друг на друга в процессе осуществления ими деятельности по достижению их интересов.

Учитывая вышеуказанные методологические подходы, теории и концепции был осуществлен выбор методов исследования. Для анализа взаимодействий государства и бизнеса, рассматриваемых как коммуникативные поля (подсистемы) системы национального сегмента киберпространства использовалась методика ресурсно-акторного анализа. Она позволяет исследовать типы ресурсов, акторов, задействованные институты и стратегии [205]. Для анализа развития компаний ИТ-сферы, определения санкционного эффекта, влияния государственного регулирования национального сегмента киберпространства использовались статистические методы анализа [145]. Они дают возможность исследователю оперировать количественными характеристиками различных свойств совокупности анализируемых объектов [147].

Метод SWOT-анализа основан на определении сильных и слабых сторон организации в определенном поле, возможностей и угроз, которые могут реализоваться под влиянием внешней среды [185]. SWOT-анализ применялся в процессе оценки перспектив достижения конгруэнтности стратегий органов государственной власти и ИТ-бизнеса в условиях внешних вызовов. Хотя SWOT-анализ в основном используется для анализа бизнес-среды, он также активно применяется в других областях, в том числе, и в политологии. SWOT-анализ есть стратегический ситуационный анализ политических механизмов и акторов политических процессов [148].

Для анализа согласования интересов государства и бизнеса использовался инструментарий теории игр в форме платежных матриц.

Помимо специализированных методов в работе используются и общенаучные методы. Анализ – метод, направленный на разложение объекта

на составляющие его элементы. В свою очередь, синтез позволяет объединить результаты анализа в общее целое. Анализ и синтез являются взаимодополняющими методами. Индукция позволяет вывести общее положение из изучения ряда частных единичных фактов. Дедукция – это аналитическое рассуждение от общего к частному. Дедукция базируется на принципе обобщения. Исторический метод заключается в выявлении исторических фактов и в воссоздании на их основе исторических процессов и логики их развития. Логический метод основан на изучении закономерностей, причинно-следственных связей процессов и явлений. Под вторичным анализом данных в данной работе понимается совокупность методов и приемов получения нового знания, посредством применения к информации из ранее проведенных исследований новых исследовательских целей, задач, методик и методов анализа информации. Анализ нормативно-правовых документов состоит в смысловой интерпретации источников информации.

Результаты структурной операционализации взаимодействия государства и ИТ-бизнеса представлены в таблице 2.

Таблица 2 – Структурная операционализация

Показатели	Переменные	Индикатор
1	2	3
Ресурсно-акторный анализ		
Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации	Нормативно-правовые акты	Приказы и рекомендации, затрагивающие сферу ИТ
	Особо значимые проекты	Выдано на проект – млрд рублей Количество проектов Количество видов деятельности, подпадающих под категорию ИТ Количество программ Срок действия программ
	Лицензирование в сфере ИТ	Количество компаний, прошедших лицензирование продукции Количество лицензионных списков Количество лицензионных требований

Продолжение таблицы 2

1	2	3
	Вывоз с территории страны товаров Утверждение перечня видов деятельности в области ИТ Реализация государственных проектов в сфере ИТ Субсидирование компаний Образование	Количество правил Количество выданных разрешений Количество видов деятельности в сфере ИТ Количество государственных проектов в сфере ИТ Количество прошедших отбор компаний Размер субсидий млн руб. Перечень приоритетных специальностей – количество
Государственная Дума Федерального Собрания Российской Федерации	Нормативно-правовые акты Налоговые льготы	Федеральные законы Налоговые вычеты в процентах Пониженная ставка в процентах суммы начисленных налогов к уплате – млн руб.
Министерство экономического развития Российской Федерации	Нормативно-правовые акты Определение национальных целей Экспериментальный правовой режим в сфере ИТ Стимулирование спроса на инновационную продукцию	Приказы Национальные цели в сфере ИТ Количество программ по достижению целей Количество требований, необходимых для присоединения компании к режиму Количество задействованных компаний Срок действия экспериментального правового режима Срок участия субъекта экспериментального правового режима Территории режима Количество продукции в перечне инновационной, высокотехнологичной продукции Процент повышения спроса на инновационную продукцию, произведенную в регионе, со стороны компаний с государственным участием и естественных монополий Процент повышения спроса на инновационную продукцию со стороны региональных органов исполнительной власти и их подведомственных организаций

Продолжение таблицы 2

1	2	3
Правительство Российской Федерации	Нормативно-правовые акты Субсидии из федерального бюджета бизнесу в сфере ИТ Правила предоставления права на получение отсрочки от призыва Налоговые и таможенные льготы Утверждение концепции технологического развития страны Аккредитация организации	Постановления и распоряжения Правила отбора компаний и предоставления субсидий. Количество граждан, получивших отсрочку Количество перечней (по типу материалов и продукции) Размер налоговых ставок по налогу на прибыль организаций в процентах Размер тарифов страховых взносов в процентах Количество положений концепции Количество аккредитованных ИТ-компаний
Президент Российской Федерации	Нормативно-правовые акты Меры по обеспечению ускоренного развития ИТ-сферы страны	Указы Президента Российской Федерации Количество мер
Федеральная служба безопасности Российской Федерации	Нормативно-правовые акты Защита информации Мониторинг защищенности информационных ресурсов Лицензирование	Приказы Количество требований по защите информации Количество проверок по определению защищенности информационных ресурсов Количество и содержание требований необходимых для прохождения лицензирования
Федеральная служба по техническому и экспортному контролю Российской Федерации	Нормативно-правовые акты Лицензирование Профилактика нарушений	Приказы Количество компаний, прошедших лицензирование продукции Количество лицензионных списков Количество лицензионных требований Количество проверок Количество профилактических мероприятий
Министерство труда и социальной защиты	Нормативно-правовые акты Утверждение профессионального стандарта специалистов	Приказы Количество требований для профессионального стандарта специалистов

Продолжение таблицы 2

1	2	3
Российской Федерации		Количество ИТ профессий с установленными стандартами
Министерство финансов Российской Федерации	Нормативно-правовые акты	Приказы, письма
Федеральная налоговая служба Российской Федерации	Нормативно-правовые акты Налоговые проверки аккредитованных ИТ-организаций	Письма Количество проверок Срок льготного периода налоговых проверок
Министерство науки и высшего образования Российской Федерации	Нормативно-правовые акты ИТ-образование	Количество программ повышения квалификации в сфере ИТ Количество бюджетных мест в вузах по ИТ специальностям Количество платных мест в вузах по ИТ специальностям Количество студентов, обучаемых в вузах по программам бакалавриата на ИТ специальностях Количество студентов, обучаемых в вузах по программам магистратуры на ИТ специальностях
Федеральное агентство по управлению государственным имуществом	Нормативно-правовые акты Вхождение в капитал	Методические рекомендации Количество ИТ-компаний, в которых государству принадлежит пакет в размере 100 %; Количество ИТ-компаний, в которых государству принадлежит контрольный пакет акций; Количество ИТ-компаний, в которых государство выступает миноритарным акционером.
Бизнес Фирмы ПО	Выручка Прибыль/убыток Налоги Руководитель Совладельцы Размер предприятия	Выручка – млрд руб. Прирост выручки по сравнению с предыдущим годом в процентах Прибыль/убыток – млрд руб. Налоги – млн руб. Руководитель – физическое лицо Совладельцы – физические и юридические лица Размер предприятия – количество занятых

Продолжение таблицы 2

1	2	3
	Дочерние компании Филиалы Деятельность по ОКВЭД	Дочерние компании – количество Филиалы – количество Деятельность по ОКВЭД – виды основной деятельности
Бизнес Фирмы ПО	Арбитражные дела с органами государственной власти - Санкции - Государственные контракты - Государственная поддержка	Количество дел в качестве истца Количество дел в качестве ответчика Процент выигранных дел в качестве истца Процент выигранных дел в качестве ответчика Вид ограничительных мер Государственные контракты – млн руб. Государственная поддержка – млн руб.
Бизнес Фирмы АО	Выручка Прибыль/убыток Налоги Руководитель Совладельцы Размер предприятия Дочерние компании Филиалы Деятельность по ОКВЭД Арбитражные дела с органами государственной власти Санкции Государственные контракты Государственная поддержка	Выручка – млрд руб. Прирост выручки по сравнению с предыдущим годом в процентах Прибыль/убыток – млрд руб. Налоги – млн руб. Руководитель – физическое лицо Совладельцы – физические и юридические лица Размер предприятия – количество занятых Дочерние компании – количество Филиалы – количество Деятельность по ОКВЭД – виды основной деятельности Количество дел в качестве истца Количество дел в качестве ответчика Процент выигранных дел в качестве истца Процент выигранных дел в качестве ответчика Вид ограничительных мер Государственные контракты – млн руб. Государственная поддержка – млн руб.
Матрица теории игр		
Государство	Стратегия зависимости / возвращение к старому	(-2) – Зависимость (утрата независимости сегмента киберпространства и переход на иностранное обеспечение и регулирование)

Продолжение таблицы 2

1	2	3
		(-1) – понижение стабильности киберпространства из-за увеличения иностранного влияния
	Стратегия выживания	(0) – Выживание (сохранение стабильности киберпространства)
	Стратегия развития	(1) – Повышение стабильности киберпространства за счет доли и качества участвующих в его поддержании отечественных компаний (2) – Развитие (достижение более высокого уровня устойчивости российского сегмента киберпространства за счет развития его самообеспечения, а как следствие, снижение зарубежного влияния)
Бизнес	Стратегия зависимости / возвращение к старому	(-2) – Зависимость (вытеснение/поглощение российских компаний иностранными конкурентами) (-1) – уменьшение сферы влияния отечественного бизнеса на отечественном рынке
	Стратегия выживания	(0) – Выживание (сохранение сферы влияния бизнеса на отечественном рынке)
	Стратегия развития	(1) – постепенный захват сегмента российского рынка, принадлежавшего иностранным компаниям отечественными производителями/ повышение степени замещения иностранной продукции) (2) – Развитие (расширение сферы влияния бизнеса на рынки зарубежных государств)
SWOT-анализ		
Устойчивость российского сегмента киберпространства	Strengths – сильные стороны Weakness – слабые стороны Opportunities – возможности внешней среды Threats – угрозы внешней среды.	Баланс $\begin{cases} S+O > W+T \\ S+O = W+T \\ S+O < W+T \end{cases}$

Продолжение таблицы 2

1	2	3
Вектор стратегии государства	Strengths – сильные стороны Weakness – слабые стороны Opportunities – возможности внешней среды Threats – угрозы внешней среды	Баланс $\begin{cases} S+O>W+T \\ S+O=W+T \\ S+O<W+T \end{cases}$
Вектор стратегии бизнеса	Strengths – сильные стороны Weakness – слабые стороны Opportunities – возможности внешней среды Threats – угрозы внешней среды.	Баланс $\begin{cases} S+O>W+T \\ S+O=W+T \\ S+O<W+T \end{cases}$

Источник: составлено автором.

Для анализа согласования интересов государства и бизнеса использовался инструментарий теории игр в форме платежных матриц, смотреть в таблице 3.

Таблица 3 – Матрица стратегий

Бизнес	Государство		
	Стратегия зависимости	Стратегия выживания	Стратегия развития
Стратегия зависимости	С. Зависимости / С. зависимости	С. Выживания / С. зависимости	С. Развития / С. зависимости
Стратегия выживания	С. Зависимости / С. выживания	С. выживания / С. зависимости/	С. Развития / С. выживания
Стратегия развития	С. Зависимости / С. развития	С выживания / С. развития	С. Развития / С. развития

Источник: составлено автором.

Выводы по главе 1

Методологической основой исследования определен системный подход. Российский сегмент киберпространства рассматривается как отдельная система, которая формируется в результате взаимодействий компаний ИТ-сектора и органов государственной власти. В соответствии с неоинституциональным подходом акторы политической сферы формируют формальные правила игры в киберпространстве, а компании ИТ-сектора в процессе осуществления хозяйственной деятельности оказывают влияние на

общество и государство, что способствует появлению новых формальных и неформальных институтов. В соответствии с концепциями П. Бурдье, Н. Флигстина, Д. Макадама государство анализируется как иерархическое поле, инициирующее появления новых полей и управляющее всей совокупностью полей для достижения поставленных целей.

В качестве методологического инструмента для рассмотрения поведения акторов киберпространства используются элементы теории игр. Взаимодействие органов государственной власти и компаний ИТ-сектора можно рассматривать как кооперативную игру, где акторы обладают ресурсами и возможностями для выбора определенной стратегии, которая в значительной степени определяется влиянием их конечных целей и ограничениями вызовов внешней среды. В данном исследовании делается вывод, что для достижения устойчивости российского сегмента киберпространства необходимо найти Парето-эффективное равновесие стратегий акторов. Угрозой для обоюдного выбора стратегий, ведущих к достижению Парето-эффективности, является Парето-неэффективное равновесие Нэша.

Взаимодействие государства с компаниями ИТ-сферы наиболее точно описывает модель неокорпоративизма, акцентирующая центральную роль государства в выстраивании иерархически подчиненных полей бизнеса и других сфер общества. Для анализа взаимодействий государства и бизнеса наряду с общенаучными методами целесообразно использовать такие методы, как статистический анализ, SWOT-анализ, методику ресурсно-акторного анализа.

Баланс взаимодействий государства и бизнеса в области производства аппаратного обеспечения, программного обеспечения, кадрового обеспечения сферы ИТ создает состояние устойчивости национального сегмента киберпространства. Под государством в настоящем исследовании понимаются органы государственной власти, непосредственно участвующие во взаимодействии с компаниями ИТ-сферы. В качестве «бизнеса» в данной

работе рассматриваются наиболее крупные компании в сфере ИТ, отобранные на основе рейтингов и проанализированные на основе данных системы «Спарк-Интерфакс».

Основной функцией киберсреды является обеспечение сквозного инфокоммуникационного взаимодействия между субъектами. Она базируется на принципах агентности, информационного самообслуживания и управляемой информационной открытости. Киберпространство – это 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). Термин «информационное пространство» является более широким понятием и не подходит для пространства, созданного при помощи ИТ.

Национальный сегмент киберпространства, являясь функцией экономической деятельности акторов бизнеса и политико-административной деятельности органов государственной власти, в условиях постиндустриального общества становится значимой платформой для информационно-коммуникационного взаимодействия, создания и трансляции «картин мира». Государство стремится распространить свой суверенитет на российский сегмент киберпространства, маркируя его границы и регламентируя правила игры акторов. Для устойчивости российского сегмента киберпространства необходимо наличие инфраструктуры (программного и аппаратного обеспечения, кадров), которая в состоянии гибко адаптироваться к внешним вызовам. В данном исследовании устойчивость киберпространства определяется как динамическое состояние процессов обмена ресурсами, обеспечиваемое за счет устойчивости подсистем, из которых она состоит.

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 фирмами, 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.

Глава 2
Взаимодействие государства и бизнеса в области информационных технологий

2.1 Ресурсы, акторы, стратегии взаимодействия государства и ИТ-бизнеса в контексте геополитических вызовов 2020–2024 гг.

В данном параграфе 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.

Российский сегмент киберпространства (инфраструктуры) можно рассматривать как отдельное поле, взаимодействующее с другими полями внутри страны и за рубежом, и, в свою очередь, состоящее из полей производителей программного обеспечения, аппаратного обеспечения, как представлено на рисунке А 1. В нем действуют частные российские и зарубежные компании, а также государственные компании. При этом часть компаний, позиционирующих себя как отечественные, имеет зарубежных инвесторов. Акторы полей российского сегмента киберпространства встроены в глобальные торгово-производственные цепочки. Внешнеполитические вызовы 2014–2024 гг., а особо вызовы специальной военной операции, начавшейся в 2022 году, можно рассматривать в качестве воздействия зарубежных государственных и корпоративных полей на поле российского сегмента киберпространства с целями нанесения его инфраструктуре максимального ущерба и минимизации его устойчивости.

Российские поля ПО и АО разорвали производственные и технологические связи с иностранными полями, большинство иностранных

фирм прекратило деятельность в России. Зарубежные правительства изменили правила игры для своих компаний с целью нанести удар по экономике и государственной целостности России. В ответ российская власть и бизнес стали менять правила игры в своих полях, чтобы компенсировать ущерб и поддерживать необходимый уровень устойчивости отечественного сегмента киберпространства.

Сегмент киберпространства Российской Федерации формируется за счет взаимодействия власти и бизнеса. Киберпространство регулируется посредством нормативных правовых актов государственных органов власти Российской Федерации, которые являются акторами взаимодействия со стороны государства, что представлено в таблице 4.

Таблица 4 – Поле «государство», взаимодействующее с инфраструктурными полями киберпространства

Орган власти	Руководитель	Сфера компетенции
1	2	3
Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации	Максут Игоревич Шадаев	Стимулирование цифровизации России через льготные закупки ПО для малого и среднего бизнеса; контроль за деятельностью операторов связи для соблюдения законодательства и прав потребителей в сфере связи. Развитие инфраструктуры связи; поддержка инноваций; выработка и реализация государственной политики и нормативно-правовое регулирование в сфере информационных технологий. Смотреть в таблице Г. 1
Министерство экономического развития Российской Федерации	Максим Геннадьевич Решетников	Выработка государственной политики социально-экономического развития; нормативно-правовое регулирование экономической политики; развитие предпринимательской деятельности и лицензирование. Смотреть в таблице Г. 2
Правительство Российской Федерации	Михаил Владимирович Мишустин	Обеспечивает единые экономические правила экономической деятельности в стране. Прогнозирует социально-экономические изменения. Развивает сферы экономики посредством госпрограмм. Смотреть в таблице Г. 3

Продолжение таблицы 4

1	2	3
Президент Российской Федерации	Владимир Владимирович Путин	Определяет основные направления внутренней и внешней политики. Смотреть в таблице Г. 4
Федеральная служба безопасности Российской Федерации	Александр Васильевич Бортников	Осуществляет лицензирование субъектов, а также контроль за безопасностью и за доступом к информации. Смотреть в таблице Г. 5
Федеральная служба по техническому и экспортному контролю Российской Федерации	Владимир Викторович Селин	Осуществляет контроль над обеспечением безопасности информации, имеющей критическую важность для существования и правильного функционирования российского государства, борьбу с техническими разведками других государств на территории страны. Осуществляет контроль экспорта товаров двойного назначения и товаров. Смотреть в таблице Г. 6
Министерство труда и социальной защиты Российской Федерации	Антон Олегович Котяков	Осуществляет выработку государственной политики и нормативно-правовое регулирование Российской Федерации в сфере труда, доходов, оплаты труда, пенсионного обеспечения, условий и охраны труда. Смотреть в таблице Г. 7
Министерство финансов Российской Федерации	Антон Германович Силуанов	Разработка правовых актов в области финансов с учётом своей компетенции. Проведение мероприятий, которые помогают оздоровлению экономики страны. Анализ и прогнозирование экономического развития. Совершенствование бюджетной системы путём внедрения новых механизмов, правил и норм. Подготовка новых предложений по изменению денежно-кредитной политики страны. Подготовка инвестиционных проектов. Формирование ценовой политики. Смотреть в таблице Г. 8
Федеральная налоговая служба Российской Федерации	Даниил Вячеславович Егоров	Контроль и надзор за соблюдением законодательства о налогах и сборах. Контроль за правильностью исчисления и своевременностью внесения в бюджет налогов и иных платежей. Государственная регистрация юридических лиц и физических лиц в качестве индивидуальных предпринимателей. Смотреть в таблице Г. 9
Государственная Дума Федерального Собрания Российской Федерации	Вячеслав Викторович Володин	Принятие федеральных конституционных законов и федеральных законов. Смотреть в таблице Г. 10

Продолжение таблицы 4

1	2	3
Министерство науки и высшего образования Российской Федерации	Валерий Николаевич Фальков	Выработка и реализация государственной политики и регулирования в сфере высшего образования и инновационной деятельности, а также центров науки и высоких технологий. Социальная поддержка и защита обучающихся, осуществление молодёжной политики. Смотреть в таблице Г. 10

Источник: составлено автором.

Государство обладает политическими, административными, финансовыми ресурсами: создание формальных институтов (норм) и реализация их функционирования, бюджетное финансирование проектов, определение приоритетных направлений развития экономики. Без мер государственной поддержки в условиях противостояния со странами Запада развитие отечественных полей ПО и АО невозможно. Меры государственной поддержки бизнеса в сфере ИТ: налоговые льготы, льготные кредиты и гранты для отечественных ИТ-компаний; стимулирование спроса на продукцию и услуги отечественных ИТ-компаний, льготная ипотека и отсрочка от призыва для сотрудников и специалистов аккредитованных государством ИТ-компаний, освобождение ИТ-компаний от проверок, трудоустройство и ВНЖ для иностранных специалистов, включение российского ПО в единый реестр, аккредитация российских компаний, поддержка ИТ-образования, привлечение финансирования, поддержка особо значимых проектов, легализация серого импорта и обхода санкционных ограничений и др. Меры государственной поддержки представлены в таблице 5.

Таблица 5 – Меры воздействия государства на ИТ-компании

Меры поддержки	Кому предназначена мера
1	2
Налоговые льготы	ИТ-компании

Продолжение таблицы 5

1	2
	Индивидуальные предприниматели
Льготные кредиты	Аккредитованные ИТ-организации Любая российская организация, реализующая проекты по разработке и внедрению российских ИТ Аккредитованные российские системообразующие организации из сферы ИТ либо аккредитованные организации, входящие в группу с системообразующими организациями
Гранты	ИТ-стартапы Российские разработчики программного обеспечения Заказчики, внедряющие отечественные ИТ-решения в целях цифровой трансформации и импортозамещения
Стимулирование спроса	Получатели скидки: компании и индивидуальные предприниматели, отвечающие данным требованиям: Годовой доход организации – до 2 млрд руб. Количество сотрудников – не более 250 Включение в Единый реестр МСП
Льготная ипотека	Требования к ИТ-специалистам, которые могут претендовать на льготную ипотеку: Гражданин Российской Федерации Возраст специалиста до 50 лет включительно Основным местом работы является аккредитованная государством ИТ-компания Для граждан России в возрасте от 36 до 50 лет включительно – средняя зарплата до вычета НДФЛ за последние 3 месяца соответствует ряду требований К заёмщикам до 35 лет включительно требование к размеру зарплаты не предъявляется
Отсрочка от призыва	Сотрудникам любой организации из списка аккредитованных ИТ-компаний
Освобождение от проверок	Аккредитованным ИТ-компаниям
Трудоустройство и ВНЖ для иностранцев	Иностранным ИТ-специалистам и членам их семей Аккредитованным ИТ-компаниям
Включение в реестры	Российским разработчикам ПО
Аккредитация	Услуга доступна только юридическим лицам, работающим в сфере ИТ. Подать заявление может руководитель организации и сотрудники, у которых есть доверенность на Госуслугах
ИТ-образование	Возраст: от 16 лет Образование: высшее, среднее профессиональное и студенты Льготная категория
Привлечение финансирования	Проекты

Продолжение таблицы 5

1	2
Поддержка особо значимых проектов	Проекты

Источник: составлено автором на основе [95].

На сегмент отечественного киберпространства также влияют иностранные государственные и частные акторы посредством международных торговых соглашений, экспортно-импортных операций, введения санкций. Иностранные компании, функционирующие в российском сегменте, подчиняются как российскому законодательству, так и законодательству стран, в которых они зарегистрированы. Это также влияет на их филиалы и дочерние компании в России.

Вторым субъектом взаимодействия является бизнес: наиболее крупные компании в данной сфере, которые представлены в таблице В. 1, а также организации, лоббирующие интересы бизнеса во властных структурах, смотреть таблицу 6. Деятельность данных организаций направлена на разработку и реализацию общих проектов, обмена информацией и консолидирование запроса компаний к органам власти, что особенно важно при быстрых темпах развития и сложности производственных процессов и их взаимосвязей в кластере ИТ-технологий.

Таблица 6 – Организации, лоббирующие интересы ИТ-бизнеса

Организация	Руководитель	Деятельность
1	2	3
НО «Центр компетенций по импортозамещению в сфере информационно-коммуникационных технологий» (далее – ЦКИКТ)	(Директор) Илья Массух	Предоставление услуг в сфере импортозамещения ПО и аппаратных средств, анализа и систематизации информации о российских решениях и разработчиках в области ИКТ
Некоммерческое партнерство разработчиков программного обеспечения «РУССОФТ»	(Президент ассоциации «Руссофт») Валентин Макаров	Лоббирование в органах государственной власти интересов предприятий в сфере разработки ПО, а также содействие системе подготовки, повышения квалификации и переподготовки ИТ-кадров

Продолжение таблицы 6

1	2	3
		в России. Маркетинг продуктов и услуг в России и на глобальном рынке, а также в компаниях индустрии современных технологий управления проектами и качеством
Российская ассоциация электронных коммуникаций (далее – РАЭК)	Гребенников Сергей Владимирович (Директор) Демкина Екатерина Николаевна (Исполнительный Директор)	Консолидация мнения отрасли Аналитика и исследования GR / Взаимодействие с государством Обеспечение работы и сопровождение продуктов бизнес-кластеров РАЭК Популяризация достижений отрасли Мероприятия Спецпроекты Экспертно-консультативный совет при РАЭК

Источник: составлено автором.

Компании, функционирующие в сфере ИТ Российской Федерации, можно классифицировать на основе различных критериев. По юрисдикции собственников выделяются российские и иностранные компании. По форме собственности выделяются российские государственные и частные компании, часть фирм входит в списки аккредитованных, дотационных и приоритетных организаций [179]. Иностранные организации в условиях санкций разделяются на компании, относящиеся к странам, поддержавшим санкции (постепенно покидают российский сегмент), и к странам, не поддержавшим санкции (имеют возможность попасть в российский сегмент). По типу продукции можно выделить внутри поля сферы ИТ самостоятельные поля производителей программного обеспечения и аппаратного обеспечения.

Компании, действующие в российском сегменте киберпространства, получают прибыль, в основном, за счет удовлетворения российских потребителей (физические лица, юридические лица, государство), а также за

счет экспорта услуг. Указанные выше характеристики компаний влияют на взаимодействие с властными структурами.

Целью бизнеса является получение и увеличение прибыли. Целью государства является обеспечение стабильности и устойчивости функционирования общества. Из-за того, что цели государства являются более комплексными, чем цели бизнеса, их достижение требует задействования намного большего количества акторов и ресурсов в данных процессах. Ресурсы бизнеса: кадры с профессиональными компетенциями, финансы, ИТ-технологии. Именно бизнес реализует государственные проекты по формированию киберпространства России, ему принадлежат ИТ-технологии, от которых зависит развитие киберпространства страны.

С 2022 года национальный сегмент киберпространства функционирует в жестком режиме противодействия антироссийским санкциям и проведения специальной военной операции на Украине. Значительная часть зарубежных компаний ИТ-сферы ушла с российского рынка (184 из 196) [140]. Восьмой пакет санкций Европейского Союза от 6 октября 2022 г. [71] установил запрет на экспорт услуг по ИТ-консультациям [133]. Необходимо отметить, что в соответствии с данными санкциями запрещаются консультации как по вопросам ПО (услуги по разработке и внедрению), так и услуги по установке компьютерных сетей и оборудования. Таким образом, это является отказом от обязательств по их технической поддержке. Предусмотрены и исключения из запрета, если консультационные услуги требуются для деятельности гражданского общества, непосредственно продвигающего права человека, демократию или верховенство закона на территории Российской Федерации. Министерство финансов США запрещает предоставлять ПО и ИТ-услуги ВПК России [73]. Разрабатываются новые способы выявления компаний нарушителей санкционных ограничений [75]. Вводятся законы против зарубежных компаний, участвующих в схемах параллельного импорта, а также несоблюдающих санкционный режим [68]. Санкционные ограничения в сфере ПО направлены на сдерживание развития критической

инфраструктуры страны, обороны, а также инновационного развития экономики в целом [136].

В свою очередь, российское государство поддерживает российские бизнес-структуры в сфере ИТ, осуществляет меры, направленные на замещение иностранной продукции, на повышение безопасности российского сегмента киберпространства. Данные меры перечислены и рассмотрены в приложении Г.

Эффект влияния санкций и адаптации экономики к условиям гибридной войны на сектор ИТ можно определить через сравнительный анализ статистики показателей сектора до 2022 года и после 2022 года. В период с 2013 года по 2023 год ИТ-сфера занимала первое место по темпам прироста среди остальных областей экономики России [100].

По данным Института статистических исследований и экономики знаний НИУ ВШЭ, в период с 2019 года по 2023 год в ИТ-сфере России сохранялся позитивный тренд развития. За рассмотренный период объем реализации собственных разработок ИТ-услуг отечественных компаний вырос в 2,5 раза, что демонстрируется в таблице 7, и достиг в 2023 году 3,1 трлн. рублей. При этом рост объемов реализации продукции по экономике в среднем составил 1,6 раз. Росла доля ИТ-сферы в ВВП России, которая с 1,32% в 2019 году достигла 1,96% в 2023 году, смотреть таблицу 8.

Таблица 7 – Темп прироста ИТ-сферы России до 2023 года по сравнению с 2019 годом

Год	2019	2020	2021	2022	2023
соотношение	1	1,1	1,6	1,9	2,5

Источник: составлено автором на основе [91].

Таблица 8 – Доля ИТ-сферы в ВВП России

В процентах с 2019 г. по 2023 г.

Год	2019	2020	2021	2022	2023
Доля в ВВП	1,32	1,62	1,63	1,74	1,96

Источник: составлено автором на основе [91].

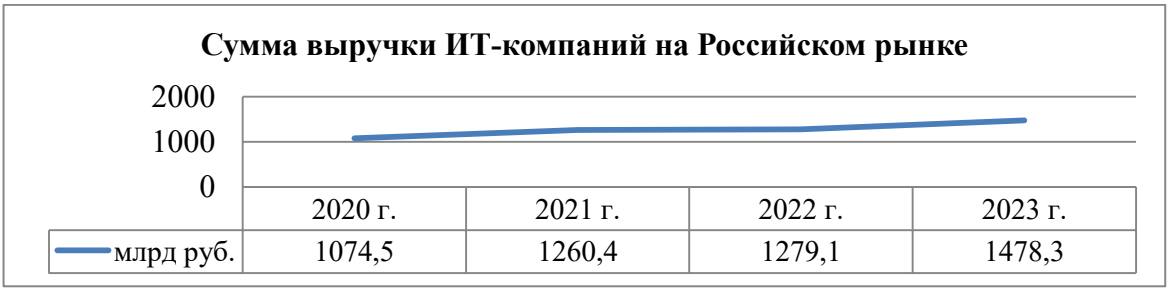
При рассмотрении статистики выручки наиболее крупных ИТ-компаний России заметен прирост суммы выручки в период 2021–2023 гг., представлено на рисунке 1. Но при этом произошло резкое падение среднего значения прироста выручки данных компаний в 2023 году, смотреть таблицу 9, что обусловлено падением прироста выручки иностранных компаний, данные по которым представлены в таблице 11. Если рассматривать прирост выручки только отечественных компаний, смотреть таблицу 10, то падение не столь значительно. Статистические данные об уплате налогов по годам показывают рост даже с учетом налоговых послаблений для компаний в данной области, представлено на рисунке 2.

Таблица 9 – Прирост выручки ИТ-компаний на российском рынке

В процентах

Год	2020	2021	2022	2023
Среднее значение	136,6	32,8	43,7	16,6

Источник: составлено автором.



Источник: составлено автором.
Рисунок 1 – Сумма выручки ИТ-компаний на российском рынке

Источник: составлено автором.
Рисунок 2 – Сумма уплаченных налогов ИТ-компаний на российском рынке

Таблица 10 – Прирост выручки отечественных компаний

В процентах

Год	2020	2021	2022	2023
Среднее значение	154,2	34,6	51,0	24,0

Источник: составлено автором.

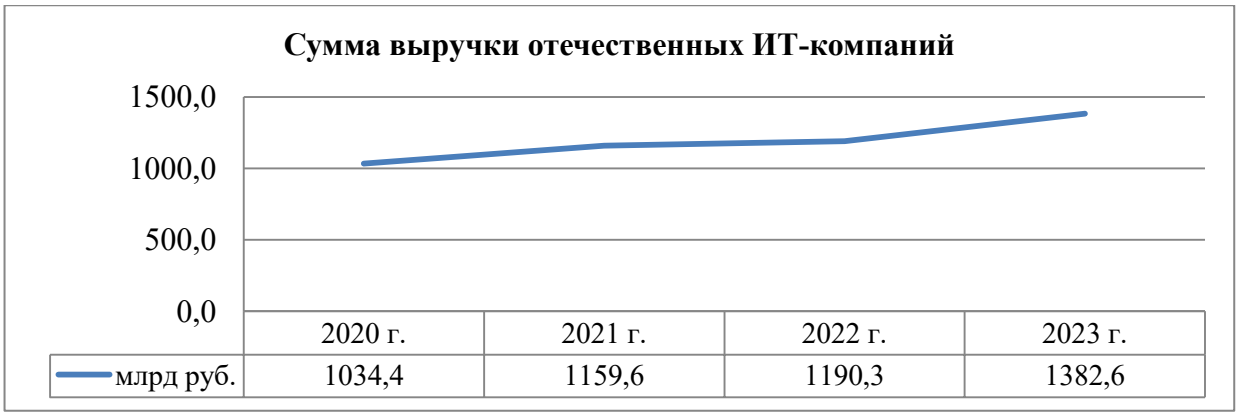
Таблица 11 – Прирост выручки иностранных компаний

В процентах

Год	2020	2021	2022	2023
Среднее значение	56,0	28,9	20,1	-11,5

Источник: составлено автором.

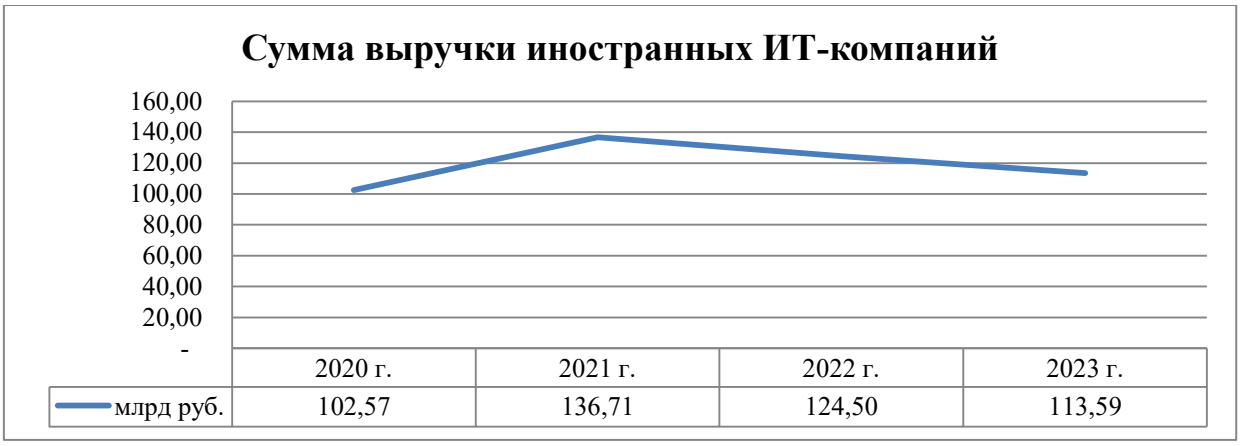
Статистические данные о выручке отечественных компаний по годам показывают рост, как представлено на рисунке 3. К тому же, среднее значение прироста выручки выше на всех этапах, чем при учете данных иностранных компаний.



Источник: составлено автором.

Рисунок 3 – Сумма выручки отечественных ИТ-компаний

На рисунке 4 показано, что с 2021 года начинается падение выручки иностранных компаний. Многие иностранные компании на 2023 год уже прекратили свою деятельность на территории Российской Федерации, часть находилась в состоянии ликвидации.



Источник: составлено автором.
Рисунок 4 – Сумма выручки иностранных ИТ-компаний

Несмотря на санкции, отечественная ИТ-сфера демонстрирует рост финансовых показателей, способность функционировать в условиях внешних ограничений, что является показателем устойчивости. Сфера ИТ включает в себя поля компаний с различными профилями, среди которых особо следует выделить компании производителей ПО и АО. Их стратегии во многом сильно отличаются в связи с различиями в конфигурации и обменах с сопредельными полями государства, секторов российской экономики и зарубежных акторов. Далее в работе производится анализ особенностей полей производителей ПО и АО.

Из 100 компаний за последние десять лет (2015-2025 гг.) только у 21 компании были арбитражные дела с органами власти. Рассматриваются только те дела, где органы власти и компания выступали либо в качестве истца, либо в качестве ответчика. Всего 93 дела, при этом в качестве истца компании выступают в 69 делах. Наибольшее количество дел у компании ПАО «Ростелеком» (29 дел) и у компании АО «Барс Груп» (22 дела). Данные по судебным делам представлены в таблице 12.

Таблица 12 – Количество судебных дел между государством и наиболее крупными компаниями в сфере ИТ с 2015 г. по 2025 г.

Компания	Всего дел	Истец/ ответчик		Иск отклонен полностью	Иск отклонен полностью или частично	Иск удовлетворен полностью или частично	Иск удовлетворен полностью	Рассматривается	Обжалуется	Исполнение обязательств по договорам
1	2	3	4	5	6	7	8	9	10	11
Государственная корпорация «Ростех»	5	истец	3	0	1	1	1	0	0	0
		ответчик	2	0	1	0	0	0	1	0
АО «Группа Телематика-Один»	1	истец	1	0	1	0	0	0	0	0
		ответчик	0	0	0	0	0	0	0	0
ПАО «Ростелеком»	29	истец	20	0	5	0	7	4	0	4
		ответчик	9	3	0	0	0	2	4	0
ПАО «Софтлайн»	1	истец	1	0	0	1	0	0	0	0
		ответчик	0	0	0	0	0	0	0	0
АО «Лаборатория Касперского»	4	истец	4	3	0	0	1	0	0	0
		ответчик	0	0	0	0	0	0	0	0
АО «Ситроникс»	4	истец	4	0	1	0	1	2	0	0
		ответчик	0	0	0	0	0	0	0	0
ПАО «Газпром Автоматизация»	1	истец	1	0	0	0	1	0	0	0
		ответчик	0	0	0	0	0	0	0	0
АО «Производственная Фирма «Скб Контур»	2	истец	1	0	1	0	0	0	0	0
		ответчик	1	0	1	0	0	0	0	0
ООО «Сап Снг»	1	истец	1	0	1	0	0	0	0	0
		ответчик	0	0	0	0	0	0	0	0

Продолжение таблицы 12

1	2	3	4	5	6	7	8	9	10	11
ООО «Газинформсервис»	3	истец	3	1	1	0	1	0	0	0
		ответчик	0	0	0	0	0	0	0	0
ООО «Организационно-Технологические Решения 2000»	3	истец	3	2	0	1	0	0	0	0
		ответчик	0	0	0	0	0	0	0	0
ООО «Компания «Тензор»	1	истец	1	0	0	0	1	0	0	0
		ответчик	0	0	0	0	0	0	0	0
ООО «Бюджетные и Финансовые Технологии»	1	истец	1	1	0	0	0	0	0	0
		ответчик	0	0	0	0	0	0	0	0
ООО «Депо Электроникс»	4	истец	1	0	0	0	0	1	0	0
		ответчик	3	0	2	0	0	0	1	0
ООО «Оранж Бизнес Сервисез»	5	истец	5	2	3	0	0	0	0	0
		ответчик	0	0	0	0	0	0	0	0
АО «Нэксайн»	1	истец	1	0	0	0	1	0	0	0
		ответчик	0	0	0	0	0	0	0	0
АО «Россети Цифра»	2	истец	2	0	0	1	1	0	0	0
		ответчик	0	0	0	0	0	0	0	0
АО «Барс Груп»	22	истец	15	1	6	6	0	0	2	0
		ответчик	7	0	6	1	0	0	0	0
ООО «Манго Телеком»	1	истец	1	1	0	0	0	0	0	0
		ответчик	0	0	0	0	0	0	0	0
ООО «Вк Цифровые Технологии»	1	истец	0	0	0	0	0	0	0	0
		ответчик	1	0	0	0	0	1	0	0
АО «Инлайн Груп»	1	истец	0	0	0	0	0	0	0	0
		ответчик	1	1	0	0	0	0	0	0

Источник: составлено автором.

Результаты исков компаний:

- иск отклонен полностью - 15,9%;
- иск отклонен полностью или частично - 29%;
- иск удовлетворен полностью или частично - 14,5%;
- иск удовлетворен полностью - 21,7%.

Результат исков органов власти:

- иск отклонен полностью - 18,2%;
- иск отклонен полностью или частично - 45,5%;
- иск удовлетворен полностью или частично - 4,5%;
- иск удовлетворен полностью - 0%.

На основе вышеприведенных данных можно сделать вывод, что компании чаще выигрывают свои иски, чем органы власти.

2.2 Взаимодействие государства и бизнеса в поле программного обеспечения

В данном параграфе анализируется деятельность акторов поля программного обеспечения (ПО), поле взаимодействия государства и бизнеса в сфере ПО, а также матрица стратегий взаимодействия государства и бизнеса в сфере ПО.

Игроков поля ПО можно охарактеризовать как наиболее ресурсных участников российской сферы ИТ. В соответствии с данными ассоциации «Руссофт», по итогам 2022 года, несмотря на общее сокращение ИТ-рынка России на 8–10% (2,75 трлн руб.), рынок ПО вырос на 1%, составив 640 млрд руб. Также произошло сокращение продукции иностранных разработчиков ПО с 34% до почти 20% [90]. В своих отчетах «Руссофт» определяет рынок ПО как совокупность всех продаж, являющихся основными для софтверных компаний, а также связанных непосредственно с разработкой ПО. В соответствии с данными «Руссофт» в 2023 году зафиксирован рост объемов

продаж отечественных софтверных компаний на 19,4% до примерно 2 трлн рублей. В свою очередь, продажи зарубежных компаний снизились в 2023 году на 30% до 5,53 млрд долл. По прогнозам «Strategy Partners» российский рынок инфраструктурного ПО будет ежегодно расти на 15% до 2030 года [92]. К 2030 году Российской Федерации предстоит сформировать цифровые платформы во всех ключевых сферах экономики и социальной сфере [106].

Из 100 крупнейших компаний сферы ИКТ 41 компанию можно отнести к разработчикам программного обеспечения (ОКВЭД 62.01 «Разработка компьютерного программного обеспечения»). В таблице Б. 1 приведены данные по динамике трех показателей 41 компании разработчиков ПО: годовая выручка (млрд руб.), прирост годовой выручки (в процентах), уплаченные налоги (млн руб.).

Компании в сфере разработки ПО за период с 2020 г. по 2023 г. демонстрируют рост выручки, как представлено на рисунке 5. При этом наибольший прирост выручки по сравнению с предыдущим годом произошел в 2020 году, смотреть таблицу 13, и связан с мерами, направленными против коронавируса (COVID-19), когда произошел скачок виртуализации человеческой деятельности. В период с 2021 г. по 2022 г. сохранялись активные темпы роста, в 2023 году наступило замедление темпов роста выручки до 26,5%, объяснимое последствием санкций и резкого сокращения деятельности на российском рынке иностранных компаний. Если рассматривать только российские компании, данные по которым представлены на рисунке 6, то темпы прироста выручки в период с 2020 г. по 2022 г. были незначительно ниже, но при этом и сокращение прироста выручки в 2023 году было не столь значительно, как показано в таблице 14.

Источник: составлено автором.

Рисунок 5 – Сумма выручки компаний в сфере ПО с 2020 г. по 2023 г.

Таблица 13 – Прирост по сравнению с предыдущим годом выручки компаний в сфере ПО с 2020 г. по 2023 г.

В процентах

Год	2020	2021	2022	2023
Среднее значение	61,5	43,0	45,5	26,5

Источник: составлено автором.

Источник: составлено автором.

Рисунок 6 – Сумма выручки отечественных компаний в сфере ПО с 2020 г. по 2023 г.

Таблица 14 – Прирост по сравнению с предыдущим годом выручки отечественных компаний в сфере ПО с 2020 г. по 2023 г.

В процентах

Год	2020	2021	2022	2023
Среднее значение	58,6	41,4	42,3	32,1

Источник: составлено автором.

В соответствии с собранными данными в таблице 15, владельцами наиболее крупных компаний-разработчиков ПО в подавляющем большинстве случаев являются физические и юридические субъекты Российской Федерации. Причем многие компании-разработчики принадлежат более крупным российским компаниям в сфере ИТ и коммуникаций (ПАО МТС, ООО Яндекс, ООО ВК) и банкам (ПАО «Сбербанк России»). Компания «Газпром» является владельцем двух компаний-разработчиков из списка. Из этого можно заключить, что наиболее крупные компании-разработчики ПО, в основном, полностью находятся в правовом поле Российской Федерации и в некоторых случаях имеют возможность ретранслировать свои интересы государству через своих владельцев.

Таблица 15 – Компании-разработчики ПО в сфере ИТ

Полное название организации	Руководитель	Совладельцы	Выручка в 2023 г., млрд руб.
1	2	3	4
АО «Цифровые Закупочные Сервисы»	Юдина Ольга Вячеславовна	ООО «Электронная Торговая Площадка Гпб»	48,2
АО «Лаборатория Касперского»	Касперский Евгений Валентинович	Головная Компания Kaspersky Labs Limited, ООО «Группа Компаний Касперского», Граждане России	47,7
ООО «Мтс Диджитал»	Воробьева Оксана Сергеевна	ПАО МТС, ООО СТРИМ, ООО Телеком Проекты	32,5

Продолжение таблицы 15

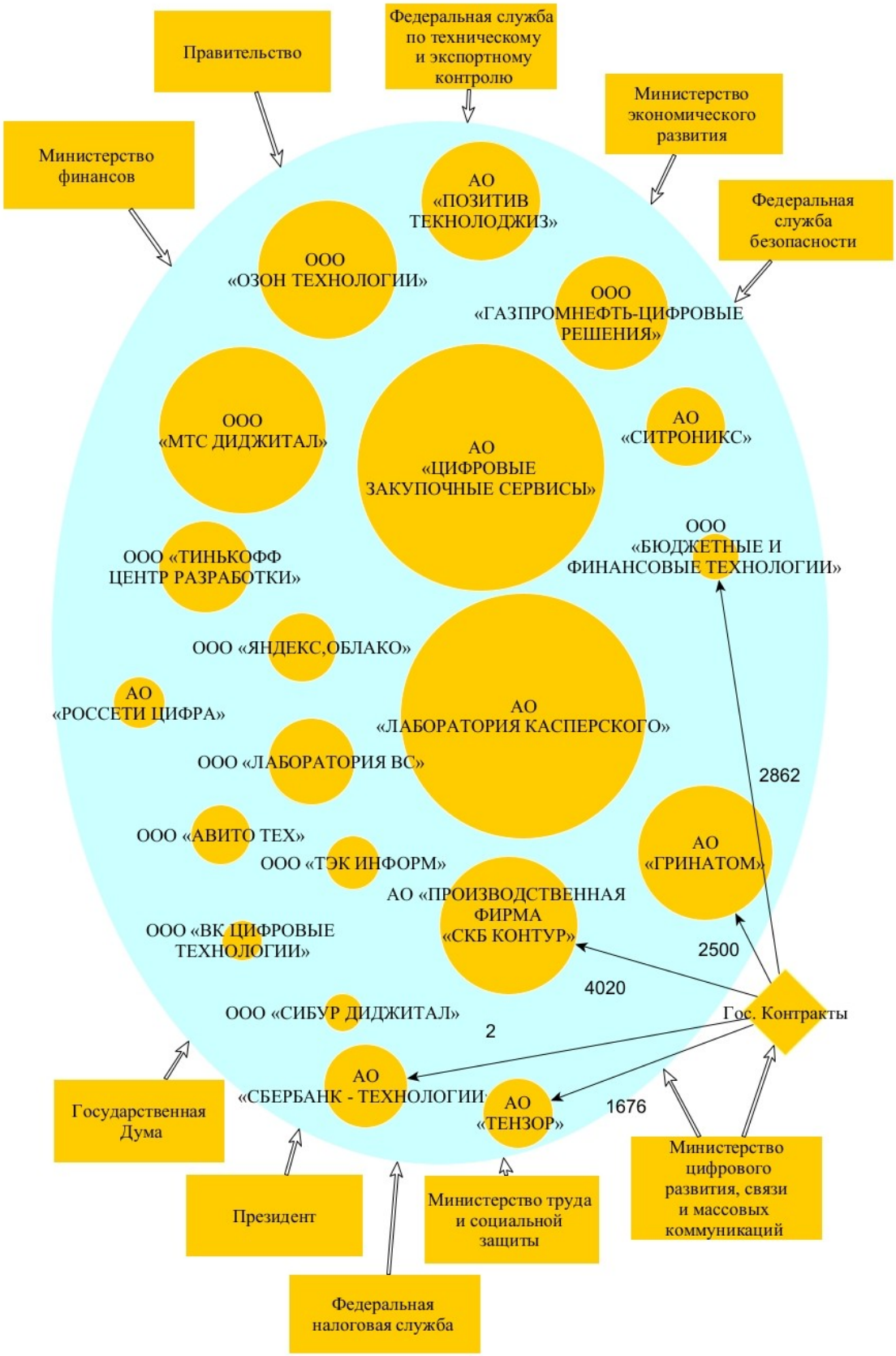
1	2	3	4
ООО «Озон Технологии»	Кайзер Борис Валерьевич	ООО «Озон Холдинг» (Принадлежит компании с Кипра) ООО «Интернет Решения»	27,1
АО «Производственная Фирма «Скб Контур»	Сродных Михаил Юрьевич	Бублик Владимир Кузьмич Рахимянов Шамиль Мубаракович и пр.	26,9
АО «Гринатом»	Ермолаев Михаил Юрьевич	АО «Атомный Энергопромышленный Комплекс»	26,3
АО «Позитив Текнолоджиз»	Баранов Денис Сергеевич	ПАО «Группа Позитив»	23,2
ООО «Газпромнефть-Цифровые Решения» (Ранее ИТСК, ООО)	Поперлюков Алексей Сергеевич	ПАО «Газпром Нефть»	22,2
ООО «Тинькофф Центр Разработки»	Борисов Сергей Станиславович	Tcs Group Holding Plc (Кипр) 49%, АО Тинькофф Банк 49%, ООО Ткс	17,9
ООО «Лаборатория ВС»	Викарук Лариса Ивановна	Никулин Максим Александрович, Денисов Евгений Викторович, Соков Максим Михайлович	16,8
АО «Сбербанк – Технологии»	Шашлов Антон Михайлович Тятюшев Максим Анатольевич	ПАО «Сбербанк России»	16,3
АО «Ситроникс»	Пожидаев Николай Николаевич	ПАО «Акционерная Финансовая Корпорация «Система»	15,5
ООО «Компания «Тензор»	Уваров Сергей Васильевич	Уваров Сергей Васильевич, Кошелев Александр Евгеньевич, Новиков Дмитрий Владимирович, Боровиков Кирилл Сергеевич, Зафиевский Дмитрий Александрович	13,7
ООО «Яндекс, Облако»	Черников Александр Владимирович	Яндекс, ООО	13,4

Продолжение таблицы 15

1	2	3	4
ООО «Авито Тех»	ООО Авито менеджмент	ООО «Кех Екоммерц»	11,7
ООО «Тэк Информ»	Козловский Игорь Валерьевич	Центрэнергохолдинг, Пао. Головная Компания Руководит ПАО Газпром	10,4
АО «Россети Цифра»	Архипов Александр Геннадьевич	ГК ПАО «Россети»	10,1
ООО «Бюджетные и Финансовые Технологии»	Зейтениди Наталья Юрьевна	РТ ЛАБС, АО	9,1
ООО «Вк Цифровые Технологии»	Управляющая компания ВК, ООО	ООО Цифровая Трансформация Плюс, ООО ВК	7,9
ООО «Сибур Диджитал»	Мельникова Алиса Валериевна	Головная Компания Сибур Холдинг, ПАО	7,4

Источник: составлено автором.

Поле взаимодействия государства и бизнеса разработчиков ПО представлено на рисунке 7. Отражены 20 наиболее крупных по критерию выручки акторов.



Источник: составлено автором.

Рисунок 7 – Поле взаимодействия государства и бизнеса сегмента ПО

Для государства и бизнеса, стремящихся достичь собственных целей, Парето-эффективной стратегией является выбор «стратегия развития – стратегия развития», что представлено в таблице 16. При этом данная стратегия является равновесием Нэша: односторонняя смена стратегии любым актором только ухудшает положение игрока (в данном случае обоих игроков). Государственная поддержка дает стимул для ускоренного развития компаний и освоения ими старых и новых рынков. Многие отечественные компании в сфере ПО уже функционируют на международном уровне и имеют возможность для реализации вложенных государством средств. В силу имеющихся у российских компаний сферы ПО компетенций, они могут занять существенную долю отечественного рынка и обеспечить высокую степень устойчивости российского сегмента киберпространства. Это позволит развивать процессы цифровизации в политике и экономике на отечественном софте, использовать возможности работы с большими данными, защищаться от хакерских атак.

Таблица 16 – Матрица исходов стратегий взаимодействия государства и бизнеса сегмента ПО

ПО		Бизнес		
		Стратегия развития	Стратегия выживания	Стратегия зависимости / возвращение к старому
Государство	Стратегия развития	2/2	1/1	1/1
	Стратегия выживания	1/-2	1/-1	1/-1
	Стратегия зависимости / возвращение к старому	-1/0	0/-1	-2/-1

Источник: составлено автором.

Компании в сфере ПО обладают рядом важных характеристик, позволяющих им демонстрировать высокие показатели устойчивости на фоне глобальных вызовов.

- Относительно низкие затраты на производство продукции.

- Возможность использовать труд релокантов.

- Качество задействованных в процессе разработки продукции специалистов является во многом основным фактором разработки ПО, а в Российской Федерации исторически сложился высокий уровень образования в сфере математики и программирования.

На основе разобранных факторов можно сделать вывод, что поле ПО является одной из основных движущих сил развития российской сферы ИТ. Также данная сфера обладает значительным потенциалом для дальнейшего развития.

2.3 Взаимодействие государства и бизнеса в поле аппаратного обеспечения

В данном параграфе анализируется деятельность акторов поля производства аппаратного обеспечения (АО), результаты легализации государством параллельного импорта, поле взаимодействия государства и бизнеса в сфере АО, а также матрица стратегий взаимодействия государства и бизнеса в сфере АО.

Сфера производства аппаратного обеспечения на территории Российской Федерации во многом отличается от сферы разработки программного обеспечения. Разработкой новых программ можно заниматься на устаревшем компьютере, и не важно, в какой стране он произведен. Также для данного процесса требуется относительно небольшая группа специалистов. Это позволило данной сфере относительно безболезненно пройти через экономические и политические потрясения периода распада СССР. Разрушение систем поставок и заводов компьютерного оборудования, которые создавались в СССР, а также процесс глобализации, приведший к доминированию на российском рынке иностранного оборудования в

сочетании с оттоком специалистов за рубеж, привели к стагнации и деградации, прежде всего, отечественного сегмента разработки аппаратного обеспечения. К тому же для производства АО требуются большие производственные мощности, а их разработка требует наличия большого количества узкоспециализированных работников, что без направленной поддержки государства реализовать невозможно.

В результате, российский рынок АО был захвачен иностранными компаниями, а отечественные разработчики и производители были вынуждены бороться за выживание. Телекоммуникационная сфера Российской Федерации в основном работает с китайскими поставщиками оборудования.

Подобная ситуация зависимости от импорта из другого государства является естественной в условиях современной глобальной экономики и допустима в мирное время, но становится критически опасной для государства в условиях глобальной геополитической нестабильности и в условиях санкционных войн. Так, после начала СВО и введенных против России санкций, российский рынок покинула компания-поставщик сетевых решений Cisco, которая занимала около 50% рынка сетевой инфраструктуры.

Степень цифровизации страны продолжает расти. Так, на начало 2024 года в Российской Федерации присвоено 45,362,176 IP-адресов [142], и функционирует 8395 DNS-серверов [132]. Как для реализации государственных инициатив по цифровизации правительства, так и для развития цифровой экономики государства необходимо активное развитие в стране мощной сферы разработки ИТ-оборудования, его составных частей и систем поддержки его работоспособности. Но при этом на современном этапе у Российской Федерации относительно слабо развита сфера производства АО.

По данным Росстата отечественный рынок ИТ рос в среднем на 14,9% с 2018 г. по 2022 г. В данный период отечественный сектор производства ИТ-оборудования вырос на 38,6%, при этом средний рост инвестиций с

учетом реинвестирования прибыли в 2018–2022 гг. составил 8,5%. Продажи аппаратных решений на российском рынке демонстрируют стабильный рост [105]:

- 2019 г. – 380,2 млрд рублей;
- 2020 г. – 459,5 млрд рублей;
- 2021 г. – 505,8 млрд рублей;
- 2022 г. – 520,7 млрд рублей;
- 2023 г. – 649,9 млрд рублей;
- 2024 г. – 743,5 млрд рублей.

Необходимо отметить, что объем доли ИТ-оборудования в общем объеме российского рынка ИТ сокращается. Так, в период с 2023 г. по 2024 г. эта доля сократилась с 24,3% до 22,7%. Сокращение является следствием более высоких темпов сферы ПО.

Проблема доступности аппаратных частей, самого оборудования и поддержки оборудования, поставленного ранее иностранными компаниями в Россию и на которых работает как подавляющая часть отечественных компаний, так и органов государственной власти, является одним из основных вызовов ИТ-сферы Российской Федерации с момента начала СВО. Как уже отмечалось, наибольший урон санкции нанесли иностранным компаниям, их представительство на российском рынке сократилась на 50% [122], а также ИТ-дистрибуторам, чья выручка сократилась в 2022 году на 25%.

Совокупный стоимостный объем импорта в Россию ИТ-оборудования в 2022 году по данным WTO составил 487,8 млрд рублей, что на 33,1% меньше показателя 2021 года. 60% данной стоимости приходится на компьютерное и серверное оборудование. На Китай (вместе с Гонконгом) в 2022 году пришлось 82% стоимости ввозимого на территорию России ИТ-оборудования. При этом на систему параллельного импорта через Казахстан пришлось всего 8%.

Государство легализовало параллельный импорт, который отличается от серых схем тем, что ввоз товаров осуществляется с разрешения государства, а также сопровождается уплатой пошлины и НДС. Не происходит уведомления иностранных правообладателей. В свою очередь, серый импорт – это поставка товаров без разрешений и без пошлин.

Необходимо отметить, что одного Китая для обеспечения России ИТ-оборудованием недостаточно, к тому же большинство альтернативных поставщиков так или иначе используют американские технологии. То же относится и к серому импорту. Параллельный и серый импорт не могут обеспечить стабильные линии поставок оборудования в долгосрочной перспективе, порождают пространство для незаконных операций, ведут к завышению цен и дополнительным транзакционным издержкам по поиску конкретного оборудования. Поэтому на современном этапе критически важно развивать отечественное производство оборудования и компонентов, в частности в области производства процессоров и микросхем [112].

Несмотря на санкции, российский сегмент АО продолжает развиваться. Происходит консолидация отечественных вендоров в целях развития производства. Так, в сегменте систем хранения данных в 2023 году были проведены три объединения крупных компаний: «Аквариус» и «Аэродиск», «Yadro» и «Raidix», «F+ tech» и «Baum». Центр компетенций «ИТ-инфраструктура» КРОК отмечает повышение спроса на клиентское оборудование в 2023 году, а также заметен значительный рост спроса на системы хранения данных, на серверное оборудование и вычислительные ресурсы, что является следствием развития облачных инфраструктур.

Параллельно повышается степень локализации ИТ-сферы России, что является следствием стимулирования отечественной сферы ИТ и санкционных ограничений. Компании начали развивать горизонтально масштабируемую инфраструктуру. В итоге, во втором полугодии 2023 года наибольшую актуальность получил тренд на программно-определяемую ИТ-инфраструктуру.

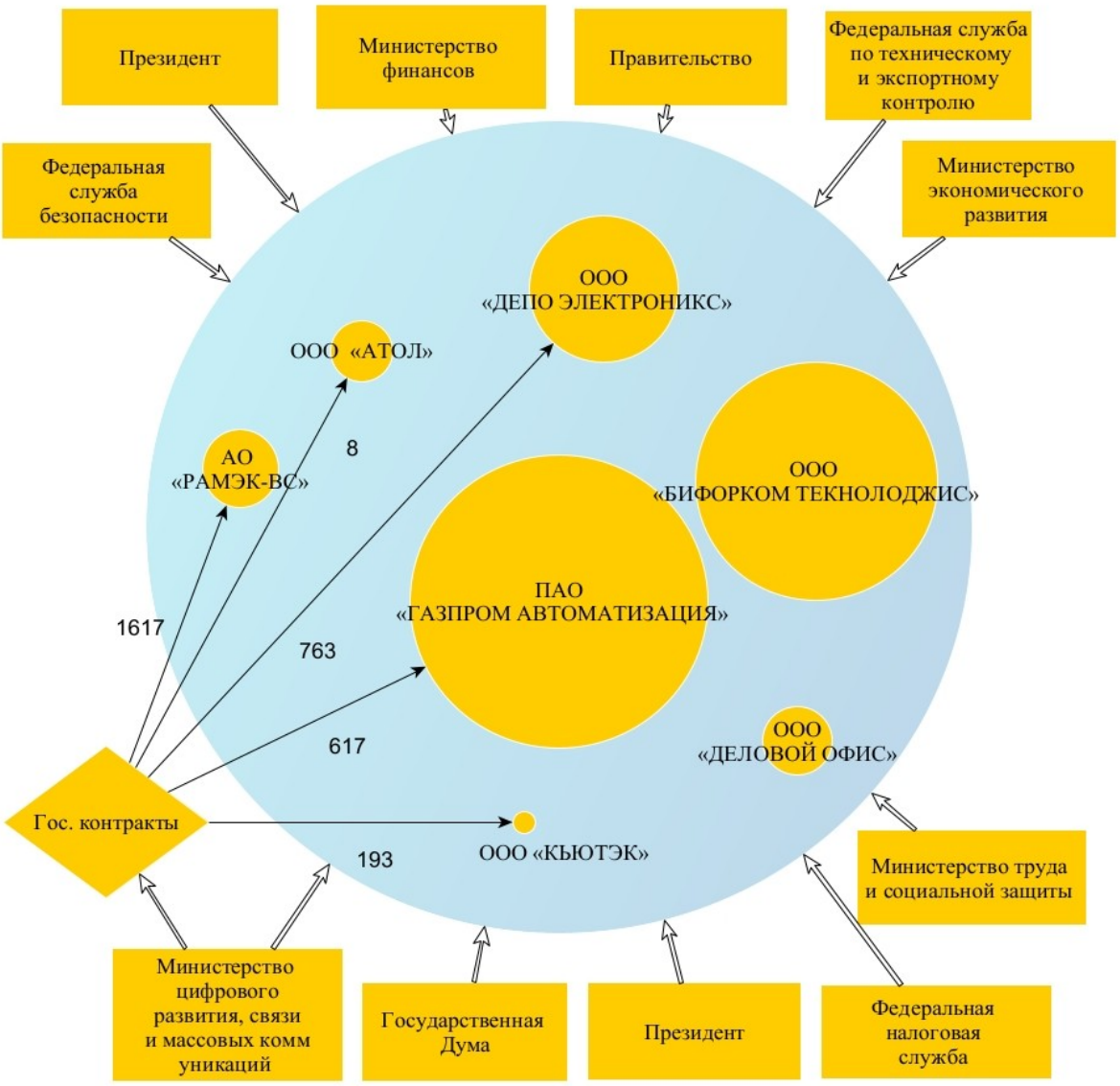
Председатель Правительства России в июне 2022 года дал поручение Минцифры и иным министерствам по созданию в России индустриальных центров компетенций (далее – ИЦК) импортозамещения цифровых решений в ключевых сферах экономики. Также дано поручение по созданию центров компетенций по развитию (далее – ЦКР) российского общесистемного и прикладного программного обеспечения. ИЦК и ЦКР традиционно для страны делают упор на взаимодействии крупнейших отечественных потребителей ИТ продукции с крупнейшими производителями, исключая из данного процесса мелкий и средний бизнес. Концентрация на наиболее крупных отечественных потребителях способствует решению краткосрочных задач, но уменьшает мотивацию создавать конкурентный по мировым стандартам продукт.

Успешность распространения российских ИТ-продуктов на рынки дружественных стран во многом зависит от уровня взаимодействия бизнеса и власти Российской Федерации. Уже существуют практические кейсы выхода на рынки Индии, Китая, Венесуэлы, Кубы и ОАЭ. Наиболее показательна сфера компьютерного и периферийного оборудования, так как заказы на них составляют 23,2% от закупок ИТ-сферы Российской Федерации в 2023 году [115]. По данным «IT Research», присутствие иностранных компаний сократилось до 6%. Такие бренды как Dell, HP и Lenovo прекратили поставки в Россию ПК.

В 2022 году доля госзакупок составляла около 20% оборота сферы ИТ Российской Федерации. В связи с тем, что государство является одним из наиболее крупных заказчиков, необходимо недопущение развития компаний монополистов в данной области и требуется стимулирование развития новых компаний. Так, 6 из 8 компаний, входящих в топ 100, имеют большое количество государственных контрактов.

Из ста наиболее крупных отечественных компаний, только 5 заняты производством компьютеров и периферийного оборудования (ОКВЭД 26.20). Производством оборудования занимаются три компании по направлениям

26.51.7, 26.11 и 26.30, данные по которым представлены на рисунке 8. Рассматривая наиболее крупные компании, производящие АО, необходимо отметить, что, несмотря на значительный рост таких компаний, как ООО «Бифорком Текнолоджис», данное поле показало незначительный рост в 2022 году в связи с общим малым количеством крупных отечественных игроков в данной области.



Источник: составлено автором.
Рисунок 8 – Поле взаимодействия государства и бизнеса сегмента АО

11 компаний относятся к категории ОКВЭД 46.5 (Оптовая торговля информационным и коммуникационным оборудованием). Из данных компаний только 6 являются российскими, смотреть таблицу 17. Данные компании сталкиваются с необходимостью перестройки своих систем иностранных закупок из-за санкционных ограничений. Доминирование продукции иностранных компаний на российском рынке ИТ-оборудования является последствием глобализации мировой экономики, в которой проще закупать продукцию международных компаний, чем вкладывать деньги в отечественное производство, а также отсутствия потребности в краткосрочной перспективе обладать развитым отечественным сегментом производства АО. Как результат – незначительность протекционистских мер до 2022 года. Но благодаря введению санкций и усилению международного противостояния ситуация на российском рынке АО начала кардинально меняться, смотреть таблицу 18.

Таблица 17 – Компании производители АО

Полное название организации	Руководитель	Совладельцы	Выручка в 2023, млрд руб.
ПАО «Газпром Автоматизация»	Бобриков Николай Михайлович	ООО Энергетические решения, АО Газстройпром, ООО Завод Калининградгазавтоматика	25,9
ООО «Депо Электроникс»	Зенин Евгений Владимирович	Эскин Сергей Вадимович, Ирисов Алексей Алексеевич	13,0
ООО «Атол»	Колчина Оксана Александровна	ООО УК АТОЛ, Макаров Алексей Петрович, Макарова Ирина Евгеньевна	5,4
ООО «Кьютэк»	Арсланова Гузель Расимовна	Шитиков Иван Александрович	1,9
ООО «Бифорком Текнолоджис»	Галенко Сергей Николаевич	Закрытый паевой инвестиционный комбинированный фонд «Б4 РАЗВИТИЕ» (управляющая компания: АО «Апекс менеджмент»)	21,0
ООО «Деловой Офис»	Волков Алексей Максимович	Солкин Игорь Геннадьевич	6,0

Источник: составлено автором.

Таблица 18 – Компании производители АО, статистика выручки

Деятельность	Полное название организации	2020 г.			2021 г.			2022 г.			2023 г.		
ОКВЭД Основной		Выручка млрд руб.	Прирост выручки, процент	Уплачено налогов всего млн руб.	Выручка млрд руб	Прирост выручки, процент	Уплачено налогов всего млн руб.	Выручка млрд руб	Прирост выручки, процент	Уплачено налогов всего млн руб	Выручка млрд руб.	Прирост выручки, процент	Уплачено налогов всего млрд руб.
26.51.7	ПАО «Газпром Автоматизация»	26,8	-42,2	-	19,5	-27,4	-	28,2	45,2	-	25,9	-8,3	-
26.20	ООО «Депо Электроникс»	5,5	6,9	353,4	5,1	-5,9	427,3	10,1	96,7	665,9	13,0	29,0	546,7
26.20	ООО «Код Безопасности»	4,9	52,0	891,8	-	-	603,4	-	-	-	-	-	-
26.20	ООО «Атол»	-	-0,9	9,2	4,9	15,4	479,7	3,9	-19,7	282,7	5,4	36,7	445,1
26.20	АО «Рамэк-Вс»	3,9	40,1	328,5	-	-	463,2	-	-	-	-	-	-
26.11	ООО «Кьютэк»	2,0	-13,9	50,5	1,5	-24,1	36,7	2,0	30,5	129,2	1,9	-4,1	71,8
26.30	ООО «Бифорком Текнолоджис»	0,5	104,3	32,2	1,1	116,8	73,3	5,2	375,1	222,3	21,0	305,9	960,2
26.20	ООО «Деловой Офис»	4,3	20,6	123,4	5,7	32,7	256,8	4,8	-16,4	216,9	6,0	24,6	44,3

Источник: составлено автором.

Данная статистика демонстрирует диспропорцию в отношении количества производителей ПО и АО России, смотреть таблицы 15 и 17. Если производители ПО создали объединение компаний-разработчиков программного обеспечения России «Руссофт», которое продвигает интересы российских компаний с помощью технологий GR, то у производителей АО нет подобных влиятельных организаций, способных агрегировать и артикулировать общий запрос на государственные меры поддержки данной сферы. Все рассмотренные наиболее крупные компании в сфере АО принадлежат российским физическим и юридическим лицам, что представлено в таблице 17.

Рассматривая компании-производители АО, можно заметить отличную от общего пула компаний динамику резкого роста в 2022 г. и 2023 г., что представлено на рисунке 9. Ее причиной стал повышенный спрос на оборудование в российском сегменте киберпространства. При этом в период 2022–2023 гг. фиксируется резкий скачок прибыли, что представлено в таблице 19. Данный скачок объясняется уходом иностранных компаний и запретом на поставку иностранного оборудования. Данный показатель демонстрирует, насколько российский рынок был захвачен иностранной ИТ-продукцией.

Источник: составлено автором.

Рисунок 9 – Сумма выручки отечественных компаний в сфере АО

Таблица 19 – Прирост по сравнению с предыдущим годом выручки российских компаний в сфере АО

В процентах

Год	2021	2022	2023	2024
Среднее значение	12,5	17,9	85,2	64,0

Источник: составлено автором.

Благодаря активной государственной поддержке наиболее крупные российские ИТ-компании не только продолжают функционировать, но и демонстрируют активный рост. Но, несмотря на предпринимаемые государством меры в данной области, развитие сферы производства АО невозможно в короткие сроки, так как оно требует не только государственных вложений и специалистов, но и развитых производственных мощностей, для создания которых требуется значительное время. Из-за разрыва отношений с иностранными компаниями недружественных стран увеличивается риск выхода из строя ранее поставленного производственного оборудования. А если учесть, что на современном этапе не происходит поставка комплектующих для ИТ-оборудования и не производится обновление ПО, процесс изнашивания оборудования идет еще быстрее.

Государство легализовало систему параллельного импорта, институционализированную Федеральным законом от 28.06.2022 № 213-ФЗ, как формального института и дополненную многочисленными неформальными институтами в виде коммерческих связей предприятий с зарубежными контрагентами. Система параллельного импорта, с одной стороны, повышает цены иностранных товаров, усложняет их получение и, во многих случаях, снижает их качество, с другой стороны, она частично способствует развитию российских аналогов при использовании систем обратной инженерии в условиях разрыва отношений с компаниями, переставшими поставлять свое оборудование в страну.

Система параллельного импорта полезна как временная краткосрочная мера по удовлетворению запросов потребителей сразу после введения санкций, чтобы смягчить переход на отечественные аналоги. Но в долгосрочной перспективе система параллельного импорта может перейти от поставки через полулегальных поставщиков санкционных товаров к нахождению стабильных легальных маршрутов и производителей из стран, не поддержавших санкции. Это не решит проблему зависимости российского сегмента от иностранных компаний, а произойдет смена тех, от кого будет зависеть Российская Федерация. Поскольку иностранные АО запрещено использовать в органах государственной власти, стратегически важных и системообразующих предприятиях, то необходимо производить отечественное и качественное оборудование, не уступающее своим иностранным аналогам. Только в таком случае можно добиться технологического суверенитета и гарантировать минимальный уровень устойчивости российского сегмента киберпространства.

Для обеспечения работоспособности систем электронного правительства и всего киберпространства Российской Федерации жизненно необходимо форсированное развитие отечественной сферы АО. Что на современном этапе достигается как за счет общих налоговых льгот, послаблений и различных дотаций, так и за счет увеличения количества государственных контрактов. Российским компаниям выгодно активно развивать свои системы и качество продукции для соответствия стандартам льготируемых предприятий.

В случае с взаимодействием компаний в сфере АО и государством наиболее выгодным для обеих сторон является сочетание стратегии развития для государства и стратегии выживания для бизнеса. Данная конфигурация стратегий обладает характеристиками Парето-эффективности и равновесности по Нэшу, что представлено в таблице 20. Компании в сфере АО намного менее развиты, чем компании разработчики ПО. Данные компании подвергаются наибольшему санкционному давлению, им

необходимо перестраивать цепочки поставок материалов и запчастей в сочетании с выполнением новых государственных требований. Их первостепенной задачей в краткосрочной перспективе является сохранение своей рыночной ниши, что возможно только с серьезной государственной поддержкой. С другой стороны, востребованность ИТ-оборудования на российском рынке продолжает расти. Поддерживая компании в сфере АО, государство создает основу для развития киберпространства в среднесрочной перспективе. Объективно стратегия выживания для бизнеса предполагает активизацию импортных поставок из Китая, который еще более монополизирует свое доминирующее положение на рынке. Задача государства в стратегии развития представляется наиболее сложной и противоречивой: сочетать финансирование импортозамещения АО с максимальной лояльностью к китайским поставщикам и поиском альтернативных каналов поставок для минимизации риска перехода поля АО под внешнее управление Китая. Именно стратегия развития способствует повышению уровня устойчивости российского сегмента киберпространства за счет сочетания поддержки максимально возможного импортозамещения и максимально широкой диверсификации зарубежных закупок и финансирования.

Таблица 20 – Матрица исходов взаимодействия государства и бизнеса сегмента АО

АО		Бизнес		
		Стратегия развития	Стратегия выживания	Стратегия зависимости / возвращение к старому
Государство	Стратегия развития	1/1	2/2	0/0
	Стратегия выживания	-1/0	0/-1	-1/-2
	Стратегия зависимости / возвращение к старому	-2/-1	1/-1	-1/-1

Источник: составлено автором.

Как показывает проведённый анализ, сфера АО требует наибольшей государственной поддержки. Нехватка АО на данном этапе компенсируется за счет возросших поставок из Китая, систем параллельного и серого импорта, что не является решением проблемы в долгосрочной перспективе. Достаточно рискованно допускать долговременную зависимость какого-либо сегмента, непосредственно связанного с национальной безопасностью, от другого, пусть и дружественного на современном этапе государства. В современном мире полную независимость от импорта в сфере ИТ не могут себе позволить даже такие геополитические лидеры как США и Китай. Тем не менее, в системообразующих секторах, обеспечивающих национальную безопасность, странам, претендующим на статус стержневых держав по С. Хантингтону, необходимо минимизировать зависимость от импорта и максимально диверсифицировать круг поставщиков. От государства ожидается долгосрочная стратегия развития киберпространства с определением места и роли органов власти и компаний сектора ИТ.

Схемы параллельного импорта и серого импорта, являясь тактически оправданными и вынужденными обстоятельствами, имеют ряд негативных последствий. Они приводят к снижению качества оборудования, проблемам с техническим обслуживанием, нарушению разнообразных международных норм (таможенное и налоговое законодательство, авторское право). К тому же угроза вторичных санкций создает риски отказа экспортеров и зарубежных банков использовать указанные схемы даже несмотря на высокую норму прибыли.

Решением данной проблемы может являться частичное использование китайского подхода в сфере стимулирования научно-технического прогресса [195]. Если государство дает разрешение отечественным компаниям активно копировать и применять иностранные технологии и методы производства, адаптируя их под свои нужды на современном этапе, это частично решает проблемы изолированности страны от технологических инноваций и

недоступности высокотехнологических комплектующих оборудования АО и ПО. Если на территории России зарубежные технологии будут распространяться на правах открытого патента, это позволит простимулировать конкуренцию между отечественными компаниями. Если у компании нет монополии на какое-либо технологическое достижение, и конкуренты могут его скопировать, то постоянные инновации и оптимизации данного процесса будут неотъемлемыми элементами политики компаний. В рамках данного подхода Российская Федерация в 2024 году продолжает выделение грантовой поддержки проектов по обратному инжинирингу [94]. Требуется актуализация устаревших стандартов и норм в сфере кибербезопасности под актуальные условия. ФСТЭК России уже были сделаны предложения со стороны АРПП «Отечественный Софт» разработать стандарты и требования к новым классам средств защиты информации (СЗИ).

Потребность в цифровой модернизации политических и экономических процессов в российском обществе будет увеличиваться в связи с тем, что органы государственной власти, системообразующие предприятия и оборонные системы переходят на преимущественное использование российского программного и аппаратного обеспечения. Органы государственной власти Российской Федерации являются одним из основных заказчиков на российском рынке ИТ. Но необходимо учитывать, что, когда на рынке есть несколько крупных заказчиков, есть риск возникновения монополий, а как следствие необходимо антимонопольное регулирование для сохранения здоровой конкуренции. Развитие цифровизации политического и экономического поля невозможно без мобилизации управляющих единиц поля. Для государственных и корпоративных менеджеров целесообразно создавать систему стимулов для поддержки и развития ИТ-технологий, вводить санкции за неисполнение показателей (например, в форме KPI).

Аудит комплектующих оборудования российских компаний производителей ИТ-оборудования способен реально определить, насколько

российская ИТ-продукция состоит из комплектующих, произведенных на территории России. В рамках данного направления работы появляются новые требования к содержанию в электронике печатных плат российского производства. Необходимо понимание, в каких комплектующих в наибольшей степени нуждаются системообразующие предприятия, системы государственного управления. На основе данных перечней дефицитных комплектующих отечественные предприятия могут получать государственную поддержку по их производству. Повышение степени кластеризации производства и разработки ИТ-оборудования на территории России со временем решит данную проблему.

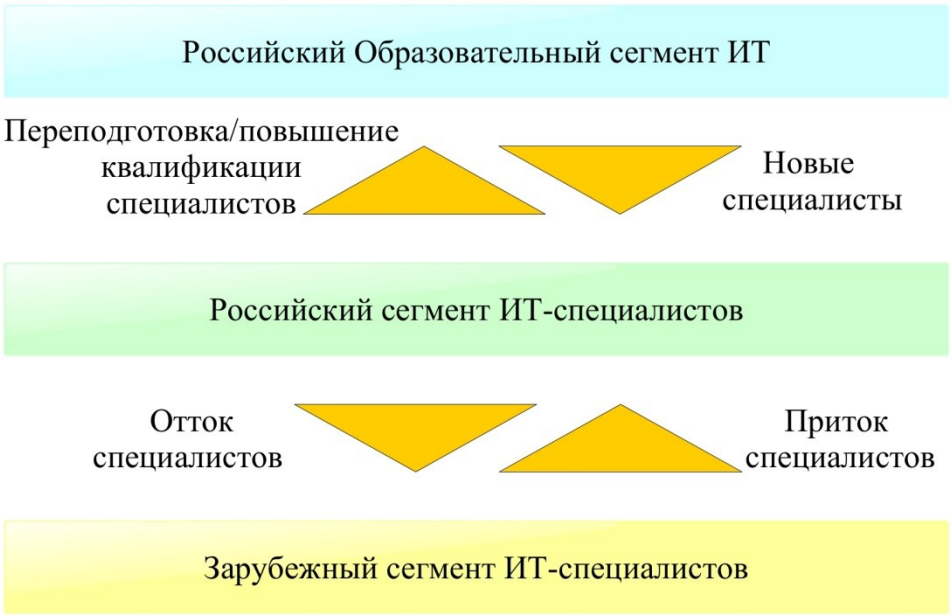
Поле производителей АО требует максимальной государственной поддержки. Требуется не только поддержка развития новых технологий, но и организация кластеров производства и систем поставок ресурсов как на государственном, так и на международном уровнях. Данные системы невозможно выстроить в краткосрочной перспективе, а как следствие требуется развитие долгосрочных государственных программ взаимодействия власти и бизнеса с целью производства АО и достижения технологического суверенитета России.

2.4 Взаимодействие государства и бизнеса в поле подготовки кадров для ИТ-сферы

В данном параграфе рассматривается подготовка новых кадров для системы государственного управления и бизнес-структур, российский сегмент ИТ-образования, проблематика релокантов, динамика кадров ИТ-специалистов в 2019–2023 гг., численность обучающихся по реализуемым образовательным программам в сфере ПО и АО.

Подготовка новых кадров для системы государственного управления и бизнес-структур является одной из наиболее важных сфер взаимодействия

государства и бизнеса. В сфере ИТ подготовка новых специалистов и развитие систем фундаментальных научных исследований обладает особенно тесной связью, так как данная сфера относится к высокотехнологичному сектору экономики страны. Вследствие этого требуются серьезные затраты бизнеса и государства на развитие образовательных программ, а также долгосрочное планирование кадровой политики. Таким образом, в системе взаимодействия государства и бизнеса появляется третья сторона, а именно, образовательный сегмент. Органы государственной власти всех уровней и компании обеспечивают спрос на специалистов ИТ-сферы, а предложение кадров осуществляется как государственными вузами, средними специальными образовательными учреждениями, так и частными образовательными структурами, и самим бизнесом, формирующим компетенции сотрудников. Помимо необходимости способствовать пополнению кадров российских ИТ-компаний перед участниками взаимодействия стоит проблема оттока специалистов за границу. Данная сфера представлена в рисунке 10.



Источник: составлено автором.
Рисунок 10 – Российский сегмент ИТ-образования

«Утечка мозгов» является одной из наиболее серьезных проблем Российской Федерации на современном этапе. Данная проблема актуализировалась в условиях антироссийских санкций после начала СВО. Российское поле ИТ-специалистов пополняется в основном благодаря российскому образовательному полю [181]. Специалисты получают образование, проходят различные курсы по повышению квалификации. Также российское поле пополняется за счет трудовой миграции из-за рубежа, но при этом отток ИТ-специалистов за рубеж является одной из наиболее серьёзных проблем данной сферы на современном этапе. Глава Минцифры России М. Шадаев отметил, что за 2022 год около 10% сотрудников ИТ-компаний покинули Россию, «порядка 100 тыс. ИТ-специалистов находятся за пределами нашей страны» [119]. Основными центрами эмиграции являются страны Европы, Казахстан и Турция. Релокацию российских ИТ-специалистов можно разделить на две основные волны: первая произошла, когда западные организации релоцировали свои наиболее ценные кадры из Российской Федерации, вторая затронула, в основном, молодых специалистов и была связана с началом частичной мобилизации осенью 2022 года.

Эмиграция ИТ-специалистов в большинстве случаев не привела к прекращению их работы на российские компании (переход на удаленный режим), русофобия в недружественных странах создает барьеры для перехода на работу в иностранные фирмы. Панические ожидания краха экономики и всеобщей мобилизации не реализовались, напротив, фиксируется экономический рост, увеличение зарплат, ИТ-специалисты получают льготы и освобождения от мобилизации. Российское налоговое законодательство ужесточило налоговые режимы для нерезидентов, чтобы минимизировать привлекательность релокации [64]. Можно предположить, что российские компании в определенной степени могут извлечь плюсы из релокации своих специалистов, ведь данные сотрудники позволяют более

тесно коммуницировать российским компаниям с иностранными заказчиками и расширять свои связи за рубежом. Также упрощается поиск иностранных специалистов для предложения им работы в российском ИТ-поле.

Хотя в долгосрочной перспективе вероятно возвращение значительной части уехавших специалистов, на современном этапе Российская Федерация принимает активные действия по релокантозамещению. На современном этапе фиксируется рост спроса на высококвалифицированные ИТ-кадры: анализ больших данных, искусственный интеллект, интернет вещей и так далее. По данным «Хэдхантер» спрос на ИТ-специалистов за год с сентября 2022 года вырос на 18% [114]. Максимально эффективное решение проблемы кадрового голода требует консолидации действий бизнеса, системы образования и государства, ведь решение данной проблемы выгодно всем трем сторонам.

Статистические подсчеты количества уехавших и оставшихся в России ИТ-специалистов в период с 2022 г. по 2024 г. затруднены из-за различной трактовки (какие профессии включать) данного понятия аналитическими агентствами. По оценке РАЭК, в период с февраля по май 2022 года Россию покинуло от 50 до 70 тысяч ИТ-специалистов. При этом около 80% из релоцировавшихся специалистов продолжали работать на российские компании из-за рубежа [118].

Необходимо отметить, что по данным опроса, проведенного РУССОФТ в 2024 году, отъезд за рубеж разработчиков ПО в 2023 году перестал быть серьезной проблемой для ИТ-индустрии Российской Федерации. За 2022 год Россию покинуло около 17 тыс. ПО специалистов для работы в иностранных компаниях по контракту или для ПМЖ, в свою очередь, в 2023 году данный показатель не превысил 3,5 тыс. [113]. На основе этого можно сделать вывод, что пик отъезда специалистов за рубеж уже прошёл.

Несмотря на отъезд специалистов, по данным Минцифры России, в течение 2022 года произошло увеличение на 13% количества сотрудников

ИТ-компаний [117], и на 2023 год в ИТ-сфере работало почти 740 тысяч человек. С другой стороны, Росстат оценил количество ИТ-специалистов в России в 2021 году в 1,45 млн человек [120]. В данной работе используются данные из исследований Росстата, представленные в таблице 21. На основе изменения количества специалистов по ИКТ и специалистов-техников в области ИКТ можно сделать вывод, что релокация незначительно повлияла на рынок труда в ИТ-сфере.

Таблица 21 – Численность ИТ специалистов

Специалисты в сфере ИКТ	2019 г.	2020 г.	2021 г.	2022 г.	2023 г.
Специалисты по информационно-коммуникационным технологиям, тыс. человек	986	1094	1131	1171	1241
Специалисты-техники в области информационно-коммуникационных технологий, тыс. человек	159	145	136	188	189

Источник: составлено автором.

С 2019 года по январь 2023 года общая динамика числа активных вакансий и резюме рекрутинговых агентств демонстрировала значительное превышение спроса над предложением в сфере ИТ. По оценке Минцифры, в ИТ-сфере работают почти 740 тысяч специалистов [117], а дефицит кадров примерно был равен 500–700 тысяч человек в 2023 году. Схожую оценку дало «ВНИИ Труда» – дефицит на российском рынке ИКТ составляет примерно 500 тыс. специалистов [93]. Идет рост активного числа ИТ-вакансий в России, что связано как с ростом темпов цифровизации, так и с политикой по импортозамещению.

На основе рассмотренных данных можно сделать вывод, что проблема нехватки кадров в российской ИТ-индустрии не является следствием санкций, связанных с СВО. Санкции лишь вскрыли и актуализировали данную проблему. С учетом взрывного роста ИТ-индустрии даже возвращение всех релокантов на родину не решит проблему дефицита кадров.

В России в 2020 году насчитывалось 1,8 миллиона ИТ-специалистов, из которых менее 1% являлись самозанятыми. Но в 2024 году процент самозанятых достиг 20% от всех ИТ-специалистов [102]. По прогнозу Ассоциации предприятий компьютерных и информационных технологий (далее – АПКИТ), потребность в ИТ-кадрах высшей квалификации в России вырастет с 327 тыс. человек в 2024 году до 367 тыс. человек в 2030 [104].

Были утверждены методики по оценке эффективности деятельности научных организаций в области научно-исследовательских, опытно-конструкторских, а также технологических работ гражданского назначения. Постулируется необходимость повышения уровня образования преподавателей, а также обучение новых специалистов в сфере ИТ. Эти цели достигаются за счет таких проектов, как «Кадры для цифровой экономики», часть национальной программы «Цифровая экономика Российской Федерации» [62].

Одним из наиболее важных законов для развития российской сферы ИТ в долгосрочной перспективе является приказ Минцифры № 712 от 26.09.2022. В соответствии с данным приказом был установлен перечень приоритетных специальностей и направлений подготовки высшего образования. По данным Минцифры на 1 декабря 2023 года около 40 тыс. человек оформило ИТ-ипотеку [98]. По данным Росстата, в 2023 году средняя зарплата в ИТ-сферы составила 155,9 тыс. рублей, что демонстрирует рост зарплаты в 1,7 раз по сравнению с показателями 2019 года [97].

Проблему кадрового голода невозможно решить в короткие сроки, только сконцентрировавшись на подготовке новых и повышении качества уже имеющихся отечественных ИТ-специалистов. «Кадровый голод» на российском рынке не уменьшится даже при постоянном росте количества выпускников вузов по ИТ-специальностям. Основная проблема российского образования в данной области заключается в малом количестве специалистов, способных транслировать актуальные знания, с учетом

высоких темпов развития ИТ-технологий. На современном этапе активно развивается проект Минцифры по обучению языкам программирования школьников в формате бесплатных курсов. Курсы по ИТ-специальностям предоставляются образовательными платформами, такими как «Яндекс. Практикум», «GeekBrains» и «Нетология».

Ключевые задачи на государственной службе и в бизнесе могут выполнять выпускники вузов-лидеров по обучению искусственному интеллекту (ИИ): МФТИ, НИУ ВШЭ, Сколтех, ИТМО, Санкт-ПетербургГУ и МГУ. В ноябре 2023 года экспертами «Альянса в сфере ИИ» по поручению Президента России от 29 января 2023 года [60], и при поддержке Правительства и Министерства науки и высшего образования Российской Федерации был составлен первый в России рейтинг вузов по качеству подготовки специалистов в сфере ИИ, в котором наивысшая оценка была получена НИУ «ВШЭ», МФТИ и Санкт-Петербургским государственным университетом ИТМО [110]. В целях создания удобной и эффективной среды для взаимодействия абитуриентов (поиск работодателя), вузов (актуализация образовательных программ), предприятий (поиск сотрудников) Комитет Совета Федерации по экономической политике выступает за создание государственной федеральной цифровой платформы «ПВА: Предприятие - Вуз - Абитуриент» [116].

В таблице 22 представлены результаты проведенного в рамках данного исследования мониторинга численности обучающихся по образовательным программам в сфере ПО и АО. Список составлен на основе рейтинга RAEX наилучших российских вузов в сфере информационных технологий 2023 года [109]. Необходимо отметить, что в рейтинге 2024 года указывается, что высшие учебные заведения, вошедшие в десятку лучших в 2023 году, несмотря на изменение мест в рейтинге, остались в десятке лидеров [108]. Количество мест по категориям учащихся подсчитано на основе данных, приведенных на официальных сайтах рассматриваемых высших учебных заведений.

Таблица 22 – Численность обучающихся по реализуемым образовательным программам в сфере ПО и АО сфере по данным на 01.02.2024

Университет	Бюджетные места, российские студенты	Платные места, российские студенты	Иностранные граждане	общее количество
1	2	3	4	5
Московский государственный университет имени М.В. Ломоносова	4836	842	380	6058
Московский физико-технический институт (национальный исследовательский университет)	5667	1450	841	7958
Университет ИТМО	5778	2591	1047	9416
Санкт-Петербургский государственный университет	5229	1261	1072	7562
Санкт-Петербургский политехнический университет Петра Великого	7198	2568	1238	11004
Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)	8865	2929	753	12547
Уральский федеральный университет имени первого Президента России Б.Н. Ельцина	960	175	1	1136
Национальный исследовательский ядерный университет «МИФИ»	2843	858	702	4403
Московский авиационный институт (национальный исследовательский университет)	4730	972	272	5702
Российский университет дружбы народов имени Патриса Лумумбы	1027	675	578	2280
Университет МИСИС	2209	2604	516	5329

Продолжение таблицы 22

1	2	3	4	5
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» имени В.И. Ульянова (Ленина)	5506	1368	1171	8045
Национальный исследовательский Томский государственный университет	1802	187	740	2729
Новосибирский национальный исследовательский государственный университет	2592	212	186	2990
Национальный исследовательский университет «МЭИ»	3715	2849	582	7146

Источник: составлено автором на основе [109].

В соответствии с таблицей 22, Московский государственный технический университет им. Н.Э. Баумана на момент начала 2024 года обучал наибольшее количество специалистов в сфере ИТ. Необходимо отметить, что подавляющая часть лидеров по рейтингу RAEX входит в рейтинг университетов софтверной индустрии РУССОФТ за 2023 год (в частности, все члены «Большой восьмерки»: Московский государственный технический университет имени Н.Э. Баумана, Московский физико-технический институт, Национальный исследовательский университет ИТМО, Московский государственный университет имени М.В.Ломоносова, Национальный исследовательский университет «Высшая школа экономики», Национальный исследовательский ядерный университет «МИФИ», Санкт-Петербургский политехнический университет Петра Великого, Санкт-Петербургский государственный университет). Рейтинг РУССОФТ демонстрирует существование «Большой восьмерки» вузов, которые по сумме набранных баллов более чем в два раза превосходят остальных участников рейтинга [111]. Многие учебные заведения, вошедшие

в рейтинг, стремятся повысить качество образования по популярным ИТ-специальностям.

В 2022 году М.В. Мишустин подписал постановление, в соответствии с которым на оценку качества подготовки ИТ-специалистов в вузах выделяется 1,5 млрд рублей [61]. В 2023 году на «цифровые кафедры» поступило 280 тыс. человек. На 2023–2024 учебный год Минобрнауки выделило российским вузам 590101 бюджетных мест, 245 тысяч из них отведено инженерным и техническим направлениям [103]. За пять лет с 2019 г. по 2024 г. произошёл рост количества ИТ-выпускников в вузах на 18% [101].

В соответствии со статистическим сборником «Образование в цифрах: 2023» составленным НИУ ВШЭ совместно с Минобрнауки, Минпросвещения и Росстатом, в России доля выпускников бакалавриата, специалитета и магистратуры в ИТ-сфере составила 5,9% по сравнению с 5,2% в США [24]. Также данное исследование показало, что количество выпускников в сфере ИКТ в 2022 году составило 39,5 тыс. человек, что на 4,6 тыс. больше чем в 2020.

В 2022/23 учебном году на бюджетные места в российские вузы, включая квоту Правительства России по ИТ-специальностям, было принято 117,1 тыс. человек при плановом значении по федеральному проекту в 90 тыс. человек. Всего, начиная с 2021 года, показатель достиг 343,2 тыс. человек, что выше плановых показателей. В приемную кампанию 2022–2023 учебного года по ИТ-специальностям на бюджетные места в вузы было подано более 1,5 млн заявлений, что на 0,1 млн больше по сравнению с предыдущим учебным годом [107]. Рост числа заявлений составил 8,19 % по сравнению с предыдущим учебным годом [96]. По данным Росстата с 2019 по 2024 год на бюджетные места по ИТ-специальностям было принято более 598 тыс. человек [99].

Таким образом, можно констатировать факт роста подготовки специалистов в сфере ИКТ в 2022–2024 гг. российскими вузами посредством увеличения обучающихся на бюджетных и коммерческих местах, а также

расширением системы ДПО. Это позволяет государству и бизнесу как субъектам спроса на кадры ИТ-специалистов получить минимально необходимое количество сотрудников, которые обеспечивают устойчивое функционирование российского сегмента киберпространства.

Выводы по главе 2

В российском сегменте ИТ действуют как отечественные (частные и государственные) компании, так зарубежные компании. Российское государство также является одним из наиболее важных игроков, так как формирует правила игры и оказывает поддержку отечественным компаниям, участвует в капитале ИТ-компаний. Российскому сегменту киберпространства для его устойчивого функционирования и развития необходимы эффективное взаимодействие органов государственной власти (создание условий для развития технологий и систем ИКТ) и бизнеса (разработка и поддержание инноваций), а также выстроенные международные отношения в сфере ИКТ.

Степень изоляции российского ИТ-сегмента от иностранных рынков и компаний продолжает увеличиваться в связи с иностранными санкциями, введенными после начала специальной военной операции в 2022 году. Уход с российского рынка иностранных компаний и запрет на поставку в Россию товаров и услуг открыл беспрецедентные возможности для роста российских ИТ-компаний. Отсутствие иностранных конкурентов и государственные меры поддержки вызвали скачкообразный рост прибылей отечественных компаний. Меры поддержки включают в себя льготные кредиты, отсрочку от армии и льготную ипотеку для специалистов, налоговые льготы и так далее.

Выделяются поле взаимодействия государства и бизнеса разработчиков ПО и поле взаимодействия государства и бизнеса производителей АО, которые обладают своими особыми стратегиями развития, опирающимися на

их ресурсный потенциал, особенности производственного процесса, зависимость от конкретных санкционных ограничений. Выделяются три основные стратегии для действий органов государственной власти и бизнеса в условиях геополитической напряженности: стратегия зависимости; стратегия выживания; стратегия развития.

Несмотря на санкции, рынок ПО продолжил рост, причем до настоящего времени происходит активное сокращение доли иностранной продукции и, как следствие, увеличение продаж отечественных софтверных компаний. Прогнозируется сохранение активных темпов роста отечественного сегмента ПО, его возможное расширение на рынки дружественных стран и создание международной экосреды российского ПО.

Необходимо отметить, что из 100 крупнейших ИТ-компаний России 41 занимается разработкой ПО, большинство из которых принадлежат российским физическим и юридическим лицам. Большое количество крупных компаний в данной области является следствием исторических и экономических особенностей Российской Федерации и может являться драйвером роста экономики в современных условиях, особенно с учетом всесторонней государственной поддержки и новых мер, ограничивающих использование государственными органами и объектами критической инфраструктуры иностранного ПО. Для российского государства и бизнеса в сфере ПО наиболее выгодным будет сочетание стратегий развития, направленных на реализацию имеющегося потенциала. Сочетание указанных стратегий является равновесием Нэша и обладает свойством Парето-эффективности. Данная подсистема функционирования киберпространства находится в наиболее выигрышном состоянии в сравнении с остальными подсистемами.

Санкции нарушили международные линии поставок компонентов и гарантийной поддержки оборудования, чем нанесли серьезный ущерб российским компаниям производителям АО. Но, несмотря на это, в 2022 г. и 2023 г. произошел значительный скачок продаж отечественного

ИТ-оборудования ввиду отсутствия на российском рынке иностранных альтернатив. В период распада СССР произошел захват российского рынка зарубежными производителями, что удерживало российские компании от активного роста, чем объясняется малое количество крупных компаний в данной сфере. Этот факт является одной из наиболее значительных угроз для российского сегмента киберпространства. Наблюдается серьёзная зависимость Российской Федерации от иностранных поставщиков АО.

На современном этапе активно поддерживается государством производство и усовершенствование ИТ-оборудования, что необходимо для развития как российской экономики, так и повышения безопасности страны. Значительную долю оборота отечественной ИТ-сферы составляют государственные закупки. Одной из особенностей обстановки на рынке АО на современном этапе является легализация параллельного импорта, что является временным решением проблемы нехватки продукции на российском рынке. Для устойчивости отечественного сегмента киберпространства оптимальным представляется сочетание стратегии развития со стороны государства и стратегии выживания для российских компаний в сфере АО (им необходимо время, ресурсы, компетенции, технологии, чтобы перестроиться под новые экономические условия). Сочетание указанных стратегий является равновесным по Нэшу и Парето-эффективным.

Одной из наиболее серьёзных проблем поддержания устойчивости национального сегмента киберпространства является нехватка квалифицированных специалистов. Данная проблема остро проявилась после введения санкций и активного релоцирования специалистов за рубеж. Нехватка кадров является системной проблемой российского сегмента 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 из-за рубежа старых специалистов, активному притоку в вузы

абитуриентов на ИТ-специальности и привлечению в страну иностранных специалистов. Решение проблемы нехватки кадров требует долгосрочного государственного планирования в сфере высшего образования и поддержки университетов.

Глава 3
Формирование устойчивого сегмента киберпространства Российской Федерации

3.1 Зарубежный опыт и возможности его адаптации в интересах повышения устойчивости российского киберпространства

В данном параграфе рассматривается: понятие «цифровой суверенитет» и его связь с различными направлениями государственной политики, анализ цифрового суверенитета ряда стран, виды цифрового суверенитета, типы стратегий, обеспечивающих суверенитет национального сегмента киберпространства.

После разоблачений Э. Сноуденом в 2013 году масштабной глобальной практики слежки разведывательных служб США и их союзников актуализировалась проблема защиты государственного суверенитета киберпространства. Информационная безопасность стала неотъемлемой частью национальной безопасности, началось перераспределение глобального киберпространства, его фрагментация на национальные сегменты. Архитектура интернета меняется вместе с политическими концепциями, отражающими особенности состояния политических систем глобальных акторов.

На современном этапе США и КНР являются двумя основными мировыми центрами в сфере ИТ-технологий. Оба государства обладают развитой научной базой, системой поддержки стартапов, крупными ТНК, которые распространяют экосистемы ИКТ на другие государства. Помимо противостояния в экономической и технологической сферах данные государства ведут активное соперничество на международных форумах и конгрессах по кибербезопасности, распространению данных и развитию новых технологий. США и КНР придерживаются несовместимых принципов

регулирования, предлагая в качестве мирового стандарта свою национальную систему контроля киберпространства. Компании из США и КНР могут рассматриваться как источники угрозы безопасности данных и критических инфраструктур для третьих стран.

С усилением значимости проблем национальной кибербезопасности в политическом дискурсе растет количество концепций, связанных с интеграцией национального контроля киберпространства в понятие государственного суверенитета. Авторы используют следующие термины: «цифровой суверенитет», «информационный суверенитет», «технологический суверенитет», «киберсуверенитет», «суверенитет Интернета» и «суверенитет данных».

Понятие «цифровой суверенитет» связывается с различными направлениями государственной политики:

- Политика государства, направленная на укрепление национальной безопасности посредством усиления государственного контроля в цифровой сфере, а также обеспечения соблюдения законов в данной области. Происходит наделение государственных, экономических субъектов полномочиями, централизующими контроль над сетевыми операциями.
- Политика государства, направленная на поддержку участников национальной цифровой экономики, обеспечение устойчивых цепочек поставок и протекционистских мер.
- Политика государства, направленная на защиту социальных и культурных норм и ценностей.
- Политика государства, направленная на помощь людям в контроле над своими данными.

Границы суверенитета в киберпространстве в различных государствах варьируются в зависимости от политического курса, экономического и технологического состояния, а также истории, культуры общества. Наиболее важным фактором является техническая возможность государства

обеспечивать соблюдение своих законов в цифровой сфере и ограничить влияние внешних игроков. Доминирующие на рынке транснациональные фирмы оказывают существенное влияние на деятельность государств, опираясь на свой ресурсный потенциал.

Впервые термин «киберсуверенитет» был популяризирован в заявлениях правительства Китайской Народной Республики как реакция на растущую консолидацию и влияние крупных корпораций в Интернете. Цифровой суверенитет становится способом противодействия «цифровому колониализму». Акцент на цифровой суверенитет наиболее явно обнаруживается в политике стран АТР, Европы, России.

КНР является международным лидером как на региональной, так и на глобальной арене по развитию и «экспорту» в другие страны своей модели киберсуверенитета. Политическая элита Китая выступает за всеобъемлющий государственный контроль над киберпространством и за локализацию данных на территории страны. Киберсуверенитет КНР обладает рядом особенностей: жесткое регулирование деятельности граждан в киберпространстве, протекционизм, развитие отечественных ИТ-компаний и производство аналогов иностранной продукции, контроль за потоками информации, поступающими в национальный сегмент Интернета Китая извне. Институты регулирования интернет-пространства носят ярко выраженный централизованный характер. Система интернет-фильтрации «Золотой щит» блокирует доступ к запрещенному иностранному контенту и источникам информации [219]. Данный проект готовился с 1998 года и начал функционировать в 2003 году.

КНР активно развивал свою систему регулирования киберпространства с 1990-х годов, когда появлялись первые законы, направленные на определение ответственных за регулирование интернет-пространства страны органов власти, а также были сформированы основные правила подключения между внутренней сетью Китая и международными сетями. Уже тогда ответственность за контроль над контентом была частично возложена на

национальные компании. В 2014 году создаются управленческие структуры, координирующие действия по регулированию интернет-пространства разными органами власти. В 2015 году вводится «Anti-Terrorism Law of China», в соответствии с которым по запросу властей провайдеры связи обязаны передавать органам власти ключи шифрования информации [67]. В 2016 году был издан «Cyberspace administration of China», определяющий порядок и специфику обеспечения безопасности информационной инфраструктуры, относящейся к стратегически важным сферам [80]. Также гражданам КНР стало необходимо предъявлять идентификационные данные для пользования интернетом. Весь опубликованный контент в киберпространстве должен храниться на территории страны в течение шести месяцев с момента публикации. В 2021 году закон «Data Security Law of the People's Republic of China» установил юридическую ответственность в отношении субъектов, находящихся за пределами материковой части КНР, которые нарушают законы и угрожают интересам национальной безопасности Китая в ходе обработки данных [79]. Таким образом, утверждается экстерриториальный характер киберсуверенитета КНР. Развитие норм регулирования киберпространства шло параллельно с ростом экономических, технических и политических возможностей КНР по реализации данных норм.

Индия в 1990–2000 гг. благодаря созданию льготной среды для ИТ-компаний привлекла ТНК ИТ-сферы, что способствовало развитию экономики страны. Появление большого числа частных поставщиков ИТ-услуг привело к необходимости регулирования, и в 1997 году было создано The Telecom Regulatory Authority of India [143]. Закон об информационных технологиях определил регулирование правоотношений в сфере ИТ [78]. В 2017 году были изданы «Правила временного приостановления предоставления телекоммуникационных услуг в случае чрезвычайных ситуаций или угрозы общественной безопасности», определяющие обстоятельства, в которых может быть произведена

преднамеренная дестабилизация работы интернета со стороны государства [76]. Ярким примером реализации данного закона является блокировка Индией на своей территории ряда китайских приложений, которые властями Индии были определены как наносящие вред целостности и суверенитету государства. Так, за 2020 год в Индии зафиксировано 129 отключений интернета [137].

На 2020 год Индия стала вторым по величине онлайн-рынком в мире [127]. Индия является мировым лидером по количеству интернет-абонентов. С 1990-х годов Индия во многом сохраняет свою специализацию на активном аутсорсинге услуг в области ИТ и программного обеспечения [216]. Развитие технологий и кадров аутсорсинга наряду с поддержкой ИТ-стартапов цифровой экономики позволили развить Индии свои ТНК. Индия в своей политике в сфере ИТ комбинирует цели по защите критически важной инфраструктуры и данных, укрепления и развития возможностей хостинга и цифровой экономики страны. На современном этапе локализация данных на территории Индии отсутствует.

Вьетнам является ярким примерном экспорта китайской модели регулирования киберпространства, что в данном случае не в полной мере сочетается с экономическим и технологическим уровнем развития страны. Закон о кибербезопасности 2019 года запрещает пользователям интернета распространение недостоверной информации и иную антигосударственную деятельность. С 2022 года ТНК на территории Вьетнама обязаны открывать местные представительства, хранить данные в течение не менее 24 месяцев на вьетнамской территории. В 2023 году была введена обязательная идентификация пользователей социальных сетей.

Закон о кибербезопасности Вьетнама направлен на защиту национальной безопасности государства, определяет обязанности органов власти, организаций и отдельных лиц. Принятые законы критикуются западными странами и международными организациями, так как они не

соответствуют международным нормам кибербезопасности и международным обязательствам Вьетнама в сфере торговли [191].

Австралийская стратегия кибербезопасности нацелена на развитие новых возможностей государства и компаний [69]. В ней акцентируется поддержка инноваций в исследованиях и разработках, направленных на суверенитет киберпространства Австралии. Политики Австралии стремятся сбалансировать интересы национальной безопасности с либерализацией торговли. На современном этапе локализация данных на территории страны не входит в число государственных целей Австралии [126]. В соответствии с «Australian Cyber Security Strategy 2023–2030» Австралия ставит перед собой цель к 2030 году стать мировым лидером в области кибербезопасности [66]. Основой австралийской политики цифрового суверенитета является повышение кибербезопасности, строительство национальных центров обработки данных. Надежность киберзащиты является фактором экономического и социального благополучия, а также быстрого восстановления после кибератак. Сформулирована концепция шести киберщитов, предполагающая сотрудничество государства и бизнеса для повышения национальной киберустойчивости.

Австралия стремится не только придерживаться международного права, но и формировать глобальные правила и стандарты кибербезопасности. Под последней понимается не только защита от угроз, но и поддержка быстрого внедрения и развития новых технологий и цифровой экономики в целом. За кибербезопасность государства отвечает Австралийский центр кибербезопасности (ACSC) [125]. Защита данных регулируется федеральным законом о неприкосновенности частной жизни 1998 года [124]. Существуют федеральные и региональные (на уровне штатов) законы, регулирующие кибербезопасность [128].

Рассматривая развитие киберпространства ЮАР, необходимо указать «Стратегию цифровой трансформации для Африки (2020–2030)», нацеленную на улучшение жизни граждан посредством создания

интегрированного и инклюзивного цифрового общества и экономики [77]. Стратегия предполагает скоординированную деятельность стран для снижения рисков и экономии средств от эффекта масштаба, использование цифровых технологий для преобразования африканских обществ и экономик, внедрение и развитие современных инструментов цифрового управления государством. Однако для достижения провозглашенных целей необходимо для начала осуществить региональную интеграцию в политической, экономической, социальной сферах (аналогично можно анализировать перспективы интеграции киберпространства России и дружественных государств постсоветского пространства). В настоящее время киберпространство многих африканских стран практически полностью зависит от ТНК из США, Европы, набирающих силу компаний Китая. Как следствие, у государств недостает ресурсов и технологий для осуществления контроля за национальными сегментами киберпространства.

ЮАР располагает одним из крупнейших рынков ИКТ в Африке, а также стала технологическим и инновационным центром на континенте. Государство поддерживает кластеры ИТ-стартапов в Кейптауне и в Йоханнесбурге, финансирует наряду с компаниями «CISCO» и «Dell» учебные центры для подготовки кадров. Однако для развития автономной системы кибербезопасности в стране не хватает финансовых, кадровых ресурсов, технологических компетенций. Можно предположить, что выбор ЮАР модели кибербезопасности будет определяться политико-экономическим балансом взаимоотношений со странами Запада и БРИКС с привлечением к сотрудничеству крупных зарубежных и отечественных компаний ИТ-сектора.

Проблема обеспечения информационной безопасности является одним из приоритетных направлений политики Евросоюза (ЕС) на современном этапе. Так, в 2020 году была принята «EU Strategy for Data» – фундаментальный документ в рамках европейской цифровой повестки [123]. Стратегия сочетает в себе экономические цели с проблематикой обеспечения

цифрового суверенитета в контексте информационной безопасности [72]. ЕС исходит из необходимости ограничить вестфальский суверенитет рамками интеграционной структуры, а не отдельных государств-членов союза [169]. Европейский регламент по защите данных оказывает влияние на правовые нормы в сфере ИТ во множестве стран вне ЕС: Бразилия, Индия, Руанда и Южная Корея [134]. У ЕС уже существует свой проект цифрового суверенитета: «Digital sovereignty for Europe» [131]. Идея шенгенской маршрутизации является примером инициативы по локализации данных в Европе. ЕС осознает угрозу постепенной потери контроля над своими данными, способности обеспечивать безопасность в цифровой среде и поддержки инноваций. Набирает популярность подход, направленный на укрепление стратегической автономии Европы в цифровой сфере. Данные предложения подверглись критике со стороны США.

Члены ЕС, такие как Франция, Германия рассматривают цифровой суверенитет, в первую очередь, как экономическую конкурентоспособность и самоопределение, снижение зависимости от иностранных цепочек поставок, поддержку отечественных компаний и киберзащиту. На первое место вышел поиск альтернатив, доминирующим на рынке неевропейским фирмам. Также рассматривается вопрос защищённости персональных данных граждан, соблюдения общественных норм и ценностей. Франция и Германия являются основной движущей силой цифрового суверенитета в Европейском союзе [141]. Данные государства в совместном документе «Gaia-X» указывают необходимость создания суверенной инфраструктуры данных, которая позволит членам ЕС безопасно обмениваться данными. Германия в 2020 году в своей официальной программе председательства в Европейском Совете указывала свое намерение установить цифровой суверенитет как основную повестку европейской цифровой политики [135]. Германские компании признают сильную зависимость от неевропейских поставщиков и партнеров, особенно из США. «Цифровой суверенитет» в Германии рассматривается как способность самостоятельно проводить цифровую трансформацию

(с точки зрения ПО, АО и различных услуг) и возможность самостоятельно определять степень зависимости от поставщиков и партнеров (с точки зрения цифровых технологий и приложений).

Великобритания выступает против признания существования специальной нормы, определяющей вмешательство в компьютерные сети другого государства без его согласия как нарушения территориального суверенитета государства. Великобритания утверждает, что правил киберсуверенитета в действующем международном праве не существует. Великобритания занимает трансатлантическую позицию в переговорах по цифровой торговле.

США обладают цифровой гегемонией, позволяющей контролировать мировые потоки информации [212]. Центральное место в стратегии Департамента в области международной политики в области киберпространства и цифровых технологий занимают усилия по укреплению цифровой солидарности, сотрудничества с союзниками, партнерами в целях формирования дизайна, разработки, управления и использования киберпространства и ИКТ для экономического процветания и интеграции. США в рамках переговоров по цифровой торговле стремятся снять барьеры для трансграничного перемещения данных, а также упростить доступ американских компаний на иностранные рынки.

В «Стратегии национальной безопасности» 2022 года США акцентированы задачи сохранения и укрепления лидерства в киберпространстве, цифровой экономике и новых ИКТ. Стратегия декларирует перераспределение ответственности за защиту киберпространства страны между правительством и организациями частного сектора. Также стратегия национальной безопасности постулирует изменение стимулов в международной политике и экономике посредством долгосрочных инвестиций в кибербезопасность. США выступают против концепции государственного контроля над национальными сегментами

киберпространства. Само понятие «киберсуверенитета» в политическом дискурсе США носит негативный характер [184].

Во внешней политике США продвигают концепцию «Цифровой солидарности» как коллективной работы для достижения общих целей, поддержки союзников и партнеров, обеспечения устойчивости в экономике и технологическом развитии. Данная концепция направлена на согласование национальных интересов США с интересами стран-партнеров. Согласование строистя на совместимых подходах к управлению в сфере ИТ-технологий. В данной концепции США выступают как надежный производитель и поставщик технологий, создатель экосистемы АО, ПО, протоколов, технических стандартов. Также в нее входят фирмы-поставщики и система поставок в целом. Отдельно выделяются операторы подводных кабелей и облачных вычислений, центры обработки данных и инфраструктуры спутниковых сетей.

США активно участвуют в международных форумах по разработке обязательств, норм, стандартов и принципов, формирующих киберпространство и влияющих на цифровые технологии. США продвигают свое видение с помощью таких площадок как «Индо-Тихоокеанская экономическая платформа для процветания», инициатива «Цифровая трансформация с участием Африки», «Американское партнерство для экономического процветания», «Глобальный форум по киберэкспертизе», G7, ОЭСР.

Основной угрозой, которую определяют США, являются авторитарные государства, которые продвигают конкурирующие формы технологического управления киберпространством. КНР определяется как самая масштабная угроза, а также как главное препятствие по проецированию мощи США в Азию. Далее в качестве угрозы рассматриваются Россия, КНДР и Иран. Выражается опасение, что будет регламентирована и ограничена деятельность американских компаний, контролирующих большие данные.

Технологические компании США являлись лидерами первой волны цифровизации, а на современном этапе активно работают над системами искусственного интеллекта (ИИ), что дает США значительные преимущества в процессе формирования будущего цифровых технологий, которые США направляют на реализацию своих международных стратегий.

Таким образом, цифровой суверенитет в современном мире имеет различные вариации, определяемые политическим выбором правящих элит и технологическими возможностями страны, что конкретизируется в разнообразных кейсах согласования интересов государства и бизнеса при взаимодействии в национальном сегменте киберпространства. Можно указать следующие виды цифрового суверенитета:

- Оборонительный – защита национального сегмента киберпространства от внешних угроз. К нему можно отнести ранние системы Китая, либо современную Беларусь.

- Экспансионистский – сочетание защиты национального сегмента киберпространства с атакующими действиями, распространение технологий, кадров, регуляторных норм на национальные сегменты киберпространства зарубежных стран. Примером служат современный Китай и частично Россия.

- Нормативный – обеспечение коллективной защиты национальных сегментов киберпространства на основе общих ценностей с ориентацией на защиту прав человека как гражданина и потребителя. Примером выступают страны ЕС.

- Постколониальный – риторическое дистанцирование от западных технологий и инфраструктуры киберпространства глобальных геополитических лидеров при недостатке своих ресурсов, технологий, кадров, что обусловливает необходимость кооперации с одним из центров силы. Данный вид свойственен странам Латинской Америки, Африки, Азии.

- Гегемонистский – продвижение своих национальных стандартов, технологий, норм регулирования в качестве мировых образцов с помощью инструментов жесткой и мягкой силы на основе обладания технологическим,

кадровым, финансовым лидерством. Примером являются США и их союзник Великобритания.

Проанализированные страновые кейсы позволяют выделить три типа стратегий, обеспечивающих суверенитет 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).

3.2 Перспективы согласования интересов государства и бизнеса в обеспечении устойчивости российского сегмента киберпространства

В данном параграфе рассматривается: взаимодействие власти и бизнеса в поле киберпространства, использование модели «Пять сил Портера» для российских компаний ИТ-сферы (АО и ПО); с использованием метода SWOT анализа политики российского государства и российского сегмента ИТ

компаний анализируются перспективы стратегий акторов политического и экономического поля для достижения устойчивости российского сегмента киберпространства.

На основе теоретической базы, проанализированной в первой главе, и данных анализа взаимодействия власти и бизнеса в период с 2019 г. по 2024 г. во второй главе, можно констатировать следующее.

Взаимодействие власти и бизнеса в поле киберпространства идет по трем основным направлениям:

- АО (Производители, разработчики, и дистрибьютеры как самого оборудования, так и его комплектующих, материалов для его производства);

- ПО (Разработчики, компании, занимающиеся кибербезопасностью);

- кадры (Специалисты ИТ-сектора, учебные заведения всех уровней, государственные и частные программы повышения квалификации).

Согласование интересов государства и бизнеса в обеспечении устойчивости российского сегмента киберпространства осуществляется посредством поддержки государством стабильного развития российских ИТ-компаний в условиях неблагоприятной внешнеполитической обстановки [178]. Взаимодействие направлено на достижение технологической независимости национального сегмента киберпространства, минимизацию дефицита продуктов, услуг и кадров за счет государственной финансовой, организационной поддержки российских ИТ-компаний. Устойчивость информационной системы государства и общества, каковой и является в постиндустриальной стадии киберпространство, становится составным элементом государственного суверенитета.

В процессах взаимодействия бизнеса и государства в поле киберпространства инициатива интеракций может исходить как от субъектов экономики, так и от субъектов политики. Так, политическое решение о введении антироссийских санкций привело к уходу или уменьшению присутствия на российском рынке крупных иностранных субъектов экономической деятельности. С другой стороны, инновационное развитие

ИТ-сектора, изменение технологий вызывают разнообразные последствия и эффекты в разных сферах общественной жизни, которые требуют мер законодательного регулирования.

На современном этапе в условиях санкционного противостояния и в целом негативной внешнеполитической ситуации цели государства и бизнеса Российской Федерации в сфере ИТ взаимодополняют друг друга. Целью органов государственной власти Российской Федерации является максимальная «национализация» (в смысле контроля отечественными акторами) инфраструктуры российского сегмента киберпространства для решения задачи обеспечения национальной безопасности. Целью российских ИТ-компаний является увеличение прибыли путем освоения той части российского рынка, которая была занята иностранными компаниями. Результатом совпадения целей государства и бизнеса становится достижение баланса интересов и выстраивание стратегии действий для обеих сторон. Власти обеспечивают политику протекционизма и финансирования национальных ИТ-компаний, которые, в свою очередь, должны в кратчайшие сроки закрыть потребности российского рынка, и, в особенности, объектов критической инфраструктуры и органов государственной власти отечественными решениями ПО и АО.

Одним из аспектов взаимодействия государства и бизнеса в исследуемый период является возможность игнорировать законы международного сообщества и отдельных государств для достижения национальных целей. В частности, приобретать дефицитную санкционную продукцию с помощью разнообразных, негласно одобряемых схем, не считаться с международным авторским правом.

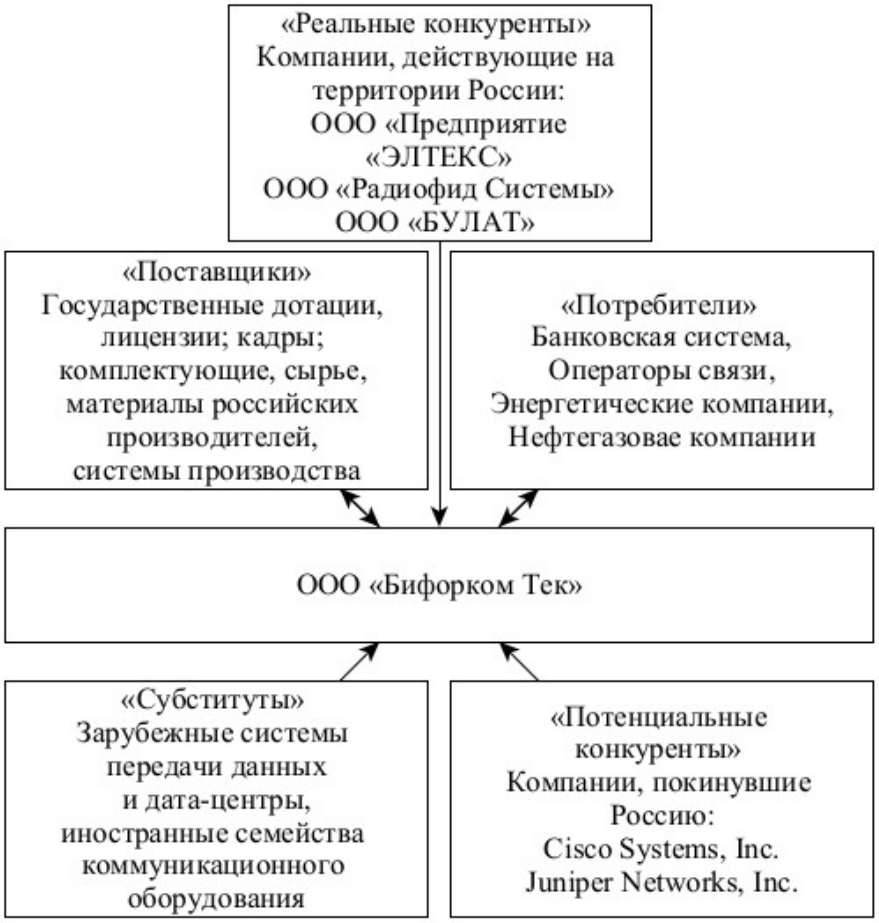
На основе собранных данных составлена схема «Пяти сил Портера» для российских компаний ИТ-сферы, что представлено на рисунке 11. Из схемы следует, что основными потребителями товаров и услуг российского ИТ-сектора являются государственные структуры, российские физические и юридические лица, а также зарубежные покупатели отечественной

продукции. Поставщиками технологий, материальных, финансовых и человеческих ресурсов выступают отечественные и зарубежные компании-производители комплектующих, сырья, материалов, образовательная система подготовки кадров, государство, банковский сектор, фондовый рынок. К реальным конкурентам относятся компании из недружественных и дружественных стран, предлагающие готовую продукцию для российского рынка. К потенциальным конкурентам можно отнести компании из недружественных и дружественных стран, которые еще не присутствуют на отечественном рынке, но потенциально могут войти на него. К товарам-заменителям можно отнести аутсорсинг программных решений и дата-центров.

Источник: составлено автором.

Рисунок 11 – «Пять сил Портера» для ИТ-сферы России

Рассмотрены наиболее крупные компании в сфере ИТ Российской Федерации, из которых выделены компании для анализа в рамках концепции «Пяти сил Портера». ООО «БифоркомТек» рассматривается как пример наиболее крупных компаний производителей АО, что представлено на рисунке 12. В сфере производства АО менее активная конкуренция на российском рынке, чем в сфере ПО в связи с небольшим количеством компаний и крайне высоким порогом для входа для новичков. Иностранные компании-конкуренты, которые до введения санкций являлись активными конкурентами, перешли в разряд потенциальных клиентов, так как в будущем, при изменении международной обстановки могут вернуться в Россию.



Источник: составлено автором.

Рисунок 12 – «Пять сил Портера» для российской компании в сфере АО

Примером компании производителя ПО стала АО «Лаборатория Касперского», что представлено на рисунке 13. В сфере ПО крайне высокая конкуренция в связи с большим количеством компаний и относительно низким порогом для входа. Существует большое количество компаний, производящих продукцию в той же области, что и АО «Лаборатория Касперского», к тому же возможно более активное использование зарубежных субститутов заменителей и аутсорсинга услуг в отличие от сферы АО. Сокращение числа реальных конкурентов из-за рубежа положительно сказывается на развитии отечественных компаний, особенно с учетом государственных дотаций и заказов.

Источник: сставлено автором.

Рисунок 13 – «Пять сил Портера» для российской компании в сфере ПО

На основе полученных расчетов данных о состоянии ИТ-компаний на период 2019–2024 гг. в условиях санкционного давления и мер государственного регулирования национального сегмента киберпространства можно сделать SWOT-анализ российского сектора ИТ, представленный в таблице 23. Анализ построен на предположении, что противостояние России и стран коллективного Запада продолжится как минимум в среднесрочной перспективе (2028–2031 гг.), и ядро политической элиты России не претерпит существенных изменений. Обоснование указанных положений в полях матрицы SWOT-анализа находится в приложении Д.

Таблица 23 – SWOT-анализ российского сегмента ИТ-компаний

S (Strengths)	W (Weaknesses)
1	2
Развита сфера разработки ПО, наличие компаний международного уровня; Рост общего вклада сферы ИТ в экономику страны, прибыльность сферы; Участие в секторе государственных корпораций, квазигосударственных компаний с финансовым и административным ресурсом; Снижение налогов для компаний и облегченный режим проверок; Дотации и отсрочки от военной службы для специалистов; Повышенный интерес молодежи к карьере в сфере ИТ	Неразвитая сфера производства АО, зависимость от импорта АО; Высокая степень зависимости от поддержки иностранного ПО; Нехватка специалистов, отток специалистов за рубеж; Санкционные трудности в приобретении необходимых комплектующих элементов, технологий, компетенци
O (Opportunities)	T (Threats)
Рост отечественных компаний на внутреннем рынке в условиях отсутствия иностранных конкурентов и наличия государственных дотаций; Выход российских компаний на рынки дружественных государств; Рост ниши импортозамещения в связи с сохранением запрета на иностранные ПО и АО в государственном секторе; Наличие большого количества рабочих мест, престижность работы в российской сфере ИТ;	Возможность введения новых санкций, присоединение к антироссийским санкциям новых государств, что затруднит доступ к импортному ПО, АО, комплектующим; После окончания СВО прекратится государственная поддержка ИТ-компаний; Перенос акцента с импортозамещения на механизм параллельного импорта; Захват отечественного рынка компаниями из стран, не поддержавших санкции; Продолжение оттока специалистов;

Продолжение таблицы 23

1	2
Возвращение уехавших специалистов; Увеличение количества ИТ-специалистов, а также повышение их качества за счет новых образовательных программ; Рост компаний в сфере АО	Экономический кризис и внедрение ИИ снизят спрос на ИТ-специалистов, что приведет к падению прибыли и зарплат; Появление компаний-монополистов из-за того, что именно государство является одним из наиболее крупных заказчиков и инвесторов; Сохранение диспропорции между компаниями-производителями ПО и АО

Источник: составлено автором.

Стратегические перспективы развития отечественного сегмента ИТ-бизнеса можно сформулировать как нестрогое неравенство, как показано в формуле (1)

$$S+O \geq W+T, \quad (1)$$

где S – Сильные стороны российского сегмента ИТ-компаний;

O – Возможности для российского сегмента ИТ-компаний;

W – Слабые стороны российского сегмента ИТ-компаний;

T – Угрозы для российского сегмента ИТ-компаний.

Сумма факторов полей «Силы» и «Возможности» практически уравновешивается суммой факторов полей «Слабости» и «Угрозы». Суммы экономических факторов перспектив развития и рисков практически равны, только незначительный перевес суммы политических факторов полей «Силы» и «Возможности» над суммой политических факторов полей «Слабости» и «Угрозы» позволяет поставить знак «больше-равно».

На основе анализа государственной политики Российской Федерации в ИТ-сфере составлен SWOT-анализ государственной политики, представленный в таблице 24. Анализ построен на предположении, что

противостояние России и стран коллективного Запада продолжится как минимум в среднесрочной перспективе (2028–2031 гг.) и ядро политической элиты России не претерпит существенных изменений. Обоснование указанных положений в полях матрицы SWOT-анализа находится в приложении Е.

Таблица 24 - SWOT-анализ российской политики в сфере ИТ

S (Strengths)	W (Weaknesses)
1	2
Выбор курса на максимальное импортозамещение; Финансовое обеспечение цифровизации политики, экономики; Льготы действующим ИТ-специалистам и подготовка новых кадров; Снижение налоговой нагрузки, упрощение администрирования ИТ-сектора; Политическое и экономическое сотрудничество с Китаем	Реактивность политики как ответа на реализовавшиеся риски; Отсутствие единой долгосрочной программы развития и поддержки; Отсутствие значимо эффекта от программ развития сферы АО, игнорирование подмены импортозамещения серым импортом; Сокращение налоговых поступлений в государственный бюджет от ИТ-компаний
O (Opportunities)	T (Threats)
Расширение цифровизации всех сфер жизни общества; Формирование стабильного пула дружественных стран с возможностью сотрудничества в сфере ИТ; Создание и укрепление цифрового суверенитета России	Сокращение программ поддержки после окончания СВО; Уменьшение финансирования и льготирования ИТ-сектора из-за бюджетного дефицита; Оптимизация государственной политики импортозамещения для открытия рынка зарубежным акторам; Отказ от курса на цифровой суверенитет и встраивание в поле киберпространства страны-геополитического лидера

Источник: составлено автором.

Стратегические перспективы политики российского государства в ИТ-сфере также можно сформулировать как нестрогое неравенство, как показано в формуле (2)

$$S+O \geq W+T, \quad (2)$$

где S – Сильные стороны российской политики в сфере ИТ;

O – Возможности для российской политики в сфере ИТ;

W – Слабые стороны российской политики в сфере ИТ;

T – Угрозы для российской политики в сфере ИТ.

Сумма факторов полей «Силы» и «Возможности» практически уравновешивается суммой факторов полей «Слабости» и «Угрозы». Сумма факторов, связанных с наличием экономических ресурсов, политической воли и групповыми интересами государственной элиты как бенефициара киберсуверенитета практически равна сумме факторов, связанных с объективными внутренними и внешними препятствиями реализации политических решений, а также инерцией «исторической колеи» импорта высокотехнологичной продукции. Основываясь на значимости для основных акторов политического режима достижения минимально необходимых параметров технологического суверенитета как элемента государственного суверенитета, можно определить неравенство в качестве нестрогого и поставить знак «больше-равно» между суммой факторов полей «Силы» и «Возможности» и суммой факторов полей «Слабости» и «Угрозы».

Исходя из SWOT-анализов ИТ-сферы и государственной политики в сфере ИТ, целесообразно провести SWOT-анализ национального сегмента киберпространства, который является общим полем для взаимодействия органов государственной власти и компаний ИТ-сектора. Анализ представлен в таблице 25. Анализ построен на предположении, что противостояние России и стран коллективного Запада продолжится как минимум в среднесрочной перспективе (2028–2031 гг.) и ядро политической элиты России не претерпит существенных изменений. Обоснование указанных положений в полях матрицы SWOT-анализа находится в приложении Ж.

Таблица 25 – SWOT-анализ российского сегмента киберпространства

S (Strengths)	W (Weaknesses)
Политический курс на суверенитет национального сегмента киберпространства; Финансовое обеспечение цифровизации всех сфер общественной жизни; Участие в ИТ-секторе государственных корпораций, квазигосударственных компаний с финансовым и административным ресурсом; Относительно высокий уровень развития в сфере разработки ПО; Политико-экономическое сотрудничество с Китаем как страной-производителем дефицитной продукции ИТ-сектора	Преимущественно реактивный характер государственной политики; Высокий уровень серого и черного импорта, использования нелицензионной продукции как результат недостаточного импортозамещения; Дефицит квалифицированных ИТ-специалистов; Технологическое отставание российского АО от иностранных аналогов; Прямые и косвенные санкционные ограничения затрудняют или блокируют доступ к технологиям, элементам материально-технической базы ИТ-сектора
O (Opportunities)	T (Threats)
Рост запроса политических, экономических акторов, граждан России на трансформацию киберпространства в формат максимально автономного национального сегмента как составной части государственного суверенитета; Рост доли ИТ-сектора в экономике страны в связи с ростом спроса на товары услуги сектора со стороны всех сфер общества; Увеличение и углубление связей с постсоветскими дружественными странами, и расширение российской экосистемы ИТ-коммуникаций; Выстраивание сотрудничества с дружественными странами для получения технологий и дефицитной продукции ИТ-сектора	В среднесрочном периоде подмена реального импортозамещения, особенно в сфере АО, серым и черным импортом; Расширение пула стран, поддержавших санкции, что затруднит или блокирует получение технологий и дефицитных товаров ИТ-сектора; Открытие российского рынка крупным зарубежным акторам из дружественных стран; Отказ от курса на цифровой суверенитет и встраивание в поле киберпространства страны-геополитического лидера; Неэффективное или нецелевое расходование бюджетных средств на программы поддержки ИТ-сектора

Источник: составлено автором.

Перспективы развития российского сегмента киберпространства как совокупности взаимодействия стратегий политических и экономических акторов в среднесрочном периоде можно представить в качестве нестрогого неравенства, как показано в формуле (3)

$$S+O \geq W+T, \quad (3)$$

где S – Сильные стороны российского сегмента киберпространства;

O – Возможности для российского сегмента киберпространства;

W – Слабые стороны российского сегмента киберпространства;

T – Угрозы для российского сегмента киберпространства.

Факторы поля «Силы», прежде всего, политические, практически уравновешиваются факторами поля «Слабости», которое включает в себя, прежде всего, экономические факторы и такой значимый внешнеполитический фактор, как международные санкции. Знак «больше-равно» определяется незначительным преимуществом суммы одновекторных стратегий государства и бизнеса (факторы поля «Возможности») над преимущественно политическими угрозами со стороны как недружественных стран, так и дружественных геополитических гегемонов.

Таким образом, российский сегмент киберпространства достигает состояния устойчивости в результате объединения полей «Силы» и «Возможности», которые отражают стратегии действий политических и экономических акторов. Совокупность полей «Слабости» и «Угрозы» отражают риски потери устойчивости российского сегмента киберпространства. Результаты исследования показывают, что сумма факторов полей «Силы» и «Возможности» несколько больше, чем сумма факторов полей «Слабости» и «Угрозы», поэтому российский сегмент киберпространства может продолжать двигаться в направлении достижения суверенитета киберпространства. Исходя из осуществленной классификации, российской практике соответствует экспансионистский вид цифрового суверенитета и первый тип стратегии обеспечения суверенитета.

Выводы по главе 3

Анализ зарубежного опыта форматирования национальных сегментов киберпространства 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, технологическое развитие определяется, прежде всего, наличием отечественных фирм по производству ПО, АО и кадровым потенциалом. Изучение зарубежных кейсов позволило выделить следующие виды цифрового суверенитета:

- Оборонительный – защита национального сегмента киберпространства от внешних угроз. К нему можно отнести ранние системы Китая либо современную Беларусь.

- Экспансионистский – сочетание защиты национального сегмента киберпространства с атакующими действиями, распространение технологий, кадров, регуляторных норм на национальные сегменты киберпространства зарубежных стран. Примером служат современный Китай и частично Россия.

- Нормативный – обеспечение коллективной защиты национальных сегментов киберпространства на основе общих ценностей с ориентацией на защиту прав человека как гражданина и потребителя. Примером выступают страны ЕС.

- Постколониальный – риторическое дистанцирование от западных технологий и инфраструктуры киберпространства глобальных геополитических лидеров при недостатке своих ресурсов, технологий, кадров, что обусловливает необходимость кооперации с одним из центров силы. Данный вид свойственен странам Латинской Америки, Африки, Азии.

- Гегемонистский – продвижение своих национальных стандартов, технологий, норм регулирования в качестве мировых образцов с помощью инструментов жесткой и мягкой силы на основе обладания технологическим,

кадровым, финансовым лидерством. Примером являются США и их союзник Великобритания.

Также на основе анализа зарубежных кейсов определены три типа стратегий, обеспечивающих суверенитет национального сегмента киберпространств:

- 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).

На основе анализа количественных данных был проведен SWOT-анализ российского сегмента ИТ-компаний, политики государства в сфере ИТ, а также интегрированный SWOT-анализ российского сегмента киберпространства. Перспективы развития отечественного сегмента ИТ-сферы и государственной политики в сфере ИТ в соответствии с алгоритмом SWOT-анализа с использованием модели пяти сил Портера можно охарактеризовать как нестрогие неравенства, дающие преимущество сумме полей «Силы» и «Возможности» по сравнению с суммой полей «Слабости» и «Угрозы».

Выявлено, что 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, использования 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: расширение пула стран, поддержавших санкции, что затруднит или блокирует получение технологий и дефицитных товаров ИТ-сектора; открытие российского рынка крупным зарубежным акторам из дружественных стран; отказ от курса на цифровой суверенитет и встраивание в поле киберпространства страны геополитического лидера; неэффективное или нецелевое расходование бюджетных средств на программы поддержки ИТ-сектора (коррупция как политико-экономическое явление).

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 «Возможности» 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.

Взаимодействие государства и бизнеса в национальном сегменте киберпространства – это согласование действий органов государственной власти и компаний ИТ-сектора для достижения целей акторов посредством максимизации выгод, рационализации целей, мобилизации ресурсов. Интересы акторов отражаются в декларируемых и недекларируемых целях. Можно предположить, что ситуационно складывающие балансы интересов государственных органов и компаний ИТ-сектора в разной степени определяют устойчивость российского сегмента киберпространства. Учитывая особенность внешнеполитических вызовов 2014–2024 гг., высокую вероятность продолжения противостояния России и коллективного Запада, можно предположить, что точка согласования интересов государства и бизнеса ИТ-индустрии будет находиться в диапазоне вышеуказанного экспансионистского вида цифрового суверенитета и первого типа стратегии обеспечения суверенитета национального сегмента киберпространства. Подобное сочетание стратегий государства и бизнеса, основанное на их ресурсных возможностях и интересах, позволит наиболее эффективным способом обеспечить устойчивость российского сегмента киберпространства.

Заключение

В качестве теоретической основы исследования взаимодействия государства и бизнеса ИТ-сферы целесообразно опираться на следующие компоненты. Системный подход позволяет анализировать российский сегмент киберпространства как отдельную систему, которая формируется в результате взаимодействий органов государственной власти и компаний ИТ-сектора. Неоинституциональный подход применим для изучения динамики формальных и неформальных правил деятельности политических и экономических акторов, стремящихся реализовать свои интересы. В соответствии с концепциями полей П. Бурдье, Н. Флигстина, Д. Макадама государство анализируется как иерархическое поле, инициирующее появления новых полей и управляющее всей совокупностью полей для достижения поставленных целей.

В качестве методологического инструмента для рассмотрения поведения акторов киберпространства используются элементы теории игр. Взаимодействие органов государственной власти и компаний ИТ-сектора можно рассматривать как кооперативную игру, где акторы обладают ресурсами и возможностями для выбора определенной стратегии, которая в значительной степени определяется влиянием их конечных целей и ограничениями вызовов внешней среды. Предполагается, что для достижения устойчивости российского сегмента киберпространства необходимо найти Парето-эффективное равновесие стратегий акторов. Угрозой для обоюдного выбора стратегий, ведущих к достижению Парето-эффективности, является Парето неэффективное равновесие Нэша.

Для анализа взаимодействия государства с компаниями ИТ-сферы целесообразно использовать концепцию неокорпоративизма, акцентирующую центральную роль государства в выстраивании иерархически подчиненных полей бизнеса и других сфер общества. Для

анализа взаимодействий государства и бизнеса целесообразно использовать такие методы, как статистический анализ, матрицы теории игр, SWOT-анализ, позволяющие не только фиксировать сложившиеся результаты, но и прогнозировать стратегии действий акторов.

Под государством в настоящем исследовании понимаются органы государственной власти, непосредственно участвующие во взаимодействии с компаниями ИТ-сферы. В качестве «бизнеса» в данной работе рассматриваются наиболее крупные компании в сфере ИТ, отобранные на основе рейтингов и проанализированные на основе данных системы «Спарк-Интерфакс». Киберпространство – это созданная для обмена информацией гибридная площадка (платформа), формируемая из совокупности всех информационных устройств, хранящих, обрабатывающих, передающих информацию и задействованных в функционировании сети интернет, а также субъектов коммуникационных, технологических, регуляторных процессов.

Устойчивость киберпространства – это динамическое состояние процессов обмена информацией в гибридном пространстве, обеспечиваемое за счет индивидуальной устойчивости подсистем, из которых оно состоит, а именно: обеспечения стабильной передачи данных, оперативной ликвидации нарушений, а также постоянного развития и обновления технологических, кадровых и регуляционных систем. Для устойчивости национального сегмента киберпространства необходимо наличие инфраструктуры (программного и аппаратного обеспечения, кадров), государственного регулирования (формальных и неформальных институтов, финансирования), которые в состоянии гибко адаптироваться к внешним вызовам. В качестве основных угроз для устойчивости национального сегмента киберпространства определены международные санкции, вероятность отказа от курса на цифровой суверенитет, высокая доля импорта, диспропорциональное развитие сферы программного и аппаратного обеспечения, нехватка кадров.

Национальный сегмент киберпространства может рассматриваться как результат экономической деятельности акторов бизнеса и политико-административной деятельности органов государственной власти. Государство стремится распространить свой суверенитет на национальный сегмент киберпространства, маркируя его границы и регламентируя правила игры акторов.

Под стратегиями акторов политики и экономики понимаются обобщенные планы действий на основе ресурсного потенциала, формальных и неформальных институтов, властных позиций внутри поля для достижения определенных целей.

В российском сегменте ИТ действуют как отечественные (частные и государственные) компании, так зарубежные компании. В период 2022–2024 гг. уход иностранных компаний в связи с политикой антироссийских санкций привел к скачкообразному росту прибылей отечественных компаний, обусловленному также льготными кредитами, снижением налогового бремени, государственными заказами. Для противодействия релокации кадров ИТ-сектора государство предложило отсрочку от службы в армии и льготную ипотеку для специалистов.

Российский сегмент ИТ-компаний состоит из поля разработчиков ПО и производителей АО, которые обладают своими особыми стратегиями развития, опирающимися на их ресурсный потенциал, особенности производственного процесса товаров и услуг, а также конкретных санкционных ограничений. В условиях геополитического кризиса условно можно обозначить три варианта стратегии каждого игрока для взаимодействия государства и бизнеса: стратегия зависимости; стратегия выживания; стратегия развития.

Из 100 крупнейших ИТ-компаний России 41 занимается разработкой ПО, большинство из которых принадлежат российским физическим и юридическим лицам. Обладающие ресурсами и компетенциями разработчики ПО с учетом всесторонней 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 (в данном случае обоих игроков).

В поле АО российские компании играли второстепенную роль по сравнению с иностранными фирмами, основная часть продукции импортировалась. Санкции нарушили каналы зарубежного импорта компонентов и гарантийной поддержки оборудования, чем нанесли серьезный ущерб российским компаниям производителям АО. Но, несмотря на это, в 2022–2023 гг. произошел значительный скачок продаж отечественного ИТ-оборудования ввиду отсутствия на российском рынке иностранных альтернатив. На современном этапе российское государство активно поддерживает производство и усовершенствование ИТ-оборудования, что необходимо для развития как российской экономики, так и повышения безопасности страны. Значительную долю оборота отечественной ИТ-сферы составляют государственные закупки. Одной из особенностей рынка ИТ на современном этапе является легализация параллельного импорта, что является временным решением проблемы нехватки ИТ-продукции на российском рынке. Для устойчивости отечественного сегмента киберпространства оптимальной представляется сочетание стратегии развития со стороны государства и стратегии выживания для российских компаний в сфере АО (им необходимо время, ресурсы, компетенции, технологии, чтобы перестроиться под новые экономические условия). Данная конфигурация стратегий обладает характеристиками Парето-эффективности и равновесности по Нэшу.

Одной из наиболее серьёзных проблем российского ИТ-сегмента является серьёзная нехватка квалифицированных специалистов. Данная проблема остро проявилась после введения санкций и активного релоцирования специалистов за рубеж. Нехватка кадров является системной проблемой российского сегмента ИТ. Она вызвана долголетним малым интересом общества к отечественной ИТ-сфере и активной «утечкой мозгов» за рубеж. Но резкий рост ИТ-компаний в 2020–2025 гг., повышение заработной платы в совокупности с государственной поддержкой способствуют возвращению из-за рубежа старых специалистов, активному притоку в вузы абитуриентов на ИТ-специальности. Решение проблемы нехватки кадров требует долгосрочного государственного планирования в сфере высшего образования и поддержки университетов.

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 (исключенности) в глобальные цепочки обмена товарами и услугами. Изучение зарубежных кейсов позволило выделить следующие виды цифрового суверенитета, нацеленного на поддержание устойчивости национального сегмента киберпространства:

- Оборонительный – защита национального сегмента киберпространства от внешних угроз. К нему можно отнести ранние системы Китая либо современную Беларусь.

- Экспансионистский – сочетание защиты национального сегмента киберпространства с атакующими действиями, распространение технологий,

кадров, регуляторных норм на национальные сегменты киберпространства зарубежных стран. Примером служат современный Китай и частично Россия.

- Нормативный – обеспечение коллективной защиты национальных сегментов киберпространства на основе общих ценностей с ориентацией на защиту прав человека как гражданина и потребителя. Примером выступают страны ЕС.

- Постколониальный – риторическое дистанцирование от западных технологий и инфраструктуры киберпространства глобальных геополитических лидеров при недостатке своих ресурсов, технологий, кадров, что обусловливает необходимость кооперации с одним из центров силы. Данный вид свойственен странам Латинской Америки, Африки, Азии.

- Гегемонистский – продвижение своих национальных стандартов, технологий, норм регулирования в качестве мировых образцов с помощью инструментов жесткой и мягкой силы на основе обладания технологическим, кадровым, финансовым лидерством. Примером являются США и их союзник Великобритания.

На основе анализа зарубежных кейсов можно выделить 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).

На основе 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 были получены следующие выводы. Перспективы развития отечественной ИТ-сферы и государственной политики в сфере ИТ характеризуются как нестрогие неравенства, в которых сумма политико-экономических факторов полей «Силы» и «Возможности» несколько превышает значение суммы политико-экономических факторов полей «Слабости» и «Угрозы».

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: расширение пула стран, поддержавших санкции, что затруднит или блокирует получение технологий и дефицитных товаров ИТ-сектора; открытие российского рынка крупным зарубежным акторам из дружественных стран; отказ от курса на цифровой суверенитет и встраивание в поле киберпространства страны геополитического лидера; неэффективное или нецелевое расходование бюджетных средств на программы поддержки ИТ-сектора (коррупция как политико-экономическое явление).

Перспективы развития российского сегмента киберпространства также могут быть охарактеризованы как нестрогое неравенство, в котором сумма факторов (в основном политических) полей «Силы» и «Возможности» несколько перевешивает значение суммы полей «Слабости» и «Угрозы» (также в основном политических). Результаты SWOT-анализа показывают реальную возможность достижения устойчивости российского сегмента киберпространства на основе конгруэнтности стратегий государства и бизнеса в сфере ПО и АО.

Согласование интересов государства и бизнеса в национальном сегменте киберпространства определяется конгруэнтностью стратегий действий органов государственной власти и компаний ИТ-сектора для достижения целей акторов (максимизации желаемого результата). Ситуационно складывающие балансы интересов государственных органов и компаний ИТ-сектора в разной степени определяют степень устойчивости российского сегмента киберпространства. Учитывая особенность внешнеполитических вызовов 2014–2024 гг., высокую вероятность продолжения противостояния России и коллективного Запада, можно предположить, что точка согласования интересов государства и бизнеса ИТ-индустрии будет находиться в диапазоне вышеуказанного экспансионистского вида цифрового суверенитета и первого типа стратегии обеспечения суверенитета национального сегмента киберпространства.

Основным интересом органов государственной власти России в настоящее время и в среднесрочной перспективе является максимальная

«национализация» (в смысле контроля отечественными акторами) 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.

Список литературы

Книги и монографии

1.Ансофф, И. Новая корпоративная стратегия / И. Ансофф, Э.Дж. Макдоннелл ; перевод с английского С. Жильцов. – Санкт-Петербург : Питер Ком, 1999. – 414 с. – ISBN 5-314-00105-5.

2. Бессонова, О.Э. Раздаточная экономика России: эволюция через трансформации / О.Э. Бессонова. – Москва : РОССПЭН, 2006. – 44 с. – ISBN 5-8243-0725-3.

3. Большой экономический словарь / А.Б. Борисов. – Москва : Книжный мир, 2003. – 895 с. – ISBN 5-8041-0049-1.

4. Большой экономический словарь : 26500 терминов / под редакцией А.Н. Азрилияна. – 7-е издание дополненое. – Москва : Институт новой экономики, 2008. – 1472 с. – ISBN 5-89378-012-4.

5. Бурдьё, П. Социология политики / П. Бурдьё ; составлен, общая редакция и предисловие Н.А. Шматко ; перевод с французского: Е.Д. Вознесенская [и др.]. – Москва : Socio-Logos, 1993. – 333 с. – ISBN 5-86709-005-1.

6. Гаман-Голутвина, О.В. Политические элиты России: Вехи исторической эволюции / О.В. Гаман-Голутвина. – Москва : РОССПЭН, 2006. – 446 с. – ISBN 5-8243-0805-5.

7.Горлушкина, Н.Н. Системный анализ и моделирование информационных процессов и систем / Н.Н. Горлушкина. – Санкт-Петербург : Университет ИТМО, 2016. – 120 с. – ISBN отсутствует.

8. Дзялошинский, И.М. Современное медиапространство России / И.М. Дзялошинский. – Москва : Аспект Пресс, 2015. – 312 с. – ISBN 978-5-7567-0774-8.

9. Жувенель, Б. де Власть. Естественная история ее возрастания / Б. де Жувенель ; перевод с французского А.В. Матешук, В.П. Гайдамака. – Москва : ИРИСЭН : Мысль, 2010. – 544 с. – ISBN 978-5-91066-036-0.

10. Кант, И. Сочинения / И. Кант. – Москва : Мысль, 1935. Том 4. – Часть 1. – 260 с. – ISBN отсутствует.

11. Кордонский, С. Сословная структура постсоветской России / С. Кордонский. – Москва : Институт Фонда «Общественное мнение», 2008. – 216 с. – ISBN 978-5-93947-025-4.

12. Кордонский, С.Г. Ресурсное государство : сборник статей / С.Г. Кордонский. – Москва : REGNUM, 2007. – 108 с. – ISBN 5-91150-006-X.

13. Коуз, Р. Фирма, рынок и право / Р. Коуз. – Москва : Новое издательство, 2007. – 224 с. – SBN 978-5-98379-087-2.

14. Краткая философская энциклопедия / Е.Ф. Губский, Г.В. Кораблева, В.А. Лутченко. – Москва : Прогресс, 1994. – 574 с. – ISBN 5-01-004135-9.

15. Крыштановская, О. Анатомия российской элиты / О. Крыштановская. – Москва : Захаров, 2005. – 384 с. – ISBN 5-8159-0457-0.

16. Ланир, Д. Вы не гаджет : манифест / Д. Ланир ; перевод с английского М. Кононенко. – Москва : Астрель : Corpus, cop, 2011. – 317 с., – ISBN 978-5-271-36292-7.

17. Луман, Н. Истина, знание, наука как система / Н. Луман. – Москва : Логос, 2016. – 408 с. – ISBN 978-5-8163-0088-9.

18. Льюс, Р.Д. Игры и решения : введение и критический обзор / Р.Д. Льюс, Х. Райфа ; перевод с английского И.В. Соловьева ; под редакцией Д.Б. Юдина; с предисловием А.А. Ляпунова. – Москва : Издательство иностранной литературы, 1961. – 642 с. – ISBN отсутствует.

19. Манойло, А.В. Государственная информационная политика в особых условиях : монография / А.В. Манойло. – Москва : МИФИ, 2003. – 388 с. – 500 экз. – ISBN 5-7262-0510-3.

20. Методология : Словарь системы основных понятий / А.М. Новиков, Д.А. Новиков. – Москва : Книжный дом «ЛИБРОКОМ», 2013. – 208 с. – ISBN 978-5-397-03756-3.

21. Николаев, И.А. Дуализм экономической стратегии России в условиях внешних ограничений : Научный доклад / И.А. Николаев. – Москва : Институт экономики РАН, 2023. – 53 с. – ISBN 978-5-9940-0737-2.

22. Новый словарь русского языка. Толково-словообразовательный : Свыше 136000 словарных статей, около 250000 семантических единиц : в 2 томах. / Т.Ф. Ефремова. – Москва : Русский язык, 2000. Том 2. – 1084 с. – ISBN 5-200-02802-7.

23. Новый экономический словарь : 10000 терминов / А.Н. Азрилиян и другие ; под редакцией А.Н. Азрилияна. – Издание 2-е, дополненное, – Москва : Институт новой экономики, 2007. – 1088 с. – ISBN 5-89378-020-5.

24. Норт, Д. Институты, институциональные изменения и функционирование экономики / Д. Норт ; перевод с английского А.Н. Нестеренко ; предисловие и научная редакция Б.З. Мильнера. – Москва : Фонд экономической книги «Начала», 1997. – 180 с. – ISBN 5-88581-006-0.

25. Образование в цифрах : 2023 : краткий статистический сборник / Т.А. Варламова, Л.М. Гохберг, О.К. Озерова [и др.]. – Национальный исследовательский университетт «Высшая школа экономики». – Москва : ИСИЭЗ ВШЭ, 2023. – 132 с. – ISBN 978-5-7598-3004-7.

26. Операции информационно-психологической войны : методы, средства, технологии. Краткий энциклопедический словарь / В.Б. Вепринцев, А.В. Манойло, А.И. Петренко, Д.Б. Фролов. – Москва : Горячая линия – Телеком, 2020. – 496 с. – ISBN 978-5-9912-0173-5.

27. Организация предпринимательской деятельности : учебник / А.Н. Асаул. – Санкт-Петербург : АНО ИПЭВ, 2009. – 336 с. – ISBN 978-5-91460-023-2.

28. Павроз, А.В. Теория политического плюрализма : сущность, противоречия, альтернатива / А.В. Павроз. – Санкт-Петербург :

Издательство Санкт-Петербургского государственного университета, 2009. – 178 с. – ISBN 978-5-288-04915-6.

29. Парсонс, Т. О социальных системах / Т. Парсонс ; под общей редакцией В.Ф. Чесноковой и С.А. Белановского. – Москва : Академический Проект, 2002. – 830 с. – ISBN 5-8291-0242-0.

30. Портер, М.Е. Конкурентное преимущество : Как достичь высокого результата и обеспечить его устойчивость : учебное пособие / М.Е. Портер – 4-е издание – Москва : Альпина Паблишер, 2016. – 715 с. – ISBN 978-5-9614-5727-8.

31. Радаев, В.В. Эволюция организационных форм в условиях растущего рынка (на примере российской розничной торговли) / В.В. Радаев. – Москва : ГУ ВШЭ, Препринт WP4/2006/06., 2006. – 57 с. – ISBN отсутствует.

32. Российская социологическая энциклопедия / под общей редакцией Г.В. Осипова. – Москва : Норма-Инфра, 1998. – 672 с. – ISBN 5-89123-163-8.

33. Словарь по обществознанию : учебное пособие для абитуриентов вузов / Ю.Ю. Петрунин, М.И. Панов, Л.Б. Логунова [и др.] ; под редакцией Ю.Ю. Петрунина. – 3-е издание. – Москва : КДУ, 2006. – 512 с. – ISBN 5-98227-117-9.

34. Современный экономический словарь-справочник / М.М. Гацалов. – Ухта : УГТУ., 2002. – 371 с. – ISBN 5-88179-274-2.

35. Стасова, Т.М. Взаимоотношения бизнеса и государства : теоретические аспекты : монография / Т.М. Стасова. – Москва : КУРС, 2012. – 184 с. – 500 экз. – ISBN 978-5-905554-27-8.

36. Филимонов, Г.Ю. Технологии «мягкой» силы на вооружении США : ответ России : монография / Г.Ю. Филимонов, О.Г. Карпович, А.В. Манойло. – Москва : РУДН, 2015. – 581 с. – 500 экз. – ISBN 978-5-209-06354-4.

37. Флигстин, Н. Теория полей / Н. Флигстин, Д. Макадам ; перевод с английского Е.Б. Головляницыной ; под научной редакцией В.В. Радаева ;

Национальный исследовательский университет «Высшая школа экономики». – Москва : Издание дом Высшей школы экономики, 2022. – 464 с. – ISBN 978-5-7598-2667-5.

38. Фон Нейман, Дж. Теория игр и экономическое поведение / Дж. фон Нейман, О. Моргенштерн ; перевод с английского под редакцией и с добавлениями Н.Н. Воробьева. – Москва : Наука, 1970. – 707 с. – ISBN отсутствует.

39. Фридман, Л. Стратегия. Война, революция, бизнес / Л. Фридман. – Москва : Кучково поле, 2017. – 768 с. – ISBN 978-5-9950-0832-3.

40. Чирикова, А.Е. Регионы-лидеры : экономика и политическая динамика (на примере Ярославской и Самарской областей) / А.Е. Чирикова, Н.Ю. Лапина. – Москва : Издателство Института социологии РАН, 2002. – 326 с. – ISBN 5-89697-072-2.

41. Шеллинг, Т. Стратегия конфликта / Т. Шеллинг ; перевод с английского Т. Даниловой. – Москва : ИРИСЭН, 2007. – 373 с. – ISBN 978-5-91066-004-9.

42. Arquilla, J. Swarming and the future of conflict / J. Arquilla, D. Ronfeldt. – Santa Monica : RAND, 2000, – 98 p. – ISBN 978-0-8330-2885-3.

43. Bentley, A.F. The process of government / A.F. Bentley. – Edit by P.H. Odegard. – Cambridge (Massachusetts) : Belknap press of Harvard university press, 1967. – XLIV, III-XVI, – 501 p. – ISBN отсутствует.

44. Betz, D.J. Cyberspace and the State. Towards a Strategy for Cyber-Power / D.J. Betz, T. Stevens. – London : Routledge, 2011. – 162 p. – ISBN 978-0-4155-2530-5.

45. Buchanan, J.M. The Calculus of Consent : Logical Foundations of Constitutional Democracy / J.M. Buchanan, G. Tullock. – Ann Arbor : The University of Michigan Press, 1962. – 361 p. – ISBN 978-0-4720-6100-6.

46. Cawson, A. Corporatism and political-theory / A. Cawson. – Blackwell : Publishers, 1986. – 174 p. – ISBN 978-0-6311-3279-0.

47. Clarke, R.A. Cyberwar. The Next Threat to National Security and What to Do About It / R.A. Clarke, R.K. Knake. – New York : Ecco, 2011. – 320 p. – ISBN 978-0061962240.

48. Hoffman, F.G. Conflict in the 21-st century. The rise of hybrid wars / F.G. Hoffman. – Arlington : Potomac Institute for policy studies, 2007. – 72 p. – ISBN отсутствует.

49. Kukkola, J. Digital Soviet Union. The Russian national segment of the internet as a closed national network shaped by strategic cultural ideas / J. Kukkola. – National Defence University Series 1 : Research Publications № 40. Helsinki : National Defence University, 2020, – 491 p. – ISBN 978-951-25-3131-8.

50. Lipton, J. Rethinking Cyberlaw : A New Vision for Internet Law / J. Lipton. – Cheltenham : Edward Elgar Publishing LTD, 2015. – 176 p – ISBN 978-1-78100-217-9.

51.Porter, M.E. Competitive Strategy : Techniques for Analyzing Industries and Competitors / M.E. Porter. – New York : Free Press, 1998. – 397 p. – ISBN 978-0-6848-4148-9.

52. Porter, M.E. The Competitive Advantage of Nations : With a New Introduction / M.E. Porter. – New York : The Free Press, 1990, Palgrave Tenth Edition, 1990 – 896 p. – ISBN 978-0-0292-5361-8.

53. Rapoport, A. Two-person game theory ; the essential ideas / A. Rapoport. – Ann Arbor : University of Michigan Press, 1966. – 229 p. – ISBN 978-0-4720-5015-4.

54. Rosenau, J. The Scientific Study of Foreign Policy / J. Rosenau. – New York : The Free Press, 1971. – 472 p. – ISBN 978-0029270103.

55. Schmitt, M.N. Tallinn manual 2.0 on international law applicable to cyber operations / M.N. Schmitt, L. Vihul. – Cambridge : Cambridge university press, 2017. – 638 p. – ISBN 978-1-3166-3037-2.

56. Smith, J.M. Evolution and the Theory of Games / J.M. Smith. – Cambridge : Cambridge University Pres, 1982. – 234 p. – ISBN 978-0-5212-8884-2.

57. Stevens, T. Cyber Threats and NATO 2030 : Horizon Scanning and Analysis / T. Stevens, A. Ertan, K. Floyd, P. Pernik. – Tallinn : NATO Cooperative Cyber Defence Centre of Excellence, 2021. – 268 p. – ISBN 978-9916-9565-0-2.

58. Truman, D.B. The Governmental Process. Political Interests and Public Opinion / D.B. Truman. – New York : Praeger, 1981. – 576 p. – ISBN 978-0-3132-2912-1.

Нормативные правовые акты

59. Российская Федерация. Законы. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ (редакция от 03.08.2018). – Справочно-правовая система «Консультант Плюс». – Текст : электронный. – URL: https://www.consultant.ru/document/cons_doc_LAW_5142/ (дата обращения: 02.03.2025).

60. Российская Федерация. Законы. Перечень поручений по итогам заседания Госсовета (утверждено Президентом РФ 29 января 2023 г. № Пр-173ГС). – Информационно-правовой портал ГАРАНТ.РУ. – Текст : электронный. – URL: https://www.garant.ru/products/ipo/prime/doc/406166551/ (дата обращения: 17.03.2025).

61. Российская Федерация. Законы. О дополнительных гарантиях и компенсациях военнослужащим и сотрудникам федеральных органов исполнительной власти, участвующим в контртеррористических операциях и обеспечивающим правопорядок и общественную безопасность на территории Северо-Кавказского региона Российской Федерации [Постановление Правительства Российской Федерации от 09.02.2004 № 65 (редакция от 26.07.2019, с изменениями от 30.12.2024)]. – Справочно-правовая система «Консультант Плюс». – Текст : электронный. – URL:

https://www.consultant.ru/document/cons_doc_LAW_46495/ (дата обращения: 17.03.2025).

62. Российская Федерация. Законы. Об определении способа перечисления средств субсидии из федерального бюджета автономной некоммерческой организации высшего образования «Университет Иннополис» на проведение повышения квалификации преподавателей высшего и среднего профессионального образования по новым программам для ИТ-специальностей и различных предметных отраслей и обеспечение достижения отдельных результатов федерального проекта «Кадры для цифровой экономики» с применением казначейского обеспечения обязательств [Приказ Минцифры России от 25.01.2021 № 27]. – Справочно-правовая система «Консультант Плюс». – Текст : электронный. – URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=EXP&n=761368#2uum7uUwbd7msvYJ (дата обращения: 20.07.2025).

63. Российская Федерация. Законы. О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы [Указ Президента Российской Федерации от 09.05.2017 № 203]. – Справочно-правовая система «Консультант Плюс». – Текст : электронный. – URL: https://www.consultant.ru/document/cons_doc_LAW_216363/ (дата обращения: 17.03.2025).

64. Российская Федерация. Законы. О внесении изменений в части первую и вторую Налогового кодекса Российской Федерации, отдельные законодательные акты Российской Федерации и о приостановлении действия абзаца второго пункта 1 статьи 78 части первой Налогового кодекса Российской Федерации : федеральный закон [принят Государственнлй Думой 31 июля 2023 года]. – Справочно-правовая система «Консультант Плюс». – Текст : электронный. – URL: https://www.consultant.ru/document/cons_doc_LAW_453241/ (дата обращения: 17.03.2025).

65. Цифровая трансформация. Термины и определения: СТБ 2583-2020. – Введен 01.03.2021. – Минск : Госстандарт Белорусский государственный институт стандартизации и сертификации , 2020. – 16 с. – ISBN отсутствует.

66. 2023–2030 Australian Cyber Security Strategy – Текст : электронный. URL: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf (дата обращения: 10.12.2024).

67. Anti-Terrorism Law of China (2018) 反恐怖主义法// China Justice Observer – Текст : электронный. – DOI отсутствует. – URL: https://www.chinajusticeobserver.com/law/x/anti-terrorism-law-20180427/intro (дата обращения: 10.12.2024).

68. Article 20, para. 1 of Directive (EU) 2024/1226 of the European Parliament and of the Council of 24 April 2024 on the definition of criminal offences and penalties for the violation of Union restrictive measures and amending Directive (EU) 2018/1673 – An official website of the European Union. – Текст : электронный. – URL : https://european-union.europa.eu/index_en (дата обращения: 17.03.2025).

69. Australia’s Cyber Security Strategy 2020 – The Department of Home Affairs Austrelian Government. – Текст : электронный. – URL: https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/australias-cyber-security-strategy-2020 (дата обращения: 20.03.2025).

70. China's Military Strategy – The State Council Information Office of the People's Republic of China – Текст : электронный. – URL: https://english.www.gov.cn/archive/white_paper/2015/05/27/content_281475115610833.htm (дата обращения: 17.05.2025).

71. Council Decision (CFSP) 2022/1909 of 6 October 2022 amending Decision 2014/512/CFSP concerning restrictive measures in view of Russia’s actions destabilising the situation in Ukraine ST/12823/2022/INIT – An official

website of the European Union. – Текст : электронный. – URL: https://eur-lex.europa.eu/eli/dec/2022/1909/oj/eng (дата обращения: 17.05.2025).

72. European data strategy – An official website of the European Union. – Текст : электронный. – DOI отсутствует. – URL: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en (дата обращения: 10.10.2024).

73. Office of foreign assets control determination pursuant to section 1(a)(ii) OF EXECUTIVE ORDER 14071 Prohibition on Certain Information Technology and Software Services – U.S. department of the treasure . – Текст : электронный. – URL: https://ofac.treasury.gov/faqs/1188 (дата обращения: 14.04.2025).

74. Overview of Cybersecurity. Recommendation ITU-T X.1205. Geneva: International Telecommunication Union (ITU). – International Telecommunication Union. – Текст : электронный. – URL: https://www.itu.int/rec/T-REC-X.1205-200804-I/en (дата обращения: 17.03.2025).

75. Preventing Russian Export Control and Sanctions Evasion: Updated Guidance for Industry. – GOV.UK. – Текст : электронный. – URL: https://www.gov.uk/government/publications/preventing-russian-export-control-and-sanctions-evasion (дата обращения: 04.03.2025).

76. Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017 // Government of India Ministry of Communications. – Текст : электронный. – URL: https://dot.gov.in/sites/default/files/Suspension%20Rules.pdf (дата обращения: 13.04.2022).

77. The digital transformation strategy for Africa (2020–2030) – Africa Union. – Текст : электронный. – URL: https://au.int/en/documents/20200518/digital-transformation-strategy-africa-2020-2030 (дата обращения: 17.05.2025).

78. The information technology ACT, 2000 – Indica Code. – Текст : электронный. – URL:

https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf (дата обращения: 13.04.2022).

79. Translation: Data Security Law of the People's Republic of China (Effective Sept. 1, 2021) – Stanford University. – Текст : электронный. – DOI отсутствует. – URL: https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/ (дата обращения: 10.12.2024).

80. 国务院关于深化制造业与互联网融合发展的指导意见 – Cyberspace administration of China – Текст : электронный. – DOI отсутствует. – URL: http://www.cac.gov.cn/2016-05/20/c_1118905368.htm (дата обращения: 10.12.2024).

Диссертации

81. Бабюк, И.А. Политика стратегического развития городских территорий в условиях цифровизации : опыт Санкт-Петербурга : в 2-х томах : специальность 5.5.2. Политические институты, процессы, технологии : диссертация на соискание ученой степени кандидата политических наук / Бабюк Ирина Анатольевна ; Санкт-Петербургский государственный университет. – Санкт-Петербург, 2023. – 253 с. – Библиогр.: с. 103-117.

82. Есиев, Э.Т. Роль виртуальных технологий конфликтной мобилизации в противодействии политическому протесту : специальность 5.5.2. Политические институты, процессы, технологии : диссертация на соискание ученой степени кандидата политических наук / Есиев Эльдар Таймуразович ; Московский государственный университет имени М.В.Ломоносова. – Москва, 2023. – 179 с. – Библиогр.: с. 161-179.

83. Курилкин, А.В. Информационные и кибернетические операции как инструмент реализации внешней политики : формы, методы, технологии : специальность 23.00.04 «Политические проблемы международных отношений, глобального и регионального развития» : диссертация на соискание ученой степени кандидата политических наук / Курилкин Антон Владимирович ; Московский государственный университет имени М.В.Ломоносова. – Москва, 2021. – 207 с. – Библиогр.: с. 179-207.

84. Филимонов, И.В. Роль государства в трансформации экосистемы цифровой экономики : специальность 5.2.1. Экономическая теория : диссертация на соискание ученой степени кандидата экономических наук / Филимонов Илья Валерьевич ; Московский государственный университет имени М.В. Ломоносова. – Москва, 2024. – 217 с. – Библиогр.: с. 186-208.

85.Филиппова, В.А. Формирование политической повестки дня в современных медиасферах (на примере России и Бразилии 2010 – 2014 гг.) : специальность 10.01.10 «Журналистика» : диссертация на соискание ученой степени кандидата политических наук / Филиппова Виктория Александровна ; Санкт-Петербургский государственный университет. – Санкт-Петербург, 2016. – 204 с. – Библиогр.: с. 174-182.

Авторефераты диссертаций

86. Алагоз, А.В. Стратегии политических интернет-коммуникаций региональных органов власти и общества в Российской Федерации : специальность 5.5.2. Политические институты, процессы, технологии : автореферат диссертации на соискание ученой степени кандидата политических наук / Алагоз Алиса Владимировна ; Уральский федеральный университет имени первого Президента России Б.Н. Ельцина. – Екатеринбург, 2024. – 22 с. – Библиогр.: с. 21-22. - Место защиты: Уральский федеральный университет имени первого Президента России Б.Н. Ельцина.

87. Лихачев, Н.А. Уголовно-правовое противодействие преступлениям в сфере обеспечения информационной безопасности : законодательный, правоприменительный и доктринальный аспекты : специальность 5.1.4. «Уголовно-правовые науки (юридические науки)» : автореферат диссератции на соискание ученой степени кандидата юридических наук / Лихачев Никита Александрович ; Кубанский государственный университет. – Краснодар, 2024. – 23 с. – Библиогр.: с. 22. – Место защиты: Кубанский государственный университет.

88. Мухаметов, Д.Р. «Умное» государство : факторы формирования и направления развития : специальность 5.5.2 Политические институты, процессы, технологии : автореферат диссертации на соискание ученой степени кандидата политических наук / Мухаметов Данияр Рустямович ; Финансовый университет. – Москва, 2023. – 26 с. – Библиогр.: с. 25-26. – Место защиты: Финансовый университет.

89. Петровский, С.В. Правовое регулирование оказания интернет-услуг : специальность 12.00.03 «Гражданское право; предпринимательское право; семейное право; международное частное право» : автореферат диссертации на соискание ученой степени кандидата юридических наук / Петровский Станислав Витальевич ; Российский государственный институт Интеллектуальной собственности Роспатента. – Москва, 2002. – 27 с. – Библиогр.: с. 27. – Место защиты: Российский государственный институт интеллектуальной собственности.

Электронные ресурсы

90. 2023 Индустрия программного обеспечения в России 2023 / Искусственный интеллект Российской Федерации : официальный сайт. – Москва. – Обновляется в течение суток. – Текст : электронный. – DOI отсутствует. – URL: https://ai.gov.ru/knowledgebase/razrabotka-i-issledovaniya-v-oblasti-ii/2023_industriya_programmnogo_obespecheniya_v_rossii_2023_russoft/ (дата обращения: 01.11.2024).

91. 2024 ИТ-отрасль : ключевые показатели развития за 2019–2023 гг., НИУ ВШЭ, Минцифры / Искусственный интеллект Российской Федерации : официальный сайт. – Москва. – Обновляется в течение суток. – Текст : электронный. – DOI отсутствует. – URL: https://ai.gov.ru/knowledgebase/infrastruktura-ii/2024_it-otrasly_klyuchevye_pokazateli_razvitiya_za_2019_2023_gg_niu_vshe_mincifry/ (дата обращения: 01.11.2024).

92. 2024 Обзор российского рынка инфраструктурного ПО и перспективы его развития, Strategy Partners / Искусственный интеллект Российской Федерации : официальный сайт. – Москва. – Обновляется в течение суток. – Текст : электронный. – DOI отсутствует. – URL: https://ai.gov.ru/knowledgebase/razrabotka-i-issledovaniya-v-oblasti-ii/2024_obzor_rossiyskogo_rynka_infrastrukturnogo_po_i_perspektivy_ego_razvitiya_strategy_partners/ (дата обращения: 01.11.2024).

93. В России предложили создать программу поддержки вернувшихся IT-специалистов / Ведомости : сайт. – Москва. – Обновляется в течение суток. – Текст : электронный. – DOI отсутствует. – URL: https://www.vedomosti.ru/society/news/2023/10/05/998915-rossii-predlozhili-sozdat-programmu (дата обращения: 24.05.2024).

94. В РФ продолжают грантовую поддержку проектов обратного инжиниринга / Ростехнадзор : официальный сайт. – Москва. – Обновляется в течение суток. – Текст : электронный. – DOI отсутствует. – URL: https://www.gosnadzor.ru/news/67/9453/ (дата обращения: 11.08.2024).

95. Государственные меры поддержки для ИТ-компаний / Госуслуги : официальный сайт. – Москва. – Обновляется в течение суток. – Текст : электронный. – DOI отсутствует. – URL: https://www.gosuslugi.ru/itindustry (дата обращения: 30.10.2024).

96. За два года на IT-специальности было зачислено 350 тыс. студентов / RSpectr : сайт. – Москва. – Обновляется в течение суток. – Текст : электронный. – DOI отсутствует. – URL: https://rspectr.com/novosti/s-2021-goda-na-it-speczialnosti-bylo-zachisleno-pochti-350-tys-rossijskih-studentov (дата обращения: 22.02.2024).

97. Зарплата ИТ-специалистов в два раза выше средней по экономике / Минцифры : официальный сайт. – Обновляется в течение суток. – Текст : электронный. – DOI отсутствует. – URL: https://digital.gov.ru/news/zarplata-it-speczialistov-v-dva-raza-vyshe-srednej-po-ekonomike (дата обращения: 12.10.2024).

98. ИТ-ипотеку оформили почти 40 тыс. человек / Минцифры : официальный сайт. – Москва. – Обновляется в течение суток. – Текст : электронный. – DOI отсутствует. – URL: https://digital.gov.ru/news/it-ipoteku-oformili-pochti-40-tys-chelovek (дата обращения: 12.12.2023).

99. ИТ-образование / Минцифры : официальный сайт. – Москва. – Обновляется в течение суток. – Текст : электронный. – DOI отсутствует. – URL: https://digital.gov.ru/activity/it-obrazovanie (дата обращения: 16.03.2025).

100. ИТ-отрасль заняла 1 место по темпам роста ключевых показателей за 4 года среди всех крупных отраслей экономики / Минцифры : официальный сайт. – Москва. – Обновляется в течение суток. – Текст : электронный. – DOI отсутствует. – URL: https://digital.gov.ru/news/it-otrasl-zanyala-1-mesto-po-tempam-rosta-klyuchevyh-pokazatelej-za-4-goda-sredi-vseh-krupnyh-otraslej-ekonomiki (дата обращения: 01.11.2024).

101. Каждый десятый выпускник вуза получил ИТ-специальность / Минцифры : официальный сайт. – Москва. – Обновляется в течение суток. – Текст : электронный. – DOI отсутствует. – URL: https://digital.gov.ru/news/kazhdyj-desyatyj-vypusknik-vuza-poluchil-it-speczialnost (дата обращения: 26.10.2024).

102. Кодеры самозанялись / Коммерсантъ : сайт. – Обновляется в течение суток. – Текст : электронный. – DOI отсутствует. – URL: https://www.kommersant.ru/doc/6693658 (дата обращения: 12.06.2024).

103. Минобрнауки России подвело итоги распределения бюджетных мест вузам и научным организациям на 2023-2024 учебный год / Минобрнауки России : официальный сайт. – Москва. – Обновляется в течение суток. – Текст : электронный. – DOI отсутствует. – URL: https://minobrnauki.gov.ru/press-center/news/novosti-ministerstva/50956/ (дата обращения: 26.10.2024).

104. Оценка численности ИТ-кадров и кадровой потребности в ИТ-специалистах до 2030 года (по итогам исследования АПКИТ) / АПКИТ : официальный сайт. – Москва. – Обновляется в течение суток. – Текст :

электронный. – DOI отсутствует. – URL: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.apkit.ru/files/2024_APKIT_IT_human%20resource_2030.pdf (дата обращения: 26.10.2024).

105. Перспективы ИТ-рынка 2024 / МТС Web Services : сайт. – Москва. – Обновляется в течение суток. – Текст : электронный. – DOI отсутствует. – URL: https://mws.ru/research/it-market-perspectives/?utm_source=organic_yandex (дата обращения: 03.03.2025).

106. Пленарное заседание Петербургского международного экономического форума / Официальный сайт Президента России : официальный сайт. – Москва. – Обновляется в течение суток. – Текст : электронный. – DOI отсутствует. – URL: http://www.kremlin.ru/events/president/transcripts/74234 (дата обращения: 01.07.2024).

107. Победителей Международной олимпиады по информатике пригласили на Конгресс молодых ученых в Сочи / Минобрнауки России : официальный сайт. – Москва. – Обновляется в течение суток. – Текст : электронный. – DOI отсутствует. – URL: https://minobrnauki.gov.ru/press-center/news/nauka-i-obrazovanie/72737/?sphrase_id=8581045 (дата обращения: 13.03.2024).

108. Предметные рейтинги вузов: информационные технологии (2024 год) / Сайт рейтинговой группы Raex : сайт. – Москва. – Обновляется в течение суток. – Текст : электронный. – DOI отсутствует. – URL: https://raex-rr.com/education/subject_ranking/Information_Technology/2024/ (дата обращения: 28.10.2024).

109. Предметные рейтинги: информационные технологии, 2023 год / Сайт рейтинговой группы Raex : сайт. – Москва. – Обновляется в течение суток. – Текст : электронный. – DOI отсутствует. – URL: https://raex-rr.com/education/subject_ranking/Information_Technology/2023/?ysclid=m2t1k57vyx71024767 (дата обращения: 28.10.2024).

110. Рейтинг вузов / Альянс в сфере искусственного интеллекта : сайт. – Москва. – Обновляется в течение суток. – Текст : электронный. – DOI отсутствует. – URL: https://rating.a-ai.ru/#rating (дата обращения: 26.10.2023).

111. Рейтинг университетов РУССОФТ: 50 самых значимых учебных заведений для софтверной индустрии в 2023 году / Руссофт : сайт. – Москва. – Обновляется в течение суток. – Текст : электронный. – DOI отсутствует. – URL: https://russoft.org/news/rejting-universitetov-russoft-50-samyh-znachimyh-uchebnyh-zavedenij-dlya-softvernoj-industrii-v-2023-godu/ (дата обращения: 02.03.2024).

112. Российский IT-рынок до СВО и после – переосмысление реальности / Digital Russia : сайт. – Москва. – Обновляется в течение суток. – Текст : электронный. – DOI отсутствует. – URL: https://d-russia.ru/rossijskij-it-rynok-do-svo-i-posle-pereosmyslenie-realnosti.html (дата обращения: 12.07.2024).

113. РУССОФТ : отъезд разработчиков ПО из России в 2023 году перестал быть серьезной проблемой для индустрии / IT Channel News : сайт. – Москва. – Обновляется в течение суток. – Текст : электронный. – DOI отсутствует. – URL: https://www.novostiitkanala.ru/news/detail.php?ID=178733 (дата обращения: 24.05.2024).

114. Рынок вакансий для IT-специалистов 2023 / Технократия : сайт. – Москва. – Обновляется в течение суток. – Текст : электронный. – DOI отсутствует. – URL: https://technokratos.com/blog/18 (дата обращения: 05.02.2024).

115. Рынок ИТ-оборудования в России / Центр экономики рынков : сайт. – Москва. – Обновляется в течение суток. – Текст : электронный. – DOI отсутствует. – URL: https://research-center.ru/rynok-it-oborudovanija-v-rossii/ (дата обращения: 02.02.2024).

116. Сенаторы предлагают разработать платформу «ПВА : Предприятие–Вуз–Абитуриент» / СенатИнформ : сайт. – Москва. – Обновляется в течение суток. – Текст : электронный. – DOI отсутствует. –

URL: https://senatinform.ru/news/senatory_predlagayut_razrabotat_platformu_pva_predpriyatie_vuz_abiturient/ (дата обращения: 12.12.2023).

117. Совещание с членами Правительства 16 августа 2023 года / Официальный сайт Президента России. – Москва. – Обновляется в течение суток. – Текст : электронный. – DOI отсутствует. – URL: http://kremlin.ru/events/president/news/72050 (дата обращения: 05.02.2024).

118. Статистика оттока ИТ-специалистов из России в 2022 году / Инклиент : сайт. – Сургут. – Обновляется в течение суток. – Текст : электронный. – DOI отсутствует. – URL: https://inclient.ru/outflow-it-specialists/ (дата обращения: 11.07.2024).

119. Хроника заседания Государственной Думы 20 декабря 2022 года Заседание № 87 / Государственная Дума : официальный сайт. – Москва. – Обновляется в течение суток. – Текст : электронный. – DOI отсутствует. – URL: http://api.duma.gov.ru/api/transcriptFull/2022-12-20# (дата обращения: 26.10.2024).

120. Цифровые мозги в дефиците. IT-отрасль остро нуждается в кадрах / Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации : официальный сайт : официальный сайт. – Москва. – Обновляется в течение суток. – Текст : электронный. – DOI отсутствует. – URL: https://digital.gov.ru/ru/events/41208/ (дата обращения: 05.04.2024).

121. Эффективное обеспечение киберстабильности / The Hague Centre for Strategic Studies : сайт. – Hague – Обновляется в течение суток. – Текст : электронный. – DOI отсутствует. – URL: https://hcss.nl/wp-content/uploads/2022/08/GCSC-Advancing-Cyberstability_RU.pdf (дата обращения 05.04.2023).

122. TAdviser : объем ИТ-рынка России за 2022 год и прогноз на 2023 год / Cinimex : сайт. – Москва – Обновляется в течение суток. – Текст : электронный. – DOI отсутствует. – URL: https://www.cinimex.ru/press-

center/news/tadviser-obem-it-rynka-rossii-za-2022-god-i-prognoz-na-2023-god/ (дата обращения: 21.07.2023).

123. A European strategy for data : официальный сайт. – European Union. – Обновляется в течение суток. – URL: https://digital-strategy.ec.europa.eu/en/policies/strategy-data (дата обращения: 10.13.2024). – Текст : электронный.

124.Australia Country Commercial Guide / Official Website of the International Trade Administration of United States : официальный сайт. – Washington. – Обновляется в течение суток. – Текст : электронный. – DOI отсутствует. – URL: https://www.trade.gov/country-commercial-guides/australia-digital-economy (дата обращения: 10.12.2024).

125. Austrelian signals directorate : официальный сайт. – Канберра – Обновляется в течение суток. – URL: https://www.cyber.gov.au/about-us (дата обращения: 10.12.2024). – Текст : электронный.

126. Certified Strategic data centres double / innovationaus.com : сайт. – Обновляется в течение суток. – Текст : электронный. – DOI отсутствует. – URL: https://www.innovationaus.com/certified-strategic-data-centres-double/ (дата обращения: 10.12.2024).

127. Countries with the highest number of internet users as of February 2022 / STATISTA : сайт. – New York. – Текст : электронный. – DOI отсутствует. – URL: https://www.statista.com/statistics/262966/number-of-internet-users-in-selected-countries/ (дата обращения: 09.04.2024).

128. Cybersecurity Laws and Regulations Australia 2025 / ICLG : сайт. – Текст : электронный. – DOI отсутствует. – URL: https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/australia (дата обращения: 10.12.2024).

129. Cyberspace / Britannica : сайт. – London. – Текст : электронный. – DOI отсутствует. – URL: https://www.britannica.com/topic/cyberspace (дата обращения: 07.04.2023).

130. Defining a framework for decision-making in cyberspace / JSTOR : сайт. – New York. – Текст: электронный. – DOI отсутствует. – URL: https://www.jstor.org/stable/pdf/resrep11980.5.pdf (дата обращения: 07.05.2023).

131. Digital sovereignty for Europe / European Parliament : официальный сайт. – European Union. – Текст : электронный. – DOI отсутствует. – URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf (дата обращения: 10.06.2024).

132. DNS servers in Russian Federation / Public DNS Server List : сайт. – Bremen. – Обновляется в течение суток. – Текст : электронный. – DOI отсутствует. – URL: https://public-dns.infoву/nameserver/ru.html (дата обращения: 02.01.2024).

133. EUR-Lex Access to European Union Law : официальный сайт. – European Union. – Обновляется в течение суток. – URL: https://eur-lex.europa.eu/eli/dec/2022/1909/oj (дата обращения: 05.05.2024). – Текст : электронный.

134. General data protection regulation (GDPR) / European Union : официальный сайт. – European Union. – Текст: электронный. – DOI отсутствует. – URL: https://eur-lex.europa.eu/EN/legal-content/summary/general-data-protection-regulation-gdpr.html (дата обращения: 10.06.2024).

135. Germany’s Presidency of the Council of the European Union / eu2020.de : сайт. – European Union. – Текст : электронный. – DOI отсутствует. – URL: https://www.eu2020.de/eu2020-en (дата обращения: 10.03.2025).

136. Imposing Additional Sanctions on Those Supporting Russia’s War Against Ukraine / U.S. department of state : официальный сайт – Washington. – Обновляется в течение суток. – Текст : электронный. – DOI отсутствует. – URL: https://www.state.gov/imposing-additional-sanctions-on-those-supporting-russias-war-against-ukraine/ (дата обращения: 01.11.2024).

137. India's Shutdown Numbers : официальный сайт. – New Delhi India. – Обновляется в течение суток. – URL: https://internetshutdowns.in/ (дата обращения: 17.04.2022). – Текст : электронный.

138. NATO Glossary of Terms and Definitions AAP-06 Edition 2018 / NATO Standardization Office : официальный сайт. – Brussels. – Обновляется в течение суток. – Текст : электронный. – DOI отсутствует. – URL: nso.nato.int/nso/ZPUBLIC/_BRANCHINFO/TERMINOLOGY_PUBLIC/NON-CLASSIFIED%20NATO%20GLOSSARIES/AAP-6.PDF (Дата обращения: 07.04.2023).

139. New Conditions and Constellations in Cyber / The Hague Centre for Strategic Studies : сайт. – Hague. – Обновляется в течение суток. – Текст: электронный. – DOI отсутствует. – URL: https://hcss.nl/wp-content/uploads/2021/12/Cyberstability-Paper-Series.pdf (дата обращения: 07.05.2023).

140. Over 1,000 Companies Have Curtailed Operations in Russia–But Some Remain / Yale school of management : сайт. – New Haven. – Обновляется в течение суток. – Текст: электронный. – DOI отсутствует. – URL: https://som.yale.edu/story/2022/over-1000-companies-have-curtailed-operations-russia-some-remain (дата обращения: 25.11.2023).

141. Russia’s Quest for Digital Sovereignty / Deutsche Gesellschaft für Auswärtige Politik : сайт. – Berlin. – Обновляется в течение суток. – Текст : электронный. – DOI отсутствует. – URL: https://dgap.org/en/research/publications/russias-quest-digital-sovereignty (дата обращения: 10.06.2024).

142. Russian Federation IP Address Ranges / IP2Location : сайт. – George Town. – Обновляется в течение суток. – Текст: электронный. – DOI отсутствует. – URL: https://lite.ip2location.com/russian-federation-ip-address-ranges (дата обращения: 01.01.2024).

143. The Telecom Regulatory Authority of India : официальный сайт. – New Delhi. – Обновляется в течение суток. – URL: https://trai.gov.in/about-us/history (дата обращения: 12.04.2024). – Текст: электронный.

Статьи

144. Алейников, А.В. Анализ генезиса бизнеса в России : проблемное поле / А.В. Алейников // Власть. – 2009. – № 12. – С. 9-14. – ISSN 2071-5358.

145. Аннаева, М. Основные статистические методы и их применение / М. Аннаева, А. Мередов // Вестник науки. – 2023. – № 10 (67). – С. 16-19. – ISSN 2712-8849.

146. Артамонов, В.А. Гибридные войны : новые вызовы XXI века / В.А. Артамонов, Е.В. Артамонова // Большая Евразия : развитие, безопасность, сотрудничество. – 2023. – № 6-1. – С. 43-51. – ISBN 978-5-248-01064-6.

147. Ахременко, А.С. Количественный анализ политической динамики : статистический и детерминистский подходы / А.С. Ахременко // Вестник Московского университета. Серия 12. Политические науки. – 2009. – № 4. – С. 3-17. – ISSN 0868-4871.

148. Бахлов, И.В. Практика разработки комплексного прикладного политологического исследования (на примере темы «Политические механизмы территориального управления в современной России») / И.В. Бахлов, И.Г. Напалкова // ИТС. – 2011. – № 3. – С. 14-20. – ISSN 2308-1058.

149. Бессонова, О.Э. Контрактный раздаток и солидаризм - новая веха российской матрицы / О.Э. Бессонова // Мир России. Социология. Этнология. – 2019. – № 1. – С. 7-31. – ISSN 1811-0398.

150. Бессонова, О.Э. Раздаточная экономика как российская традиция / О.Э. Бессонова // Хрестоматия по россиеведению. – 2015. – № 1. – С. 59-64. – ISBN 978-5-248-00798-1.

151. Бровко, В.Ю. Особенности реализации информационного суверенитета государства в условиях нарастания гибридного противоборства / В.Ю. Бровко, Л.Н. Гарас // Вестник Московского университета. Серия 12. Политические науки. – 2021. – № 1. – С. 14-32. – ISSN 0868-4871.

152. Бродовская, Е.В. Совершенствование профилактики усиления социального недовольства в субъектах Российской Федерации / Е.В. Бродовская // Власть. – 2022. № 6. – С. 30-35. – ISSN 2071-5358.

153. Верхова, Г.В. Многоагентный подход к формированию единой геоинформационной среды / Г. В. Верхова, С.В. Акимов // Международная конференция по мягким вычислениям и измерениям. – 2021. – Том 1. – С. 286-289. – ISBN 978-5-7629-2864-9.

154. Вихман, В.В. «Цифровые двойники» в образовании : перспективы и реальность / В.В. Вихман, М.В. Ромм // Высшее образование в России. – 2021. – № 2. – С. 22-32. – ISSN 2072-0459.

155. Володенков, С.В. Влияние технологий интернет-коммуникаций на современные общественнополитические процессы : сценарии, вызовы и акторы / С.В. Володенков // Мониторинг. – 2019. – № 5 (153). – С. 341-363. – ISSN 2219-5467.

156. Володенков, С.В. Новые формы политического управления в киберпространстве XXI века : вызовы и угрозы / С.В. Володенков // Известия Саратовского университета. Новая серия. Серия Социология. Политология. – 2011. – № 2. – С.78-85. – ISSN 1818-9601.

157. Володенков, С.В. Развитие современных информационно-коммуникационных технологий как фактор формирования парадигмы общества сетевых коммуникаций / С.В. Володенков // Вестник Московского университета. Серия 12. Политические науки. – 2016. – № 2. – С. 21-34. – ISSN 0868-4871.

158. Володенков, С.В. Роль трансфера технологий в рамках геополитической стратегии России в многополярном мире / С.В. Володенков, Е.А. Кашин, С.К. Крайнов // Известия ТулГУ. Гуманитарные науки. – 2024. – № 4. – С. 49-63. – ISSN 2071-6141.

159. Володенков, С.В. Сетевые информационные войны в современных условиях : основные акторы и стратегии / С.В. Володенков, В.В. Митева // PolitBook. – 2016. – № 3. – С. 18-35 – ISSN 2307-4590.

160. Володенков, С.В. Цифровизация современного пространства общественно-политических коммуникаций : научные концепции, модели и сценарии / С.В. Володенков, С.Н. Федорченко // Вестник Томского государственного университета. Философия. Социология. Политология. – 2021. – № 60. – С. 175-193. – ISSN 2311-2395.

161. Гаджиев, Х.А. Цифровое пространство как поле политического противостояния власти и оппозиции / Х.А. Гаджиев // Политическая Наука. – 2020. – № 3. – С.147-171. – ISSN 1998-1775.

162. Гирич, В.Л. Глобальное информационное пространство и проблема доступа к мировым информационным ресурсам / В.Л. Гирич, В.Н. Чуприна. // Национальная библиотека Украины имени В.И. Вернадского. – 2007. – С. 7 – ISSN отсутствует. – DOI отсутствует. – URL: https://web.archive.org/web/20240727035549/http:/olden.rsl.ru/upload/mba2007/mba2007_05.pdf (дата обращения: 10.10.2025).

163.Данельян, А.А. Международно-правовое регулирование киберпространства / А.А. Данельян // Образование и право. – 2020. – № 1. – С. 261-269. – ISSN 2076-1503.

164. Даниленков, А.В. Государственный суверенитет Российской Федерации в информационно-телекоммуникационной сети «Интернет» / А.В. Даниленков // Lex Russica. – 2017. – № 7 (128). – С. 154-165 – ISSN 1729-5920.

165. Добровольская, И.А. Понятие «Информационное пространство» : различные подходы к его изучению и особенности / И.А. Добровольская // Вестник РУДН. Серия : Литературоведение, журналистика. – 2014. – № 4. – С. 140-147. – ISSN 2312-9247.

166. Домбровская, А.Ю. Гражданская и политическая активность в цифровой среде : установки современных молодых россиян. / А.Ю. Домбровская // Россия : общество, политика, история. – 2023. – № 2 (7). – С. 114-131. – ISSN 2949-1142.

167. Жемчугов, А.М. Цель как основа стратегии / А.М. Жемчугов, М.К. Жемчугов // Проблемы экономики и менеджмента. – 2014. – № 8 (36). – С. 9-17. – ISSN 2223-5213.

168. Захарченко, Р.И. Методика оценки устойчивости функционирования объектов критической информационной инфраструктуры, функционирующей в киберпространстве / Р.И. Захарченко, И.Д. Королев // Наукоемкие технологии в космических исследованиях Земли. – 2018. – № 2. – С. 52-61. – ISSN 2412-1363.

169. Зиновьева, Е.С. Цифровой суверенитет европейского союза / Е.С. Зиновьева // Современная Европа. – 2021. – № 2. – С. 40-49. – ISSN 0201-7083.

170. Зудин, А.Ю. Неокорпоративизм в России? Государство и бизнес при Владимире Путине / А.Ю. Зудин // Pro et Contra. – Москва. – 2001. – № 4. Том 6. – С. 171-198. – ISSN 1560-8913.

171. Иванов, В.В. Технологический суверенитет как фактор стратегического развития / В.В. Иванов // Проектирование будущего. Проблемы цифровой реальности : труды 7-й Международной конференции (15-17 февраля 2024 г., Москва). – Москва : ИПМ имени М.В. Келдыша. – 2024. – С. 33-37. – ISBN 978-5-98354-073-6.

172. Иванова, К.А. Понятие киберпространства в международном праве / К.А. Иванова, М.Ж. Мылтыкбаев, Д.Д. Штодина // Правоприменение. – 2022. – № 4. – С. 32-44. – ISSN 2542-1514.

173. Игнатова, И.В. Предпринимательство и бизнес : терминологическая дифференциация / И.В. Игнатова // Вестник евразийской науки. – 2014. – № 6 (25). – С. 10 – ISSN 2588-0101.

174. Ирхин, Ю.В. Институционализм и неоинституционализм : направления и возможности анализа / Ю.В. Ирхин // Социально-гуманитарные знания. – 2012. – № 1. – С. 58-77. – ISSN 0869-8120.

175. Капустин, А.Я. Суверенитет государства в киберпространстве : международно-правовое измерение / А.Я. Капустин // Журнал зарубежного

законодательства и сравнительного правоведения. – 2022. – № 6. – С. 99-108. – ISSN 1991-3222.

176. Клейнер, Г.Б. Системная парадигма как теоретическая основа стратегического управления экономикой в современных условиях / Г.Б. Клейнер // Управленческие науки. – 2023. – № 1. – С. 6-19. – ISSN 2304-022X.

177. 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.

178. 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.

179. 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.

180. Ковригин, Д.Э. Российский IT-рынок в условиях санкционного давления Запада / Д.Э. Ковригин // Гуманитарные науки. Вестник Финансового университета. – 2024. – № 2. – 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).

181. 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).

182. Красиков, Д.В. Территориальный суверенитет и делимитация юрисдикций в киберпространстве / Д.В. Красиков // Государство и право в новой информационной реальности. – 2018. – № 1. – С. 99-111. – ISBN 978-5-248-00888-9.

183. Кроуч, К. Корпоративизм / К. Кроуч // Управление человеческими ресурсами / под редакцией М. Пула, М. Уорнера. – Санкт-Петербург : Питер. – 2002. – С. 923-934. – ISBN 5-318-00127-0.

184. Кутюр, С. Что означает понятие «суверенитет» в цифровом мире? / С. Кутюр, С. Тоупин // Вестник международных организаций. – 2020. – № 4. Том 15.– С. 48-69. – ISSN 1996-7845.

185. Любаненко, А.В. Формализация матричных методов в SWOT-анализе / А.В. Любаненко, В.Р. Цибульский // ВК. – 2004. – № 3. – С. 86-92. – ISSN 1999-7604.

186. Максуров, А.А. О методологических основах правового регулирования интернет-отношений / А.А. Максуров // Законодательство и экономика. – 2012. – № 2. – С. 59-61. – ISSN 0869-1983.

187. Манойло, А.В. Российский подход к формированию пространства коллективной информационной безопасности стран / А.В. Манойло // БРИКС Социальные и гуманитарные знания. – 2018. – № 3 (15). Том 4.– С. 156-163. – ISSN 2412-6519.

188. Манойло, А.В. Современные стратегии кибербезопасности и кибероборонь НАТО / А.В. Манойло // АПЕ. – 2020. – № 3. – С. 160-184. – ISSN 0235-5620.

189. Матвеев, А.А. Прошлое, настоящее и будущее неоинституционального подхода в политической науке / А.А. Матвеев // Управленческое консультирование. – 2021. – № 5. – С. 45-62. – ISSN 1816-8590.

190. Мигулева, М.В. Киберпространство как социальный институт : признаки, функции, характеристики / М.В. Мигулева // Дискурс-Пи. – 2020. – № 4 (41). – С. 199-212. – ISSN 1817-9568.

191. Минбалеев, А.В. Правовое обеспечение кибербезопасности во Вьетнаме / А.В. Минбалеев // Вестник УрФО. – 2019. – № 1 (31) – С. 64-68. – ISSN 2225-5435.

192. Наумов, В.Б. Общие вызовы права и государственного управления в цифровую эпоху / В.Б. Наумов // Ленинградский юридический журнал. – 2019. – № 1 (55). – С. 43-56. – ISSN 1813-6230.

193. Никипорец-Такигава, Г.Ю. Методологические проблемы формирования концепции национальной кибербезопасности Российской Федерации / Г.Ю. Никипорец-Такигава // Гуманитарные науки. Вестник Финансового университета. – 2022. – № 12 (1). – С. 70-74. – ISSN 2226-7867.

194. О'Доннелл, Г. Делегативная демократия / Г. О'Доннелл // Пределы власти. – 1994. – № 2-3. – С. 47-69. – ISBN отсутствует.

195. Островский, А.В. Стратегия интеллектуальной собственности Китая / А.В. Островский // Правовая информатика. – 2015. – № 1. – С. 49-56. – ISSN 1994-1404.

196. Павроз, А.В. Группы интересов в системе политического представительства : современные тенденции / А.В. Павроз // ПОЛИТЭКС. – 2013. – № 3. – С. 265-271. – ISSN 2618-9577.

197. Павроз, А.В. Неоконсервативная концепция сильного государства как новая модель социально-политического взаимодействия / А.В. Павроз // Политика и общество. – 2010. – № 3. – С. 21-27. – ISSN 1812-8696.

198. Парма, Р.В. Политическая мобилизация протестных настроений в России и Беларуси на цифровых медиа-платформах / Р.В. Парма // Известия ТулГУ. Гуманитарные науки. – 2023. – № 1. – С. 46-57 – ISSN 2071-6141.

199. Перегудов, С.П. Неокорпоративизм и парламентская демократия / С.П. Перегудов // Советское государство и право, Москва. – 1980. – № 3. – С. 91-99. – ISBN отсутствует.

200. Першин, Ю.Ю. Записки о «гибридной войне» / Ю.Ю. Першин // Вопросы безопасности. – 2016. – № 4. – С. 63-85. – ISSN 2409-7543.

201. Печников, А.А. Размышления о вебометрическом рейтинге / А.А. Печников // Научная периодика : проблемы и решения. – 2014. – № 1 (19). – С. 17-21. – ISSN 2409-4714.

202. Питерс, Г. Политические институты : вчера и сегодня. – Политическая наука : новые направления / Г. Питерс ; перевод М.М. Гурвица, А.Л. Демчука, Т.В. Якушевой // Москва : Вече. – 1999. – С. 218-231. – ISBN 5-7838-0441-X.

203. Радченко, Т.В. Правовые аспекты определения границ киберпространства / Т.В. Радченко, К.В. Шевелева // Вестник экономики, управления и права. – 2024. – № 3. – С. 62-68. – ISSN 2072-0033.

204. Расторгуев, С.В. Концептуализация взаимоотношений акторов политической и экономической сфер / С.В. Расторгуев // Власть. – 2016. – № 7. – С. 16-21 – ISSN 2071-5358.

205. Расторгуев, С.В. Ресурсно-акторный анализ в политических исследованиях / С.В. Расторгуев // Гуманитарные науки. Вестник Финансового университета. – 2022. – № 2. – С. 45-52 – ISSN 2226-7867.

206. Розин, В.М. Интернет – новая информационная технология, семиозис, виртуальная среда / В.М. Розин // Влияние Интернета на сознание и структуру знания. Москва : Институт философии РАН. – 2004. – С. 3-23. – ISBN 5-201-02111-5.

207. Сидорова, А.П. Понятие цифрового пространства и его характеристики. Возможности и угрозы использования цифрового пространства / А.П. Сидорова // Научный диалог : молодой ученый : сборник научных трудов по материалам XXVIII междунарой научной конференции. – Санкт-Петербург. Международная Объединенная Академия Наук. – 2020. – С. 48-55. – ISBN 001-000001-0613-YS.

208. Стародубцев, Ю.И. Структурно-функциональная модель киберпространства / Ю.И. Стародубцев, П.В. Закалкин, С.А. Иванов // Вопросы кибербезопасности. – 2021. – № 4 (44). – С. 16-24 – ISSN 2311-3456.

209. Стрельцов, А. Суверенитет и юрисдикция государства в среде информационно-коммуникационных технологий в контексте международной безопасности / А. Стрельцов // Международная жизнь. – 2017. – № 2. – С.87-106. – ISSN 0130-9625.

210. Терентьева, Л.В. Понятие киберпространства и очерчивание его территориальных контуров / Л.В. Терентьева // Правовая информатика. – 2018. – № 4. – С. 66-71. – ISSN 1994-1404.

211. Ушкин, С.Г. Теоретико-методологические подходы к изучению сетевой протестной активности : от «умной толпы» к «слактивизму» / С.Г. Ушкин // Мониторинг общественного мнения : экономические и социальные перемены. – 2015. – № 3. – С. 3-12. – ISSN 2219-5467.

212. Фельдман, П.Я Информационно-коммуникационные технологии в реализации внешнеполитической стратегии США / П.Я Фельдман // Русская политология. – 2016. – № 1. – ISSN 2541-965X.

213. Флигстин, Н. Теория полей / Н. Флигстин, Д. Макадам // Экономическая социология. – 2022. – № 1. – С. 60-100 – ISSN 1726-3247.

214. Хайкин, М.М. Проблемы устойчивого развития экономических систем (На примере Ямало-Ненецкого автономного округа) / М.М. Хайкин, А.Е. Пахомова // Вестник Алтайской академии экономики и права. – 2024. – № 5-2. – С. 326-335. – ISSN 1818-4057.

215. Хуторной, С.Н. Киберпространство и реальный мир / С.Н. Хуторной // Вестник Московского государственного областного университета. Серия Философские науки. – 2011. – № 2. – С. 67-71. – ISSN 2072-8530.

216. Цветкова, Н.Н. Развитие сектора ит-услуг в Индии и стратегия «цифровая Индия» / Н.Н. Цветкова // Восточная аналитика. – 2021. – № 4. – С. 43-61. – ISSN 2227-5568.

217. Шабров, О.Ф. Модернизация в эпоху постмодерна / О.Ф. Шабров // Власть. – 2017. – № 11 (25). – С. 13-21. – ISSN 2071-5358.

218. Шабров, О.Ф. Управление и самоорганизация как факторы стабильности и развития / О.Ф. Шабров // Эффективные технологии в системе государственного и муниципального управления. – Майкоп, Ростов-на-Дону : Издательство СКАГС. – 1999. – С. 180-194. – ISBN 5-8954-6028-3.

219. Шапорто, Т.В. Интернет-политика Китая как залог политической стабильности / Т.В. Шапорто, А.Ю. Мохорова // Россия в глобальном мире. – 2021. – № 18 (41). – С. 135-142. – ISSN 2304-9472.

220. Шиманская, А. Теоретические подходы к исследованию понятия цифрового пространства / А. Шиманская // Банковский вестник. – 2023. – № 2 (715). – С. 36-42. – ISSN 2071-8896.

221. Шмиттер, Ф. Неокорпоратизм / Ф. Шмиттер // Полис. Политические исследования. – 1997. – № 2. – С. 14-22. – ISSN 1684-0070.

222. Ясин, Е. Бремя государства и экономическая политика / Е. Ясин // Вопросы экономики. – 2002. – № 11. – С. 4-30. – ISSN 0042-8736.

223. Almond, G.A. A Developmental Approach to Political Systems / G.A. Almond // World Politics. – 1965. – № 17 (2). – С. 183-214. – ISBN отсутствует.

224. Buchanan, J.M. The Limits of Liberty between Anarchy and Leviathan / J.M. Buchanan // Political Theory. – 1975. – № 4 (3). – P. 388-391. – ISSN 0007-1234.

225. Clark, D. Characterizing Cyberspace : Past, Present and Future / D. Clark // ECIR Working Paper. MIT Political Science Department. – 2010. № 2010-3 – P.18 – ISBN отсутствует.

226. Desforges A. Representations of Cyberspace : A Geopolitical Tool / A. Desforges // Éditions La Découverten. – 2014. – № 152-153. – P. 67-81. – ISBN 978-2-70717-898-5.

227. Eichensehr, K.E. Data extraterritoriality / K.E. Eichensehr // Texas law review. – 2017. – Volume 95. – P. 145-160. – ISSN 0040-4411.

228. Epifanova, A. Deciphering Russia's «Sovereign Internet Law» Tightening Control and Accelerating the Splinternet / A. Epifanova // DGAP ANALYSIS. – 2020. – № 2. – P. 11. – ISSN 1611-703.

229. Farris, C.D. The Political System : An Inquiry into the State of Political Science. David Easton / C.D. Farris // The Journal of Politics. – 1953. – № 15 (4). – P. 544-547. – ISSN 1468-2508.

230. Kohl, U. Jurisdiction in cyberspace / U. Kohl // Research handbook on international law and cyberspace / Edited by N. Tsagourias, R. Buchan. – Cheltenham ; Northampton : Edward Elgar publishing – 2015. – P. 33. – ISBN 978-1-7825-4739-6.

231. Lehmbruch, G. Introduction : Neo-corporatism in comparative perspective / G. Lehmbruch // Patterns of corporatist policy / Edit by Lehmruch G. Schm.il.te P.C. – London : Beverly Hills. – 1982. – P. 1-28. – ISBN 978-0-8039-9833-9.

232. March, J.G. The New Institutionalism : Organizational Factors in Political Life / J.G. March, J.P. Olsen // The American Political Science Review. – 1984. – № 3. Volume 78. – P. 734-749. – ISSN 1537-5943.

233.Mayer, M. International politics in the digital age : Power diffusion or power concentration? / M. Mayer, N. de Scalzi, L. Martino, I. Chiarugi. – Proc. 27th SISP Conf, 2013. – 64 p. – ISSN отсутствует.

234. Nash, J. Non-Cooperative Games / J. Nash // The Annals of Mathematics, Second Series. – 1951. – Issue 2. Volume 54. – P. 286-295. – ISSN 0003-486X.

235. Neuman, J. von Zur Theorie der Gesellschaftsspiele / J. von Neuman // Mathematische Annalen. – 1928. – P. 295-320. – ISSN 0025-5831.

236. Panitch, L. Recent theoretizations of corporatism : Reflections on a growth industry / L. Panitch // British Journal of Sociology, London. – 1980. – № 2. Volume 31 – P. 159-198. – ISSN 0007-1315.

237. Peregudov, S.P. Business and State Bureaucracy in Russia / S.P. Peregudov // Russian Politics & Law. – 2009. – № 47 (4). – P. 43-57. – ISSN 1061-1940.

238. Sapir, J. The Strategic Imperative and the Paradigm Shift in Economics / J. Sapir // Strategizing : Theory and Practice. – 2021. – № 1. Volume 1. – P. 1-14. – ISSN 2782-2435.

239. Shapley, L.S. method for evaluating the distribution of power in a committee system / L.S. Shapley, M. Shubik // American Political Science Review. – 1954. – № 48 – P. 787-792. – ISSN 0003-0554.

240. Streeck, W. Industrial Relations Today : Reining in Flexibility / W. Streeck // MPIFG Working Paper, № 08/3, Max Planck Institute for the Study of Societies, Cologne, 2008 – P. 21. – ISSN 1864-4333.

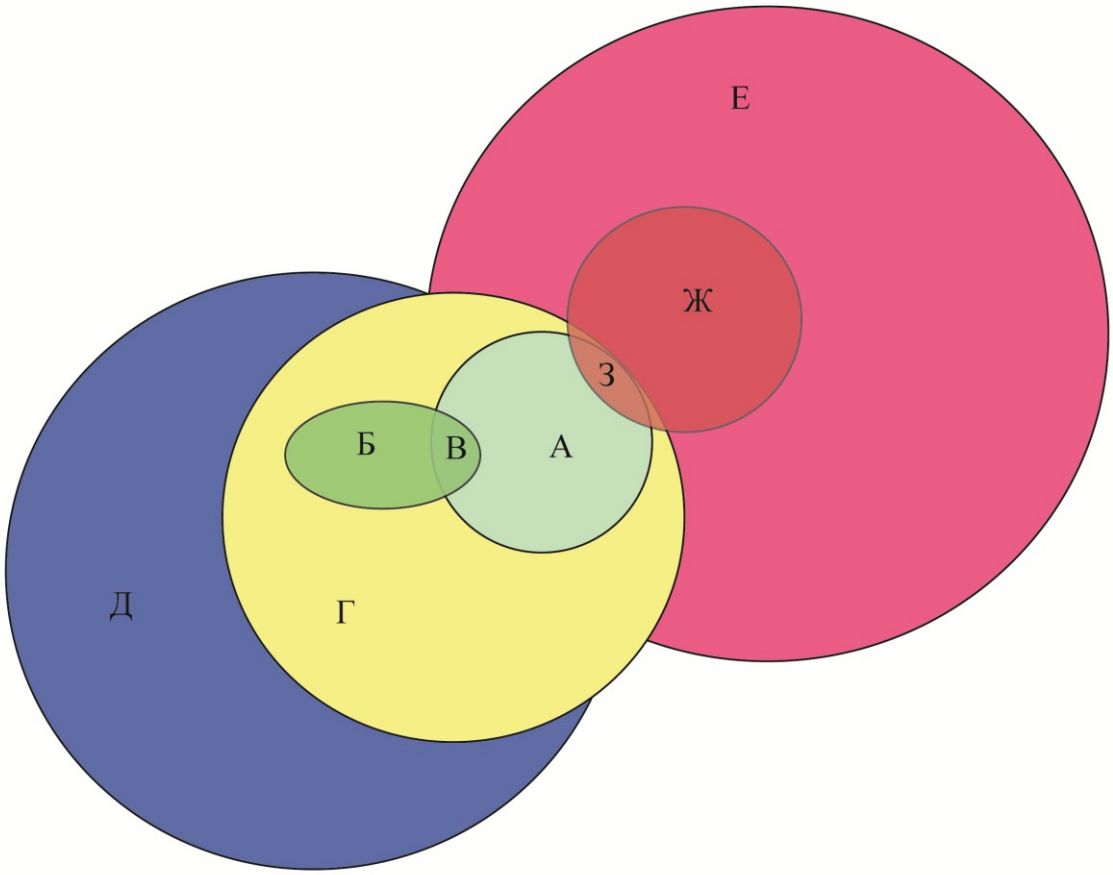
241. Talos, E. Sozialpartnerschaft und Neokorporativismustheorien / E. Talos // Österr. Z. Politikwiss., Wien. – 1982. – № 3. – P. 263-285. – ISSN 0378-5149.

242. Tsagourias, N. The legal status of cyberspace / N. Tsagourias // Research handbook on international law and cyberspace. – St. Louis : Edward Elgar publ. – 2017. – P. 13-29. – ISSN 978-1-78643-758-7.

Приложение А

(информационное)

Российский сегмент ИТ-компаний



А - Совокупность ИТ компаний, действующих на территории России;
Б - Государственные компании;
В - Государственные компании в сфере ИТ;
Г - Российская экономика;
Д - Российская сфера политического регулирования;
Е - Сфреа влияния иностранных государств;
Ж - Иностранные ИТ компании;
З - Иностранные компании действующие в российском сегменте ИТ;

Источник: составлено автором.

Рисунок А. 1 – Российский сегмент ИТ-компаний

Приложение Б

(информационное)

Финансовая деятельность крупнейших компаний ИТ-сферы 2020–2023 гг.

Таблица Б. 1 – Анализ финансовой деятельности компаний IT сферы

Полное название организации	2020 г.			2021 г.			2022 г.			2023 г.		
	Выручка, млрд руб.	Прирост выручки, процент	Уплачено налогов всего, млн руб.	Выручк, млрд руб.	Прирост выручки, процент	Уплачено налогов всего млн руб.	Выручк, млрд руб.	Прирост выручки, процент	Уплачено налогов всего млн руб.	Выручк, млрд руб.	Прирост выручки, процент	Уплачено налогов всего млн руб.
1	2	3	4	5	6	7	8	9	10	11	12	13
Государственная корпорация по содействию разработке, производству и экспорту высокотехнологичной промышленной продукции «Ростех»	-	-	-	-	-	-	-	-	-	-	-	-
Общество с ограниченной ответственностью «Ф-плюс оборудование и разработки»	-	-	-	-	-	-	-	-	-	-	-	-
Акционерное общество «Группа Телематика-один»	0,2	111,8	35,5	0,2	3,5	11,2	0,2	1,5	15,9	0,2	14,9	8,5
Общество с ограниченной ответственностью «О-си-эс-центр»	180,1	25,3	-	217,3	20,6	-	142,0	-34,6	-	119,9	-15,6	-
Публичное акционерное общество «Ростелеком»	348,3	8,9	-	350,6	0,7	-	364,8	4,1	-	407,5	11,7	-

Продолжение таблицы Б. 1

1	2	3	4	5	6	7	8	9	10	11	12	13
Общество с ограниченной ответственностью «Мтс Диджитал»	8,0	35,7	1265,0	11,9	48,9	1824,6	22,6	90,8	-	32,5	43,7	-
Общество с ограниченной ответственностью «Икс Холдинг»	31,0	46,4	23,2	24,9	-19,7	94,4	26,2	5,4	-	-	-	-
Общество с ограниченной ответственностью «Техкомпания Хуавэй»	127,7	-11,3	-	112,8	-11,7	-	82,3	-27,1	-	-	-	-
Публичное акционерное общество «Софтлайн»	48,7	18,1	-	51,7	6,1	-	35,7	-31,0	-	33,7	-5,5	-
Общество с ограниченной ответственностью «Новый Ай Ти Проект»	24,7	39,4	-	44,3	79,7	-	54,7	23,3	-	92,4	68,9	-
Общество с ограниченной ответственностью «1С»	0,2	-16,2	54,4	-	-	69,5	-	-	-	-	-	-
Акционерное общество «Лаборатория Касперского»	32,5	-4,7	-	35,4	9,0	-	36,4	2,8	-	47,7	31,0	-
Акционерное общество «Ситроникс»	4,4	48,8	651,0	5,9	31,8	735,3	11,6	98,3	998,3	15,5	33,3	900,6
Акционерное общество «Ибс Ит Услуги»	-	-98,4	0,5	-	150,0	0,7	0,7	1271,4	4,5	1,0	45,3	37,6
Акционерное общество «Инфосистемы Джет»	22,2	-10,9	-	28,9	30,5	-	25,6	-11,3	-	28,2	10,0	-
Акционерное общество «Айсиэл-Кпо Вс»	1,4	-38,7	218,7	1,2	-14,6	152,7	1,1	-8,2	97,1	1,4	25,6	155,1

Продолжение таблицы Б. 1

1	2	3	4	5	6	7	8	9	10	11	12	13
Ассоциация участников Рынка информационных технологий «Лига Цифровой Экономики»	-	299,8	-	-	12,6	-	-	-72,7	-	-	-70,2	-
Общество с ограниченной ответственностью «Рубитех»	25,0	7295,3	1189,2	18,7	-25,5	1532,9	25,2	35,0	2383,3	22,0	-12,6	2446,6
Акционерное общество «Ай-Теко»	13,0	-11,7	-	14,4	10,8	-	12,9	-10,2	-	18,2	40,2	-
Публичное акционерное общество «Газпром Автоматизация»	26,8	-42,2	-	19,5	-27,4	-	28,2	45,2	-	25,9	-8,3	-
Акционерное общество «Производственная фирма «Скб Контур»	16,5	17,0	-	18,1	10,0	-	21,7	19,5	-	26,9	24,0	-
Общество с ограниченной ответственностью «Монт»	24,3	31,4	-	26,5	9,1	-	25,2	-5,2	-	35,5	41,0	-
Акционерное общество «Максимателеком»	10,0	110,1	283,3	7,8	-22,8	423,8	16,7	115,0	809,0	2,8	-83,0	264,4
Общество с ограниченной ответственностью «М-инвест»	10,9	19,5	168,5	14,1	29,0	230,2	15,6	10,8	371,6	14,9	-4,8	365,9
Общество с ограниченной ответственностью «Инвента»	6,3	-13,4	148,5	17,1	169,1	255,6	21,4	25,1	378,5	12,6	-40,9	26,9
Общество с ограниченной ответственностью «Сап Снг»	35,8	0,5	-	36,7	2,5	-	16,3	-55,6	-	1,4	-91,3	-

Продолжение таблицы Б. 1

1	2	3	4	5	6	7	8	9	10	11	12	13
Общество с ограниченной ответственностью «Газпром Информ»	13,2	9,5	3516,2	12,4	-6,5	-	19,1	53,9	-	22,7	19,1	-
Общество с ограниченной ответственностью «Озон Технологии»	3,7	261,0	908,3	7,6	106,1	1354,9	18,6	145,6	3182,3	27,1	45,5	-
Общество с ограниченной ответственностью «Облачные Технологии»	3,3	1357,5	243,6	8,9	166,8	316,1	15,6	76,2	917,2	-	-	-
Общество с ограниченной ответственностью «Норникель Спутник»	9,4	8,0	2984,8	11,7	24,3	3486,4	18,5	58,0	4652,3	22,0	18,8	7722,5
Акционерное общество «Гринатом»	11,0	40,7	3381,7	13,1	18,7	4198,1	18,1	38,5	5274,6	26,3	45,1	-
Общество с ограниченной ответственностью «Газпромнефть-цифровые решения»	16,2	35,3	4256,4	15,0	-7,1	4779,0	17,8	18,6	4345,4	22,2	24,6	4584,7
Общество с ограниченной ответственностью «Безопасная Информационная Зона»	9,0	350,6	1065,1	2,8	-68,9	478,4	7,5	169,7	1557,9	-	-	-
Общество с ограниченной ответственностью «Сигма»	4,7	51,5	644,3	5,3	12,0	1040,9	4,7	-11,1	-	5,1	8,1	978,8
Общество с ограниченной ответственностью «Газинформсервис»	8,9	24,8	1736,3	10,5	17,6	2378,7	15,6	48,0	2996,8	36,0	131,4	3296,2

Продолжение таблицы Б. 1

1	2	3	4	5	6	7	8	9	10	11	12	13
Акционерное общество «Цифровые Закупочные Сервисы»	-	-	0,2	2,5	-	37,1	15,9	533,7	210,9	48,2	202,0	2529,3
Общество с ограниченной ответственностью «Стримит»	11,2	61,5	81,6	3,9	-64,9	59,5	0,3	-93,4	26,9	-	-99,5	1,7
Общество с ограниченной ответственностью «Рнт»	19,4	32,6	-	28,7	47,9	-	15,0	-47,6	-	2,2	-85,1	-
Общество с ограниченной ответственностью «Эйчпи инк»	30,6	4,8	-	42,1	37,6	-	15,0	-64,3	-	-	-	-
Акционерное общество «Позитив Текнолоджиз»	4,6	41,8	244,0	6,4	39,6	187,7	12,2	91,7	-	23,2	89,2	-
Общество с ограниченной ответственностью"Организационно-Технологические Решения 2000»	6,5	50,3	894,9	6,1	-6,4	1211,7	6,9	12,9	883,3	6,1	-11,8	1105,4
Акционерное общество «Сбербанк – Технологии»	9,4	4,2	3343,3	9,3	-1,1	1611,2	12,6	34,8	-	16,3	29,6	-
Общество с ограниченной ответственностью «Авито Тех»	-	-	-	2,8	-	241,8	12,5	342,9	2301,4	11,7	-6,5	2583,1
Общество с ограниченной ответственностью «Делл»	41,8	25,7	-	55,1	31,9	-	9,8	-82,2	-	-	-	-

Продолжение таблицы Б. 1

1	2	3	4	5	6	7	8	9	10	11	12	13
Общество с ограниченной ответственностью «Сбербанк-Сервис»	13,2	6,0	-	13,0	-1,2	-	10,4	-20,4	-	9,4	-8,9	-
Общество с ограниченной ответственностью «Эвотор Офд»	0,2	-32,9	96,3	3,8	68,3	167,7	0,7	-80,3	181,2	0,9	23,3	178,3
Общество с ограниченной ответственностью «Компания «Тензор»	7,0	12,0	526,2	9,3	32,8	536,9	10,6	13,8	462,5	13,7	29,5	701,2
Общество с ограниченной ответственностью «Лукойл-Технологии»	8,2	0,4	-	9,2	13,1	-	10,9	17,9	-	19,1	75,2	-
Общество с ограниченной ответственностью «Хиквижн»	5,6	58,5	206,4	7,6	34,7	234,5	10,9	42,6	390,1	12,7	17,5	1592,9
Общество с ограниченной ответственностью «Тинькофф Центр Разработки»	2,2	57,1	148,9	4,2	89,6	360,5	10,7	154,3	1932,7	17,9	66,7	3685,6
Общество с ограниченной ответственностью «Бюджетные и Финансовые Технологии»	2,5	69,2	364,0	3,4	36,7	341,8	7,8	130,1	1229,5	9,1	15,9	846,4
Общество с ограниченной ответственностью «Акстим»	8,0	18,7	2206,8	11,0	36,9	3188,9	10,2	-6,7	3335,8	10,7	4,8	3216,1

Продолжение таблицы Б. 1

1	2	3	4	5	6	7	8	9	10	11	12	13
Акционерное общество «Нокиа солюшнз энд нетворкс»	3,6	-3,1	1194,9	2,4	-34,0	859,4	2,2	-9,3	764,1	-	-100,0	85,0
Общество с ограниченной ответственностью «Глоубайт»	1,9	36,0	453,7	1,7	-7,5	369,7	2,3	33,2	374,0	2,3	-1,7	487,4
Общество с ограниченной ответственностью «Депо Электроникс»	5,5	6,9	353,4	5,1	-5,9	427,3	10,1	96,7	665,9	13,0	29,0	546,7
Общество с ограниченной ответственностью «Сиссофт Солюшнс»	-	-85,3	1,0	-	-	0,3	-	-	-	-	-	-
Общество с ограниченной ответственностью «Сеть дата-центров «Селектел»	3,3	43,6	341,9	4,8	44,9	592,5	8,1	67,9	1374,9	10,2	25,1	2510,0
Общество с ограниченной ответственностью «Асбис»	-	205,4	0,1	19,4	97,2	0,1	12,7	-34,7	0,1	10,9	-13,6	-
Акционерное общество «Информационные Технологии и Коммуникационные Системы»	5,4	34,8	690,0	4,7	-12,5	1066,8	5,9	23,8	-	-	-	-
Общество с ограниченной ответственностью «Технологический Центр Дойче Банка»	8,8	18,1	724,8	10,3	16,6	188,0	8,6	-16,9	186,4	2,3	-73,3	135,5

Продолжение таблицы Б. 1

1	2	3	4	5	6	7	8	9	10	11	12	13
Акционерное общество «Управляющая Компания Диасофт»	-	-	0,2	1,2	-	0,3	1,2	-3,7	0,1	2,0	67,7	0,1
Общество с ограниченной ответственностью «Оранж Бизнес Сервисез»	9,1	2,6	-	9,6	5,6	759,6	8,3	-13,1	641,1	6,6	-20,7	821,4
Общество с ограниченной ответственностью «Программный Продукт»	2,2	44,8	305,0	2,5	12,9	282,6	4,1	64,6	368,7	5,9	44,7	436,0
Акционерное общество «Нэксайн»	-	-	3123,4	-	-	1310,4	-	-	-	-	-	-
Общество с ограниченной ответственностью «Лаборатория Вс»	1,5	14,9	67,9	3,9	159,7	135,9	8,0	105,7	437,3	16,8	111,3	1322,7
Акционерное общество «Россети Цифра»	7,5	69,9	644,1	10,7	41,9	1039,3	7,9	-26,1	855,1	10,1	27,5	948,9
Общество с ограниченной ответственностью «Яндекс.Облако»	1,0	456,7	15,2	2,8	191,3	170,4	7,8	177,8	224,1	13,4	70,6	255,0
Акционерное общество «Научно-исследовательский и проектно-конструкторский институт информатизации, автоматизации и связи на железнодорожном транспорте»	6,3	-20,1	1065,0	6,8	9,4	1246,2	7,5	10,1	-	-	-	-

Продолжение таблицы Б. 1

1	2	3	4	5	6	7	8	9	10	11	12	13
Общество с ограниченной ответственностью «Магнит Ит Лаб»	-	243,6	8,1	-	40,4	8,4	0,1	87,4	9,8	0,1	87,1	22,1
Общество с ограниченной ответственностью «Тр-Линк»	6,1	48,7	352,4	6,9	12,1	416,1	7,4	8,1	511,7	10,3	38,2	1111,2
Акционерное общество «Барс Груп»	3,3	30,9	697,5	3,3	0,7	798,5	4,5	34,9	790,3	4,9	9,6	889,9
Общество с ограниченной ответственностью «Код Безопасности»	4,9	52,0	891,8	-	-	603,4	-	-	-	-	-	-
Общество с ограниченной ответственностью «Айти Солюшнс Рус»	5,3	-5,1	388,7	4,9	-8,7	195,4	4,9	-0,3	183,2	-	-	2,0
Общество с ограниченной ответственностью «Майкрософт Рус»	6,5	-5,5	1478,7	6,9	5,3	1475,8	6,4	-6,6	1715,7	0,2	-96,7	178,4
Акционерное общество научно-инженерное предприятие «Информзащита»	4,7	7,1	371,5	4,4	-7,5	275,1	4,6	4,7	297,3	4,6	0,5	253,4
Общество с ограниченной ответственностью «Ксерокс (Снг)»	12,6	-7,1	-	14,3	13,5	-	6,7	-53,4	-	4,8	-28,4	-
Общество с ограниченной ответственностью «Русбитех-Астра»	2,0	81,2	209,0	-	-	158,5	-	-	-	-	-	-

Продолжение таблицы Б. 1

1	2	3	4	5	6	7	8	9	10	11	12	13
Общество с ограниченной ответственностью «Синто»	3,2	86,0	86,3	3,4	6,6	95,7	5,3	55,8	224,1	6,1	14,9	271,7
Общество с ограниченной ответственностью «Уральский центр систем безопасности»	3,9	26,7	513,8	4,9	26,1	586,6	5,3	8,8	422,6	8,7	62,1	837,6
Общество с ограниченной ответственностью «Манго Телеком»	3,3	10,4	347,1	4,0	21,1	531,7	4,5	12,2	627,2	5,1	13,6	645,3
Общество с ограниченной ответственностью «Терралинк»	1,6	1,7	80,5	2,5	55,1	158,8	3,4	34,4	285,6	5,4	59,0	317,7
Общество с ограниченной ответственностью «Интел Текнолоджис»	1,0	10,6	106,9	1,3	26,1	124,9	0,3	-74,1	145,2	-	-	4,6
Общество с ограниченной ответственностью «Атос айти солюшенс энд сервисез»	5,0	10,5	521,1	6,7	35,2	559,0	5,3	-21,1	521,1	3,7	-30,9	449,2
Общество с ограниченной ответственностью «Транснефть-Технологии»	4,4	7,3	972,0	4,7	7,0	1052,9	6,0	26,2	-	7,0	17,3	2210,6
Общество с ограниченной ответственностью «ВК цифровые технологии»	0,8	360,7	53,6	2,2	155,6	222,3	5,0	130,6	375,2	7,9	57,8	656,4

Продолжение таблицы Б. 1

1	2	3	4	5	6	7	8	9	10	11	12	13
Общество с ограниченной ответственностью «Атол»	-	-0,9	9,2	4,9	15,4	479,7	3,9	-19,7	282,7	5,4	36,7	445,1
Акционерное общество «Рамэк-Вс»	3,9	40,1	328,5	-	-	463,2	-	-	-	-	-	-
Общество с ограниченной ответственностью «Сиско Солюшенз»	35,4	11,8	-	33,9	-4,1	-	5,1	-84,8	-	-	-	-
Общество с ограниченной ответственностью «Группа компаний «Корус Консалтинг»	2,8	-8,7	222,8	4,1	43,4	364,3	1,9	-54,1	248,5	2,6	40,4	350,9
Акционерное общество «Инлайн Груп»	6,5	6,1	450,4	4,3	-34,4	301,5	4,3	0,4	244,6	3,1	-26,8	343,2
Общество с ограниченной ответственностью «Тэк Информ»	3,7	-23,8	659,2	4,2	11,1	377,1	5,6	33,9	431,0	10,4	87,0	543,9
Общество с ограниченной ответственностью «Сибур Диджитал»	3,7	-5,8	914,7	4,4	17,9	809,6	5,6	26,1	981,7	7,4	32,2	1371,4
Акционерное общество «Универсальные технологии»	0,1	58,4	1,4	0,1	45,4	2,0	0,1	12,2	2,4	0,1	-30,4	3,1
Общество с ограниченной ответственностью «Технопром»	1,6	35,8	115,6	4,3	169,7	129,6	3,9	-9,6	148,1	3,9	1,2	283,6

Продолжение таблицы Б. 1

1	2	3	4	5	6	7	8	9	10	11	12	13
Общество с ограниченной ответственностью «Кьютэк»	2,0	-13,9	50,5	1,5	-24,1	36,7	2,0	30,5	129,2	1,9	-4,1	71,8
Общество с ограниченной ответственностью «Вентра»	1,6	38,4	562,9	1,9	15,4	709,4	3,0	58,2	957,6	3,8	29,7	1098,0
Общество с ограниченной ответственностью «Бифорком Текнолоджис»	0,5	104,3	32,2	1,1	116,8	73,3	5,2	375,1	222,3	21,0	305,9	960,2
Акционерное общество «Неофлекс Консалтинг»	2,1	38,8	442,4	3,4	61,3	664,5	4,2	26,3	811,3	2,5	-41,1	778,1
Общество с ограниченной Ответственностью «Рсхб-Интех»	1,2	37,5	420,0	3,1	167,5	770,7	5,0	61,7	580,2	7,2	43,6	416,8
Общество с ограниченной ответственностью «Деловой Офис»	4,3	20,6	123,4	5,7	32,7	256,8	4,8	-16,4	216,9	6,0	24,6	44,3

Источник: составлено автором.

Приложение В

(информационное)

Данные крупнейших компаний ИТ-сферы

Таблица В. 1 – Краткая информация о крпунейших компаниях ИТ-сферы

Полное название организации	Дата регистрации	Руководитель	Совладельцы	Размер предприятия	Колличество дочерних компаний	Колличество филиалов	Деятельность ОКВЭД Основной	Перецень санкций	Колличество государственных контрактов	Государственная поддержка
1	2	3	4	5	6	7	8	9	10	11
Государственная корпорация по содействию разработке, производству и экспорту высокотехнологичной промышленной продукции «Ростех»	23.11.2007	Чемезов Сергей Викторович	Федеральное Агентство по Управлению Государственным Имуществом, Государственная Корпорация по Содействию Разработке, Производству и Экспорту Высокотехнологичной Промышленной Продукции «Ростех»	-	145	29	64.99 Предоставление прочих финансовых услуг, кроме услуг по страхованию и пенсионному обеспечению, не включенных в другие группировки	HM Treasury (UK) OFAC (USA) NSDC (Ukraine) Special Economic and Other Restrictive Measures (Sanctions) UK sanctions list	209	-

Продолжение таблицы В. 1

1	2	3	4	5	6	7	8	9	10	11
Общество с ограниченной ответственностью «Ф-плюс оборудование и разработки»	22.12.2021	Мельников Алексей Сергеевич	Корнев Владимир Николаевич Мельников Алексей Сергеевич	-	8	-	26.20.4 Производство средств защиты информации, а также информационных и телекоммуникационных систем, защищенных с использованием средств защиты информации	-	-	Получатель поддержки как субъект МСП
Акционерное общество «Группа Телематика-один»	22.01.2015	Парамонов Леонид Сергеевич	Компания «А-Вин Консалтантс Лимитед»	Малые	2		72.19 Научные исследования и разработки в области естественных и технических наук прочие	-	75	Получает поддержку как субъект МСП
Общество с ограниченной ответственностью «О-си-эс-центр»	17.07.2003	Черненко Александр Владимирович Беневициар - Голышкин Андрей Валерьевич	Общество с Ограниченной Ответственностью «Группа Компаний О-Си-Эс»	Крупные	1	3	46.51 Торговля оптовая компьютерами, периферийными устройствами к компьютерам и программным обеспечением	-	179	-

Продолжение таблицы В. 1

1	2	3	4	5	6	7	8	9	10	11
Публичное акционерное общество «Ростелеком»	09.09.2002	Осеевский Михаил Эдуардович	Телеком Инвестиции, АО Мобител, ООО Осеевский Михаил Эдуардович Кириенко Владимир Сергеевич Рысакова Галина Васильевна Сапунов Алексей Валерьевич Костин Андрей Леонидович Меньшов Кирилл Алексеевич Анохин Сергей Николаевич Шумейко Анна Викторовна Каплунов Павел Григорьевич Устинов Антон Алексеевич Колесников Александр Вячеславович Центральный Телеграф, Пао	Крупные	31	71	61.10 Деятельность в области связи на базе проводных технологий	OFAC (USA) NSDC (Ukraine) Special Economic and Other Restrictive Measures (Sanctions)	-	-
Общество с ограниченной ответственностью «Мтс Диджитал»	11.01.2012	Воробьева Оксана Сергеевна	Мтс, Пао Стрим, ООО Телеком Проекты, ООО	Крупные	1	7	62.01 Разработка компьютерного программного обеспечения	-	-	-

Продолжение таблицы В. 1

1	2	3	4	5	6	7	8	9	10	11
Общество с ограниченной ответственностью «Икс Холдинг»	06.12.2018	Черепенников Антон Андреевич	Хк Икс, ООО Икс Менеджмент, ООО	Средние	2	-	64.20 Деятельность холдинговых компаний	OFAC (USA) NSDC (Ukraine) Special Economic and Other Restrictive Measures (Sanctions)	-	-
Общество с ограниченной ответственностью «Техкомпания Хуавэй»	15.09.2000	Лю Пэн	Huawei Technologies Coöperatief U.A.	Крупные	1	10	Торговля оптовая программным обеспечением	-	-	-
Публичное акционерное общество «Софтлайн»	09.12.2002	Разуваев Владимир Эдуардович	Общество с Ограниченной Ответственностью «Аталайя»	Крупные		26	Торговля оптовая неспециализированная	-	-	-
Общество с ограниченной ответственностью «Новый Ай Ти Проект»	20.10.2015	Ткачев Станислав Игоревич	Башлыков Александр Александрович	Крупные	1	3	46.51 Торговля оптовая компьютерами, периферийными устройствами к компьютерам и программным обеспечением	OFAC (USA) NSDC (Ukraine) Special Economic and Other Restrictive Measures (Sanctions)	62	-

Продолжение таблицы В. 1

1	2	3	4	5	6	7	8	9	10	11
Общество с ограниченной ответственностью «1С»	26.08.2010	Нуралиев Борис Георгиевич	Акционерное Общество «1с Акционерное Общество», Нуралиев Борис Георгиевич	Средние	135	-	Разработка компьютерного программного обеспечения	NSDC (Ukraine) Special Economic and Other Restrictive Measures (Sanctions)	4	-
Акционерное общество «Лаборатория Касперского»	26.06.1997	Касперский Евгений Валентинович	Головная Компания Kaspersky Labs Limited ·,Общество с Ограниченной Ответственностью «Группа Компаний Касперского», Граждане России	-	5	-	62.01 Разработка компьютерного программного обеспечения	NSDC (Ukraine) Special Economic and Other Restrictive Measur es (Sanctions)	-	-
Акционерное общество «Ситроникс»	09.12.2002	Пожидаев Николай Николаевич	Публичное Акционерное Общество «Акционерная Финансовая Корпорация «Система»	Крупные	14	-	62.01 Разработка компьютерного программного обеспечения; 63.11.9 деятельность по предоставлению услуг по размещению информации прочая	NSDC (Ukraine) Special Economic and Other Restrictive Measures (Sanctions)	-	-
Акционерное общество «Ибс Ит Услуги»	02.07.1998	Кочаров Григорий Ованесович	Общество с Ограниченной Ответственностью «Ибс Холдинг	Малые	9	-	Деятельность по управлению финансово-промышленными группами	-	-	-

Продолжение таблицы В. 1

1	2	3	4	5	6	7	8	9	10	11
Акционерное общество «Инфосистемы Джет»	25.03.1993	Иванов Геннадий Иванович, Молодых Олег Эдуардович	Пинакль, Зао Колесов Валентин Валентинович Молодых Олег Эдуардович	Крупные	1	-	Деятельность консультативная и работы в области компьютерных технологий	NSDC (Ukraine) Special Economic and Other Restrictive Measures (Sanctions)	-	-
Акционерное общество «Айсиэл-Кпо Вс»	11.11.1994	Степанов Евгений Витальевич	Нпо Вс, ООО Дьячков Виктор Васильевич Джидиси Сервисез, ООО Силантьева Элина Анатольевна Степанов Евгений Витальевич Гузаиров Айдар Фаилевич Кульмяков Игорь Викторович Ляшко Дмитрий Анатольевич Соловьев Сергей Владимирович	Средние	6	-	Разработка компьютерного программного обеспечения	NSDC (Ukraine) Special Economic and Other Restrictive Measures (Sanctions)	-	-
Ассоциация участников Рынка информационных технологий «Лига Цифровой Экономики»	30.10.2017	Шилов Сергей Александрович	Общество с Ограниченной Ответственностью «Философия.Ит» Общество с Ограниченной Ответственностью «Р.Т Решения»	Микро	-	-	Деятельность, связанная с использованием вычислительной техники и информационных технологий, прочая	NSDC (Ukraine) Special Economic and Other Restrictive Measures (Sanctions)	-	-

Продолжение таблицы В. 1

1	2	3	4	5	6	7	8	9	10	11
Общество с ограниченной ответственностью «Рубитех»	25.07.2016	Ведёхин Игорь Анатольевич	Общество с Ограниченной Ответственностью «Рубитех Холдинг»	Крупные	-	-	Деятельность консультативная и работы в области компьютерных технологий	-	78	Получает поддержку как субъект МСП
Акционерное общество «Ай-Теко»	05.03.1997	Подшивалов Виталий Вячеславович	Ай-Теко Инвест, АО	Крупные	11	9	62.09 Деятельность, связанная с использованием вычислительной техники и информационных технологий, прочая	NSDC (Ukraine) Special Economic and Other Restrictive Measures (Sanctions)	1 327	Субсидии На Государственную Поддержку Развития Кооперации Российских Образовательных Учреждений Высшего Профессионального Образования (ПОСТ.ПРАВ .РФ №218 от 09.04.10)
Публичное акционерное общество «Газпром Автоматизация»	05.08.1993	Бобриков Николай Михайлович	ООО Энергетические Решения, АО Газстройпром, ООО Завод Калининградгазавтоматика	Крупные	11	2	26.51.7 Производство приборов и аппаратуры для автоматического регулирования или управления	OFAC (USA) NSDC (Ukraine) Special Economic and Other Restrictive Measures (Sanctions)	617	-

Продолжение таблицы В. 1

1	2	3	4	5	6	7	8	9	10	11
Акционерное общество «Производственная фирма «Скб Контур»	26.03.1992	Сродных Михаил Юрьевич	Бублик Владимир Кузьмич Рахимянов Шамиль Мубаракович и пр. в 2020	Крупные	17	5	62.01 Разработка компьютерного программного обеспечения	NSDC (Ukraine) Special Economic and Other Restrictive Measures (Sanctions)	4020	-
Общество с ограниченной ответственностью «Монт»	25.01.2002	Москалев Дмитрий Владиславович	Общество с Ограниченной Ответственностью «Вин»	Крупные	1	-	46.51.2 Торговля оптовая программным обеспечением	NSDC (Ukraine) Special Economic and Other Restrictive Measures (Sanctions)	13	-
Акционерное общество «Максимателеком»	25.11.2004	Лобанов Денис Валерьевич	Акционерное Общество «Инвестмир» Общество с Ограниченной Ответственностью «Смартмолл"	Крупные	2	-	46.51 Торговля оптовая компьютерами, периферийными устройствами к компьютерам и программным обеспечением 63.11 Деятельность по обработке данных, предоставление услуг по размещению информации и связанная с этим деятельность	-	96	-

Продолжение таблицы В. 1

1	2	3	4	5	6	7	8	9	10	11
Общество с ограниченной ответственностью «М-инвест»	10.03.2005	Машенин Андрей Александрович	Машенин Андрей Александрович	Крупные	-	-	46.14.1 Деятельность агентов по оптовой торговле вычислительной техникой, телекоммуникационным оборудованием и прочим офисным оборудованием	-	562	-
Общество с ограниченной ответственностью «Инвента»	04.05.2016	Шемаханов Андрей Юрьевич	Андреева Людмила Ивановна Шемаханов Андрей Юрьевич	Крупные	-	-	63.11.1 Деятельность по созданию и использованию баз данных и информационных ресурсов	-	-	-
Общество с ограниченной ответственностью «Сап Снг»	10.09.2001	Житникова Ксения Александровна	Акционерная Компания «Сап Аг»	Крупные	1	2	62.02 Деятельность консультативная и работы в области компьютерных технологий	-	115	-
Общество с ограниченной ответственностью «Газпром Информ»	18.09.1998	Бурушкин Алексей Анатольевич	Публичное Акционерное Общество «Газпром»	Крупные	-	19	63.11.1 Деятельность по созданию и использованию баз данных и информационных ресурсов	-	456	-

Продолжение таблицы В. 1

1	2	3	4	5	6	7	8	9	10	11
Общество с ограниченной ответственностью «Озон Технологии»	13.05.2019	Кайзер Борис Валерьевич	Общество с Ограниченной Ответственностью «Озон Холдинг» Общество с Ограниченной Ответственностью «Интернет Решения»	Крупные	-	-	62.01 Разработка компьютерного программного обеспечения	-	-	-
Общество с ограниченной ответственностью «Облачные Технологии»	04.10.2016	Хлебородов Денис Сергеевич	-	Крупные	-	-	63.11 Деятельность по обработке данных, предоставление услуг по размещению информации и связанная с этим деятельность	-	4	-
Общество с ограниченной ответственностью «Норникель Спутник»	17.03.2010	Лопацинский Антон Михайлович	Акционерное Общество «Норильский Горно-Металлургический Комбинат Им. А.П. Завенягина»	Крупные	-	4	62.03.13 Деятельность по сопровождению компьютерных систем	-	58	-
Акционерное общество «Гринатом»	18.12.2009	Ермолаев Михаил Юрьевич	Акционерное Общество «Атомный Энергопромышленный Комплекс»	Крупные	2	13	62.01 Разработка компьютерного программного обеспечения	NSDC (Ukraine) Special Economic and Other Restrictive Measures (Sanctions)	2500	-

Продолжение таблицы В. 1

1	2	3	4	5	6	7	8	9	10	11
Общество с ограниченной ответственностью «Газпромнефть-цифровые решения»	01.04.2008	Поперлюков Алексей Сергеевич	Публичное акционерное общество «ГАЗПРОМ НЕФТЬ»	Крупные	-	-	62.01 Разработка компьютерного программного обеспечения	NSDC (Ukraine) Special Economic and Other Restrictive Measures (Sanctions)	67	-
Общество с ограниченной ответственностью «Безопасная Информационная Зона»	30.03.2016	Самарцев Дмитрий Викторович	Общество с Ограниченной Ответственностью «Управляющая Компания «Бизон»	Крупные	-	-	63.11.1 Деятельность по созданию и использованию баз данных и информационных ресурсов	NSDC (Ukraine) Special Economic and Other Restrictive Measures (Sanctions)	13	-
Общество с ограниченной ответственностью «Сигма»	15.04.2005	Колодей Сергей Михайлович	Общество с Ограниченной Ответственностью «Интер Рао-Стройинвест» Общество с Ограниченной Ответственностью «Актив-Энергия»	Средние	2	-	62.01 Разработка компьютерного программного обеспечения	-	262	-
Общество с ограниченной ответственностью «Газинформсервис»	11.02.2004	Глыбовский Сергей Иосифович	Пустарнаков Валерий Федорович	Крупные	2	4	62.09 Деятельность, связанная с использованием вычислительной техники и информационных технологий, прочая	-	420	-

Продолжение таблицы В. 1

1	2	3	4	5	6	7	8	9	10	11
Акционерное общество «Цифровые Закупочные Сервисы»	22.10.2020	Юдина Ольга Вячеславовна	Общество с Ограниченной Ответственностью «Электронная Торговая Площадка Гпб»	Крупные	-	-	62.01 Разработка компьютерного программного обеспечения	-	-	-
Общество с ограниченной ответственностью «Стримит»	11.06.2013	Кудрявцева Наталья Владимировна	Кудрявцева Наталья Владимировна	Малые			46.51 Торговля оптовая компьютерами, периферийными устройствами к компьютерам и программным обеспечением	-	257	-
Общество с ограниченной ответственностью «Рнт»	22.11.2001	Пискунов Владислав Сергеевич	Егоров Александр Геннадьевич	Крупные	-	6	62.01 Разработка компьютерного программного обеспечения	-	109	-
Общество с ограниченной ответственностью «Эйчпи инк»	18.05.2015	Зайцева Евгения Викторовна	Головнная Компания HP INC. Alpha Holding One B.V. Нидерланды	Крупные	-	-	46.51 Торговля оптовая компьютерами, периферийными устройствами к компьютерам и программным обеспечением	-	2	-
Акционерное общество «Позитив Текнолоджиз»	09.10.2007	Баранов Денис Сергеевич	Публичное Акционерное Общество «Группа Позитив»	Крупные	-	6	62.0 Разработка компьютерного программного обеспечения, консультационные услуги в данной области и другие сопутствующие услуги	OFAC (USA) NSDC (Ukraine) Special Economic and Other Restrictive Measures (Sanctions)	21	-

Продолжение таблицы В. 1

1	2	3	4	5	6	7	8	9	10	11
Общество с ограниченной ответственностью «Организационно-Технологические Решения 2000»	17.08.2000	Манохин Сергей Юрьевич	ООО Капитал Трейд, Брызгалов Алексей Алексеевич, Крикунчик Денис Григорьевич, Рыбаков Дмитрий Михайлович	Крупные	-	17	62.01 Разработка компьютерного программного обеспечения	NSDC (Ukraine) Special Economic and Other Restrictive Measures (Sanctions)	615	-
Акционерное общество «Сбербанк - Технологии»	06.07.2011	-	Публичное Акционерное Общество «Сбербанк России»	Крупные	-	-	62.01 Разработка компьютерного программного обеспечения	OFAC (USA) NSDC (Ukraine) Special Economic and Other Restrictive Measures (Sanctions)	2	-
Общество с ограниченной ответственностью «Авито Тех»	04.05.2021	Авито Менеджмент ООО,	Общество с Ограниченной Ответственностью «Кех Екоммерц»,	Крупные	-	-	62.01 Разработка компьютерного программного обеспечения	-	-	-
Общество с ограниченной ответственностью «Делл»	17.05.2007	Алюшина Наталия Владимировна	Dell Technologies Inc. · Сша	Крупные	-	-	46.51 Торговля оптовая компьютерами, периферийными устройствами к компьютерам и программным обеспечением	-	-	-

Продолжение таблицы В. 1

1	2	3	4	5	6	7	8	9	10	11
Общество с ограниченной ответственностью «Сбербанк-Сервис»	08.08.2013	Евтушенко Алексей Юрьевич	Публичное Акционерное Общество «Сбербанк России»	Крупные	-	1	62.02 Деятельность консультативная и работы в области компьютерных технологий 95.11 Ремонт компьютеров и периферийного компьютерного оборудования	OFAC (USA) NSDC (Ukraine) Special Economic and Other Restrictive Measures (Sanctions)	186	-
Общество с ограниченной ответственностью «Эвотор Офд»	30.05.2016	Баров Алексей Вениаминович	ООО Эвотор, Уланов Алексей Валентинович	Малые	1	-	61.10 Деятельность в области связи на базе проводных технологий	-	32	-
Общество с ограниченной ответственностью «Компания «Тензор»	10.06.1999	Уваров Сергей Васильевич	Уваров Сергей Васильевич, Кошелев Александр Евгеньевич, Новиков Дмитрий Владимирович, Боровиков Кирилл Сергеевич, Зафиевский Дмитрий Александрович	Крупные		102	62.01 Разработка компьютерного программного обеспечения	-	1676	-
Общество с ограниченной ответственностью «Лукойл-Технологии»	01.11.2018	Кренкель Эрнст Теодорович	Лукойл, ПАО	Крупные	1	21	63.11.1 Деятельность по созданию и использованию баз данных и информационных ресурсов	-	4	-

Продолжение таблицы В. 1

1	2	3	4	5	6	7	8	9	10	11
Общество с ограниченной ответственностью «Хиквижн»	06.02.2015	Тан Го-Лун	Hdt International Limited Сянган	Крупные	-	1	46.90 Торговля оптовая неспециализированная	-	-	-
Общество с ограниченной ответственностью «Тинькофф Центр Разработки»	09.11.2016	Борисов Сергей Станиславович	Tcs Group Holding Plc 49%, АО Тинькофф Банк 49%, ООО Ткс	Крупные	7	-	62.01 Разработка компьютерного программного обеспечения	-	-	-
Общество с ограниченной ответственностью «Бюджетные и Финансовые Технологии»	06.11.2007	Зейтениди Наталья Юрьевна	Рт Лабс, АО	Крупные	2	2	62.01 Разработка компьютерного программного обеспечения	-	2 862	выделен Минобрнауки 410 млн руб.
Общество с ограниченной ответственностью «Акстим»	15.11.2002	Диланян Вартан Петрович	Диланян Вартан Петрович, Киреев Сергей Евгеньевич, Одинаева Ирина Владимировна, Ильин Юрий Михайлович, Малькова Лариса Михайловна, Топоров Дмитрий Сергеевич	Крупные	2	2	70.22 Консультирование по вопросам коммерческой деятельности и управления 46.51 Торговля оптовая компьютерами, периферийными устройствами к компьютерам и программным обеспечением	-	35	-
Акционерное общество «Нокиа солюшнз энд нетворкс»	09.04.1997	Парфенов Игорь Борисович	NOKIA SOLUTIONS AND NETWORKS B.V.	Крупные			95.12 Ремонт коммуникационного оборудования	-	-	-

Продолжение таблицы В. 1

1	2	3	4	5	6	7	8	9	10	11
Общество с ограниченной ответственностью «Глоубайт»	07.05.2015	Кудич Алексей Викторович	Кудич Алексей Викторович, Скудин Владимир Валерьевич, Лисицин Евгений Вячеславович	Крупные	-	-	62.01 Разработка компьютерного программного обеспечения	-	10	-
Общество с ограниченной ответственностью «Депо Электроникс»	02.06.2008	Зенин Евгений Владимирович	Эскин Сергей Вадимович, Ирисов Алексей Алексеевич	Крупные	1	-	26.20 Производство компьютеров и периферийного оборудования	NSDC (Ukraine) Special Economic and Other Restrictive Measures (Sanctions)	763	455 млн руб. Минпрторг
Общество с ограниченной ответственностью «Сиссофт Солюшнс»	11.04.2017	Тикуркин Максим Александрович	Тикуркин Максим Александрович	1	-	-	62.01 Разработка компьютерного программного обеспечения	-	-	Получатель поддержки как субъект МСП
Общество с ограниченной ответственностью «Сеть дата-центров «Селектел»	11.09.2008	Любимов Олег Игоревич	Компания с ограниченной ответственностью «ЛВЛ1 МЕНЕДЖМЕНТ ЛТД»	Крупные	2	2	63.11 Деятельность по обработке данных, предоставление услуг по размещению информации и связанная с этим деятельность	-	7	-

Продолжение таблицы В. 1

1	2	3	4	5	6	7	8	9	10	11
Общество с ограниченной ответственностью «Асбис»	05.10.2000	Галямов Эдуард Ринатович	Asbisc Enterprises Plc	Крупные	-	-	46.51 Торговля оптовая компьютерами, периферийными устройствами к компьютерам и программным обеспечением	NSDC (Ukraine) Special Economic and Other Restrictive Measures (Sanctions)	4	-
Акционерное общество «Информационные Технологии и Коммуникационные Системы»	21.03.1995	Чапчаев Андрей Анатольевич	Юридические и Физические Лица	Крупные	4	-	62.01 Разработка компьютерного программного обеспечения	-	469	1100 млн руб. Минпромторг
Общество с ограниченной ответственностью «Технологический Центр Дойче Банка»	31.07.2014	Бабыкин Иван Евгеньевич	Deutsche Bank Ag ·	Крупные	-	1	62.01 Разработка компьютерного программного обеспечения	-	-	-
Акционерное общество «Управляющая Компания Диасофт»	08.01.2015	Рощупкин Олег Митрофанович	-	Средние	11	-	64.20 Деятельность холдинговых компаний	-	-	-
Общество с ограниченной ответственностью «Оранж Бизнес Сервисез»	13.02.2003	Овчаренко Сергей Валерьевич	Orange ·	Крупные	1	33	61.10.1 Деятельность по предоставлению услуг телефонной связи	-	230	-

Продолжение таблицы В. 1

1	2	3	4	5	6	7	8	9	10	11
Общество с ограниченной ответственностью «Программный Продукт»	26.08.2002	Подобайло Николай Николаевич	Шунаев Александр Сергеевич, Александров Сергей Анатольевич	Крупные	1	-	62.01 Разработка компьютерного программного обеспечения	-	313	Получатель поддержки как субъект МСП
Общество с ограниченной ответственностью «Лаборатория Вс»	21.09.2011	Викарук Лариса Ивановна	Никулин Максим Александрович, Денисов Евгений Викторович, Соков Максим Михайлович	Крупные	2	3	62.01 Разработка компьютерного программного обеспечения	-	-	-
Акционерное общество «Россети Цифра»	07.10.1999	Архипов Александр Геннадьевич	-	Крупные		2	62.01 Разработка компьютерного программного обеспечения	-	162	-
Общество с ограниченной ответственностью «Яндекс.Облако»	13.07.2018	Черников Александр Владимирович	Яндекс, ООО	Крупные	-	-	62.01 Разработка компьютерного программного обеспечения	-	-	-
Акционерное общество «Научно-исследовательский и проектно-конструкторский институт информатизации, автоматизации и связи на железнодорожном транспорте»	08.08.2007	Долгий Александр Игоревич	Открытое Акционерное Общество «Российские Железные Дороги»	Крупные	1	4	72.19 Научные исследования и разработки в области естественных и технических наук прочие	NSDC (Ukraine) Special Economic and Other Restrictive Measures (Sanctions)	796	-

Продолжение таблицы В. 1

1	2	3	4	5	6	7	8	9	10	11
Общество с ограниченной ответственностью «Магнит Ит Лаб»	23.01.2019	Медведева Ксения Владимировна	Магнит, ПАО	Микро	-	-	62.01 Разработка компьютерного программного обеспечения	-	-	-
Общество с ограниченной ответственностью «Тр-Линк»	02.11.2009	Лю Чжифэн	Big Field Global Pte. Ltd. ·	Крупные	-	-	46.6 Торговля оптовая прочими машинами, оборудованием и принадлежностями	-	2	-
Акционерное общество «Барс Груп»	03.09.2012	Ахмеров Тимур Маратович	Граждане России	Крупные	-	13	62.01 Разработка компьютерного программного обеспечения	-	1045	-
Общество с ограниченной ответственностью «Код Безопасности»	09.10.2008	Голов Андрей Викторович	ООО Рцр, Генс Филипп Георгиевич	333	1	-	26.20 Производство компьютеров и периферийного оборудования	NSDC (Ukraine) Special Economic and Other Restrictive Measures (Sanctions)	12	Получатель поддержки как субъект МСП
Общество с ограниченной ответственностью «Айти Солюшнс Рус»	20.02.2014	Морякова Елена Владимировна	Deutsche Telekom Ag ·	Крупные	-	-	62.01 Разработка компьютерного программного обеспечения	-	-	-
Общество с ограниченной ответственностью «Майкрософт Рус»	26.05.2004	Орндорфф Бенджамин Оуэн	Microsoft Corporation ·	Крупные	-	15	62.01 Разработка компьютерного программного обеспечения	-	58	-

Продолжение таблицы В. 1

1	2	3	4	5	6	7	8	9	10	11
Акционерное общество научно-инженерное предприятие «Информзащита»	22 Августа 1995	Ефимов Петр Валентинович	Генс Филипп Георгиевич	Крупные	3	-	62.01 Разработка компьютерного программного обеспечения	NSDC (Ukraine) Special Economic and Other Restrictive Measures (Sanctions)	1262	-
Общество с ограниченной ответственностью «Ксерокс (Снг)»	14.10.1993	Бобров Максим Вячеславович	Xerox Holdings Corporation ·	Крупные	-	2	46.66 Торговля Оптовая прочей офисной техникой и оборудованием	-	319	-
Общество с ограниченной ответственностью «Русбитех-Астра»	13.10.2016	Сивцев Илья Игоревич	Группа Астра, Пао \Генс Филипп Георгиевич	Зоб	-	8	62.01 Разработка компьютерного программного обеспечения	NSDC (Ukraine) Special Economic and Other Restrictive Measures (Sanctions)	1	Получатель поддержки как субъект МСП
Общество с ограниченной ответственностью «Синто»	12.09.2005	Савченко Дмитрий Петрович	Савченко Дмитрий Петрович	Крупные	-	-	46.66 Торговля оптовая прочей офисной техникой и оборудованием 26.11 Производство элементов электронной аппаратуры 26.12 Производство электронных печатных плат	NSDC (Ukraine) Special Economic and Other Restrictive Measures (Sanctions)	1985	Получатель поддержки как субъект МСП

Продолжение таблицы В. 1

1	2	3	4	5	6	7	8	9	10	11
Общество с ограниченной ответственностью «Уральский центр систем безопасности»	08.05.2007	Богданов Валентин Викторович	Пустарнаков Валерий Фёдорович, Антипинский Андрей Сергеевич	Крупные	1	1	62.09 Деятельность, связанная с использованием вычислительной техники и информационных технологий, прочая	NSDC (Ukraine) Special Economic and Other Restrictive Measures (Sanctions)	377	-
Общество с ограниченной ответственностью «Терралинк»	17.05.1995	Кудинов Алексей Анатольевич	Шаронов Валерий Анатольевич	Крупные	1	-	62.01 Разработка компьютерного программного обеспечения	-	41	-
Общество с ограниченной ответственностью «Интел Текнолоджис»	17.02.2012	Клушина Алина Валентиновна	Intel Corporation	Малые	-	2	73.11 Деятельность рекламных агентств	-	-	-
Общество с ограниченной ответственностью «Атос айти солюшенс энд сервисез»	01.11.2010	Декало Алексей Николаевич	Инвест Холдинг 4, ООО	Крупные	-	2	62.02.9 Деятельность консультативная в области компьютерных технологий прочая	-	10	-
Общество с ограниченной ответственностью «Транснефть-Технологии»	08.08.2012	Дворников Дмитрий Юрьевич	ООО Транснефть Финанс, Ао Связьтранснефть	Крупные	6	-	63.11.1 Деятельность по созданию и использованию баз данных и информационных ресурсов	-	140	-

Продолжение таблицы В. 1

1	2	3	4	5	6	7	8	9	10	11
Общество с ограниченной ответственностью «ВК цифровые технологии»	29.09.2017	Управляющая Компания Вк, ООО	ООО Цифровая Трансформация Плюс, ООО Вк	Крупные	-	-	62.01 Разработка компьютерного программного обеспечения	-	10	-
Общество с ограниченной ответственностью «Атол»	28.04.2016	Колчина Оксана Александровна	Ук Атол, ООО \Макаров Алексей Петрович, Макарова Ирина Евгеньевна	Крупные	-	1	26.20 Производство компьютеров и периферийного оборудования	-	8	-
Акционерное общество «Рамэк-Вс»	31.10.1996	Агапов Алексей Анатольевич	Акционерное Общество «Центральное Конструкторское Бюро Морской Техники «Рубин»	435ч	-	1	26.20 Производство компьютеров и периферийного оборудования	NSDC (Ukraine) Special Economic and Other Restrictive Measures (Sanctions)	1671	100 млн руб. Минпромторг
Общество с ограниченной ответственностью «Сиско Солюшенз»	23.07.2013	Горюшина Наталья Германовна	Cisco Systems, Inc. ·	Крупные	-	-	46.52 Торговля оптовая электронным и телекоммуникационным оборудованием и его запасными частями	-	15	-
Общество с ограниченной ответственностью «Группа компаний «Корус Консалтинг»	30.06.2000	Семенов Александр Владимирович	Семенов Александр Владимирович, Голубева Марина Николаевна, Рахманов Александр Юрьевич, Аксельрод Александр Викторович, Макарова Юлия Александровна	Средние	8	2	62.01 Разработка компьютерного программного обеспечения	NSDC (Ukraine) Special Economic and Other Restrictive Measures (Sanctions)	219	-

Продолжение таблицы В. 1

1	2	3	4	5	6	7	8	9	10	11
Акционерное общество «Инлайн Груп»	11.02.2000	Ромашкин Алексей Иванович	Граждане России	Крупные	1	-	62.02 Деятельность консультативная и работы в области компьютерных технологий	NSDC (Ukraine) Special Economic and Other Restrictive Measures (Sanctions)	237	-
Общество с ограниченной ответственностью «Тэк Информ»	02.03.2015	Козловский Игорь Валерьевич	Центрэнергохолдинг, Пао. Головная Компания Руководит Пао Газпром	Крупные	-	13	62.01 Разработка компьютерного программного обеспечения	-	281	-
Общество с ограниченной ответственностью «Сибур Диджитал»	01.11.2017	Мельникова Алиса Валериевна	Головная Компания Сибур Холдинг, Пао	Крупные	-	17	62.01 Разработка компьютерного программного обеспечения	-	-	-
Акционерное общество «Универсальные технологии»	11.02.2010	Витоженц Александр Генрихович	Витоженц Александр Генрихович, Бровко Лев Николаевич, Иудин Виктор Владимирович	Крупные	-	-	46.51.1 Торговля оптовая компьютерами и периферийными устройствами	-	167	-
Общество с ограниченной ответственностью «Технопром»	02.11.2011	Свиридов Евгений Николаевич	Гловная Компания (Сигма Инвестментс, АО)	Крупные	-	-	62.09 Деятельность, связанная с использованием вычислительной техники и информационных технологий, прочая	-	59	Получатель поддержки как субъект МСП

Продолжение таблицы В. 1

1	2	3	4	5	6	7	8	9	10	11
Общество с ограниченной ответственностью «Кьютэк»	01.02.2006	Арсланова Гузель Расимовна	Шитиков Иван Александрович	Средние	1	-	26.11 Производство элементов электронной аппаратуры	-	193	Получатель поддержки как субъект МСП, Субсидии от Минпромторг
Общество с ограниченной ответственностью «Вентра»	17.05.2000	Черников Александр Александрович	Компания с Ограниченной Ответственностью «Сантими Кэпитал» Сша, Закрытый Паевой Инвестиционный Комбинированный Фонд «Фонд Пре-Айпио 1» (Управляющая Компания: АО Вим Инвестиции), Симонова Марина Львовна, Карабанова Екатерина Владимировна, Дрозд Александр Сергеевич, Алексеев Тимофей Викторович	Крупные	11	2	70.22 Консультирование по вопросам коммерческой деятельности и управления	-	2	-
Общество с ограниченной ответственностью «Бифорком Текнолоджис»	21.09.2015	Галенко Сергей Николаевич	Закрытый Паевой Инвестиционный Комбинированный Фонд «Б4 Развитие» (Управляющая Компания: АО «Апекс Менеджмент»)	Крупные	-	-	26.30 Производство коммуникационного оборудования	-	-	Получатель поддержки как субъект МСП

Продолжение таблицы В. 1

1	2	3	4	5	6	7	8	9	10	11
Акционерное общество «Неофлекс Консалтинг»	21.05.2009	Рубан Олег Викторович	Граждане России	Крупные	2	6	62.01 Разработка компьютерного программного обеспечения	-	57	-
Общество с ограниченной ответственностью «Рсхб-Интех»	01.09.2016	Сандуковский Михаил Александрович	ООО Агроторг-Трейд, ООО Тда Тульский	Крупные	-	2	62.01 Разработка компьютерного программного обеспечения	-	1	-
Общество с ограниченной Ответственностью «Деловой Офис»	14.02.2011	Волков Алексей Максимович	Солкин Игорь Геннадьевич	Крупные	-	1	26.20 Производство компьютеров и периферийного оборудования	-	-	Получатель поддержки как субъект МСП

Источник: составлено автором.

Приложение Г

(информационное)

Законодательные акты Российской Федерации в сфере ИТ, принятые в 2020–2023 гг.

Таблица Г. 1 – Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации, Нормативные правовые акты в сфере ИТ

Дата	Полное название документа
1	2
17.12.2020	Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 17.12.2020 № 715 «Об утверждении типовых условий контрактов на выполнение работ по созданию и (или) развитию (модернизации) государственных (муниципальных) и (или) иных информационных систем»
25.01.2021	Приказ Минцифры России № 27 «Об определении способа перечисления средств субсидии из федерального бюджета автономной некоммерческой организации высшего образования «Университет Иннополис» на проведение повышения квалификации преподавателей высшего и среднего профессионального образования по новым программам для ИТ-специальностей и различных предметных отраслей и обеспечение достижения отдельных результатов федерального проекта «Кадры для цифровой экономики» с применением казначейского обеспечения обязательств»
01.02.2021	Приказ Минцифры России № 49 «Об определении способа перечисления из федерального бюджета субсидии автономной некоммерческой организации «Университет Национальной технологической инициативы 2035» на проведение обучения по дополнительным профессиональным программам с использованием мер государственной поддержки для получения новых востребованных на рынке труда цифровых компетенций и обеспечение достижения отдельных результатов федерального проекта «Кадры для цифровой экономики» с применением казначейского обеспечения обязательств»
14.04.2021	Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 14.04.2021 № 379 «О Конкурсной комиссии по отбору заявок на получение из федерального бюджета субсидий организациям, осуществляющим производство, распространение и тиражирование социально значимых программ в области электронных средств массовой информации, на создание и поддержание в информационно-телекоммуникационной сети «Интернет» сайтов, имеющих социальное или образовательное значение»
02.08.2021	Приказ Минцифры России от 02.08.2021 № 782 (с изм. от 28.11.2022) «Об утверждении состава и Положения о межведомственной рабочей группе по вопросам подготовки разъяснений условий использования налоговых преференций для организаций, осуществляющих деятельность в области информационных технологий, а также формирования предложений по мерам налогового стимулирования и поддержки отрасли информационных технологий»
30.08.2021	Протокол заседания межведомственной рабочей группы по вопросам подготовки разъяснений условий использования налоговых преференций для организаций, осуществляющих деятельность в области информационных технологий, а также формирования предложений по мерам налогового стимулирования и поддержки отрасли информационных технологий

Продолжение таблицы Г. 1

1	2
10.09.2021	Приказ Минцифры России № 946 «О внесении изменений в приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 20.09.2018 № 486 «Об утверждении методических рекомендаций по переходу государственных компаний на преимущественноеиспользование отечественного программного обеспечения, в том числе отечественного офисного программного обеспечения»
15.09.2021	Приказ Минцифры России № 979 «О внесении изменений в приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 08.05.2019 № 184 «Об утверждении методических рекомендаций по переходу предприятий, учреждений и организаций, подведомственных федеральным органам исполнительной власти, органам исполнительной власти субъектов Российской Федерации, органам местного самоуправления и государственным внебюджетным фондам, на преимущественное использование отечественного программного обеспечения, в том числе отечественного офисного программного обеспечения»
11.10.2021	Разъяснение в части толкования выражений «разрабатывают и реализуют разработанные ими программы для ЭВМ, базы данных» и «разработанные ею программы для ЭВМ, базы данных», а также перечня документов, которые могут быть использованы организацией для подтверждения факта участия в разработке программ для ЭВМ и баз данных для их использования государственными органами, органами местного самоуправления, юридическими и физическими лицами
21.10.2021	Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 21.10.2021 № 1085 «Об утверждении Административного регламента предоставления Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации государственной услуги по государственной аккредитации организаций, осуществляющих деятельность в области информационных технологий»
21.10.2021	Приказ Минцифры России № 1085 «Об утверждении административного регламента предоставления Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации государственной услуги по государственной аккредитации организаций, осуществляющих деятельность в области информационных технологий»
17.01.2022	Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 17.01.2022 № 27 «Об утверждении Требований к оказанию услуг подвижной радиосвязи и подвижной радиотелефонной связи при использовании бизнес-моделей виртуальных сетей подвижной радиосвязи и подвижной радиотелефонной связи»
18.01.2022	Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 18.01.2022 № 31 «Об утверждении порядка и сроков представления в федеральное государственное бюджетное учреждение «Российская академия наук» проектов тематики научных исследований, проектов планов научных работ и отчетов о проведенных научных исследованиях, о полученных научных и (или) научно-технических результатах за отчетный финансовый год научных организаций и образовательных организаций высшего образования, осуществляющих научные исследования за счет средств федерального бюджета, находящихся в ведении Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации а также сроков проведения федеральным государственным бюджетным учреждением «Российская академия наук» оценки и подготовки им заключений по таким проектам тематики научных

Продолжение таблицы Г. 1

1	2
	исследований, планов научных работ, отчетам, а также по проектам программ развития указанных организаций»
03.02.2022	Приказ Минцифры России № 86 «О внесении изменений в План (дорожную карту) реализации Концепции построения и развития узкополосных беспроводных сетей связи «Интернета вещей» на территории Российской Федерации, утвержденный приказом Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 28.11.2019 № 773»
10.03.2022	Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 10.03.2022 № 184 "Об утверждении методики оценки результативности деятельности научных организаций, подведомственных Министерству цифрового развития, связи и массовых коммуникаций Российской Федерации, выполняющих научно-исследовательские, опытно-конструкторские и технологические работы гражданского назначения»
10.03.2022	Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 10.03.2022 № 183 «Об утверждении Положения о комиссии по оценке результативности деятельности научных организаций, подведомственных Министерству цифрового развития, связи и массовых коммуникаций Российской Федерации, выполняющих научно-исследовательские, опытно-конструкторские и технологические работы гражданского назначения»
10.03.2022	Приказ Минцифры России № 186 «Об утверждении Методических рекомендаций по обеспечению необходимого уровня безопасности в сфере информационно-коммуникационных технологий государственных корпораций, компаний с государственным участием, а также их дочерних организаций и зависимых обществ»
18.03.2022	Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 18.03.2022 № 214 «Об утверждении Порядка выдачи Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации разрешений на вывоз за пределы территории Российской Федерации на территории государств - членов Евразийского экономического союза отдельных видов товаров»
23.05.2022	Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 23.05.2022 № 431 «О признании утратившими силу некоторых приказов Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации в сфере грантовой поддержки проектов по разработке и внедрению отечественных продуктов, сервисов и платформенных решений»
24.06.2022	Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 24.06.2022 № 494 «О временном сокращении перечней лицензионных требований в сфере телевизионного вещания и (или) радиовещания в 2022 году»
01.08.2022	Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 01.08.2022 № 573 «Об утверждении основных принципов функционирования программы для электронных вычислительных машин, которая предназначена для поиска, просмотра и приобретения программ для электронных вычислительных машин, применяемых потребителями с использованием технически сложных товаров»

Продолжение таблицы Г. 1

1	2
01.08.2022	Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 01.08.2022 № 570 «ехнологического оборудования, комплектующих и запасных частей к нему, сырья и материалов, ввозимых для исключительного использования на территории Российской Федерации в рамках реализации инвестиционных проектов в области информации и связи, а также формы подтверждения целевого назначения в отношении технологического оборудования, комплектующих и запасных частей к нему, сырья и материалов, ввозимых для исключительного использования на территории Российской Федерации в рамках реализации инвестиционных проектов в области информации и связи»
02.09.2022	Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 02.09.2022 № 641 «Об утверждении Порядка выдачи Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации разрешений на вывоз за пределы территории Российской Федерации отдельных видов товаров по перечню согласно приложению № 4 к постановлению Правительства Российской Федерации от 9 марта 2022 г. № 312 «О введении на временной основе разрешительного порядка вывоза отдельных видов товаров за пределы территории Российской Федерации»
13.09.2022	Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 13.09.2022 № 660 «Об утверждении перечня программ для электронных вычислительных машин, размещаемых в программе для электронных вычислительных машин, которая предназначена для поиска, просмотра и приобретения программ для электронных вычислительных машин, применяемых потребителями с использованием технически сложных товаров, в обязательном порядке»
26.09.2022	Приказ министерства цифрового развития, связи и массовых коммуникаций рф от 26 сентября 2022 г. № 712 «О рекомендованном перечне приоритетных специальностей и направлений подготовки высшего образования для обеспечения основных потребностей аккредитованных организаций, осуществляющих деятельность в области информационных технологий, и операторов связи в квалифицированных кадрах»
27.09.2022	Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 27.09.2022 № 715 «Об утверждении Порядка выдачи Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации подтверждения целевого назначения товаров, используемых в целях развития цифровых технологий, ввозимых на территорию Российской Федерации в целях реализации мер, направленных на повышение устойчивости экономик государств — членов Евразийского экономического союза»
08.10.2022	Приказ Минцифры России от 08.10.2022 № 766 «О перечне видов деятельности в области информационных технологий»
31.01.2023	Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 31.01.2023 № 62 «Об утверждении классификатора программно-аппаратных комплексов и Правил применения классификатора программно-аппаратных комплексов»

Продолжение таблицы Г. 1

1	2
29.03.2023	Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, Федеральной службы безопасности Российской Федерации от 29.03.2023 № 321/147 «Об утверждении Типовых требований к плану мероприятий по внедрению собственниками или иными владельцами технологических сетей связи, имеющих уникальный идентификатор совокупности средств связи и иных технических средств в информационно- телекоммуникационной сети «Интернет», технических средств, обеспечивающих выполнение установленных действий при проведении оперативно-разыскных мероприятий»
11.05.2023	Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 11.05.2023 № 449 «Об утверждении перечня видов деятельности в области информационных технологий»

Источник: составлено автором.

Таблица Г. 2 – Министерство экономического развития Российской Федерации, Нормативные правовые акты в сфере ИТ

Дата	Полное название документа
30.12.2020	Приказ Минэкономразвития России от 30.12.2020 № 876 (ред. от 22.07.2021) «Об утверждении ведомственной программы цифровой трансформации Министерства экономического развития Российской Федерации на 2021 - 2023 годы»
01.10.2021	Единый план по достижению национальных целей развития Российской Федерации на период до 2024 года и на плановый период до 2030 года
29.12.2021	Ведомственная программа цифровой трансформации Министерства экономического развития Российской Федерации на 2022-2024 годы
30.12.2021	Ведомственная программа цифровой трансформации Министерства экономического развития Российской Федерации на 2021-2023 годы, утверждена приказом Минэкономразвития России от 30 декабря 2020 г. № 876 (редакция от 22.07.2021)
16.02.2022	Ведомственная программа цифровой трансформации Министерства экономического развития Российской Федерации на 2022-2024 годы
18.02.2022	Приказ Минэкономразвития России от 18.02.2022 № 67 (ред. от 23.12.2022) «О государственной информационной системе «Экономика» (вместе с «Концепцией создания государственной информационной системы «Экономика»)
30.12.2022	Ведомственная программа цифровой трансформации Минэкономразвития России на 2023 год и плановый период 2024-2025 годов
11.02.2021	Приказ Минэкономразвития России от 11 февраля 2021г. № 63 «Об утверждении положения о Департаменте цифровой трансформации Министерства экономического развития Российской Федерации»
14.07.2021	Приказ Минэкономразвития России от 14 июля 2021 г. № 427 «О внесении изменений в приложения № 1, № 2 и № 3 к приказу Минэкономразвития России от 18 ноября 2020 г. № 755 «Об утверждении требований к форме и содержанию инициативного предложения об установлении экспериментального правового режима в сфере цифровых инноваций и проекта программы экспериментального правового режима в сфере цифровых инноваций, а также перечня документов, прилагаемых к инициативному предложению об установлении экспериментального правового режимав сфере цифровых инноваций»

Продолжение таблицы Г. 2

1	2
14.07.2021	Приказ Минэкономразвития России от 14 июля 2021 г. № 428 «О внесении изменений в приложение № 2 к приказу Минэкономразвития России от 18 ноября 2020 г. № 754 «Об утверждении формы заявки на присоединение к экспериментальному правовому режиму в сфере цифровых инноваций, перечня прилагаемых к ней документов, порядка направления, порядка и сроков ее рассмотрения, порядка направления претенденту мотивированного отказа в присоединении к экспериментальному правовому режиму в сфере цифровых инноваций, формы заключения регулирующего органа и состава содержащихся в нем сведений»
28.04.2022	Постановление Правительства Российской Федерации от 28 апреля 2022 № 775 «О внесении изменений в государственную программу Российской Федерации «Экономическое развитие и инновационная экономика»

Источник: составлено автором.

Таблица Г. 3 – Постановление Правительства Российской Федерации, Нормативные правовые акты в сфере ИТ

Дата	Полное название документа
1	2
02.02.2021	Постановление Правительства Российской Федерации от 02.02.2021 № 103 «Об утверждении Правил предоставления из федерального бюджета субсидий организациям, осуществляющим производство, распространение и тиражирование социально значимых программ в области электронных средств массовой информации, на создание и поддержание в информационно-телекоммуникационной сети «Интернет» сайтов, имеющих социальное или образовательное значение»
02.04.2021	Постановление Правительства Российской Федерации от 02.04.2021 № 527 «О внесении изменений в постановление Правительства Российской Федерации от 28 августа 2019 г. № 1114»
14.05.2021	Постановление Правительства РФ от 14 мая 2021 г. № 733 «Об утверждении Положения о федеральной государственной информационной системе «Единая информационная платформа национальной системы управления данными» и о внесении изменений в некоторые акты Правительства Российской Федерации
16.06.2021	Постановление Правительства Российской Федерации от 16.06.2021 № 914 «О приостановлении действия абзаца второго пункта 6 Правил хранения операторами связи текстовых сообщений пользователей услугами связи, голосовой информации, изображений, звуков, видео- и иных сообщений пользователей услугами связи»
28.06.2021	Постановление Правительства Российской Федерации от 28.06.2021 № 1031 «Об утверждении Правил предоставления субсидии из федерального бюджета Российскому фонду развития информационных технологий на возмещение затрат по использованию субъектами малого и среднего предпринимательства российского программного обеспечения»
18.09.2021	Распоряжение Правительства Российской Федерации от 18.09.2021 № 2608-р
22.09.2021	Постановление Правительства Российской Федерации от 22.09.2021 № 1589 «О внесении изменения в постановление Правительства Российской Федерации от 20 июля 2013 г. № 606»
22.10.2021	Распоряжение Правительства Российской Федерации от 22.10.2021 № 2998-р

Продолжение таблицы Г. 3

1	2
30.11.2021	Постановление Правительства Российской Федерации от 30.11.2021 № 2098 «О внесении изменений в постановление Правительства Российской Федерации от 18 ноября 2020 г. № 1867"
17.12.2021	Распоряжение Правительства Российской Федерации от 17.12.2021 № 3670-р «О присуждении премий Правительства Российской Федерации 2021 года в области средств массовой информации»
25.12.2021	Постановление Правительства Российской Федерации от 25.12.2021 № 2469 «О Правительственной комиссии по определению перечня отечественных социально значимых информационных ресурсов»
03.02.2022	Постановление Правительства Российской Федерации от 03.02.2022 № 94 «Об утверждении Правил предоставления субсидий из федерального бюджета российскому юридическому лицу на разработку и реализацию на регулярной основе программы кибергигиены и повышения грамотности широких слоев населения по вопросам информационной безопасности»
03.02.2022	Постановление Правительства РФ от 03.02.2022 № 94 «Об утверждении Правил предоставления субсидий из федерального бюджета российскому юридическому лицу на разработку и реализацию на регулярной основе программы кибергигиены и повышения грамотности широких слоев населения по вопросам информационной безопасности»
24.03.2022	Постановление Правительства РФ от 24.03.2022 № 448 „Об особенностях осуществления государственного контроля (надзора), муниципального контроля в отношении аккредитованных организаций, осуществляющих деятельность в области информационных технологий, и о внесении изменений в некоторые акты Правительства Российской Федерации»
28.03.2022	Постановление Правительства РФ от 28 марта 2022 г. № 490 «Об утверждении Правил предоставления права на получение отсрочки от призыва на военную службу гражданам Российской Федерации, работающим в аккредитованных организациях, осуществляющих деятельность в области информационных технологий»
01.04.2022	Распоряжение Правительства Российской Федерации от 01.04.2022 № 714-р
06.04.2022	Постановление Правительства Российской Федерации от 06.04.2022 № 598 «О внесении изменений в Правила предоставления субсидии из федерального бюджета Российскому фонду развития информационных технологий на поддержку проектов по разработке и внедрению российских решений в сфере информационных технологий»
06.04.2022	Постановление Правительства Российской Федерации от 06.04.2022 № 601 «О внесении изменений в Правила предоставления субсидии из федерального бюджета федеральному государственному бюджетному учреждению «Фонд содействия развитию малых форм предприятий в научно-технической сфере» на осуществление поддержки проектов малых предприятий по разработке, применению и коммерциализации российских цифровых решений и признании утратившим силу подпункта «л» пункта 2 изменений, которые вносятся в постановление Правительства Российской Федерации от 3 мая 2019 г. № 554, утвержденных постановлением Правительства Российской Федерации от 31 августа 2019 г. № 1127»
06.04.2022	Постановление Правительства Российской Федерации от 06.04.2022 № 599 «О внесении изменений в Правила предоставления субсидии из федерального бюджета некоммерческой организации Фонд развития Центра разработки и коммерциализации новых технологий на обеспечение первого масштабного внедрения российских решений в сфере информационных технологий»

Продолжение таблицы Г. 3

1	2
06.04.2022	Постановление Правительства РФ от 06.04.2022 № 599 «О внесении изменений в Правила предоставления субсидии из федерального бюджета некоммерческой организации Фонд развития Центра разработки и коммерциализации новых технологий на обеспечение первого масштабного внедрения российских решений в сфере информационных технологий»
06.04.2022	Постановление Правительства РФ от 06.04.2022 № 598 (ред. от 22.11.2022) «О внесении изменений в Правила предоставления субсидии из федерального бюджета Российскому фонду развития информационных технологий на поддержку проектов по разработке и внедрению российских решений в сфере информационных технологий»
06.04.2022	Постановление Правительства РФ от 06.04.2022 № 601 «О внесении изменений в Правила предоставления субсидии из федерального бюджета федеральному государственному бюджетному учреждению «Фонд содействия развитию малых форм предприятий в научно-технической сфере» на осуществление поддержки проектов малых предприятий по разработке, применению и коммерциализации российских цифровых решений и признании утратившим силу подпункта «л» пункта 2 изменений, которые вносятся в постановление Правительства Российской Федерации от 3 мая 2019 г. № 554, утвержденных постановлением Правительства Российской Федерации от 31 августа 2019 г. № 1127»
26.04.2022	Постановление Правительства Российской Федерации от 26.04.2022 № 754 «Об утверждении Правил предоставления субсидий из федерального бюджета российским кредитным организациям на возмещение недополученных ими доходов по кредитам, выданным аккредитованным системообразующим организациям в сфере информационных технологий, а также организациям, входящим в группу лиц системообразующей организации в сфере информационных технологий»
30.04.2022	Постановление Правительства РФ от 30 апреля 2022 г. № 805 "Об утверждении Правил предоставления субсидий из федерального бюджета акционерному обществу «ДОМ.РФ» в виде вклада в имущество акционерного общества «ДОМ.РФ", не увеличивающего его уставный капитал, на цели возмещения кредитным и иным организациям недополученных доходов по жилищным (ипотечным) кредитам (займам), выданным работникам аккредитованных организаций, осуществляющих деятельность в области информационных технологий, и Правил возмещения кредитным и иным организациям недополученных доходов по жилищным (ипотечным) кредитам (займам), выданным работникам аккредитованных организаций, осуществляющих деятельность в области информационных технологий»
09.05.2022	Постановление Правительства РФ ОТ 9 МАЯ 2022 Г. № 834 «Об установлении особенностей ввоза в Российскую Федерацию шифровальных (криптографических) средств и товаров, их содержащих»
19.05.2022	Распоряжение Правительства РФ от 19 мая 2022 г. № 1235-р О выделении в 2022 г. Минцифры России бюджетных ассигнований из резервного фонда Правительства РФ на предоставление субсидий из федерального бюджета российским кредитным организациям на возмещение недополученных ими доходов по кредитам, выданным системообразующим организациям в сфере информации и связи, относящимся к медиаотрасли, и организациям, входящим в группу лиц системообразующей организации в сфере информации и связи, относящейся к медиаотрасли

Продолжение таблицы Г. 3

1	2
27.05.2022	Постановление Правительства Российской Федерации от 27.05.2022 № 954 «Об утверждении Правил предоставления субсидий из федерального бюджета российским кредитным организациям на возмещение недополученных ими доходов по кредитам, выданным системообразующим организациям в сфере информации и связи, относящимся к медиаотрасли, и организациям, входящим в группу лиц системообразующей организации в сфере информации и связи, относящейся к медиаотрасли»
30.06.2022	Постановление Правительства Российской Федерации от 30.06.2022 № 1177 «О внесении изменений в Правила возмещения кредитным и иным организациям недополученных доходов по жилищным (ипотечным)кредитам (займам), выданным работникам аккредитованных организаций, осуществляющих деятельность в области информационных технологий»
01.07.2022	Постановление Правительства Российской Федерации от 01.07.2022 № 1193 «Об утверждении Правил предоставления из федерального бюджета субсидии на предоставление талантливым школьникам 8 - 11 классов возможности прохождения дополнительного двухлетнего курса обучения современным языкам программирования на базе автономной некоммерческой организации «Университет Национальной технологической инициативы 2035»
22.07.2022	Постановление Правительства Российской Федерации от 22.07.2022 № 1310 «Об утверждении перечня электронной (радиоэлектронной) продукции для целей применения пониженных налоговых ставок по налогу на прибыль организаций и тарифов страховых взносов»
22.07.2022	Правительство Российской Федерации постановление от 22 июля 2022 года № 1311 Об утверждении перечня материалов и технологий для производства электронной компонентной базы (электронных модулей) для целей применения пониженных налоговых ставок по налогу на прибыль организаций и тарифов страховых взносов
13.08.2022	Распоряжение Правительства РФ от 13 августа 2022 г. № 2234-р Об утверждении перечня программ для электронных вычислительных машин, странами происхождения которых являются РФ или другие государства - члены Евразийского экономического союза, которые должны быть предварительно установлены на отдельные виды технически сложных товаров в 2023 г. (с изменениями и дополнениями)
02.09.2022	Распоряжение Правительства Российской Федерации от 02.09.2022 № 2523-р
30.09.2022	Постановление Правительства Российской Федерации от 30.09.2022 № 1729 «Об утверждении Положения о государственной аккредитации российских организаций, осуществляющих деятельность в области информационных технологий»
10.10.2022	Постановление Правительства РФ от 10 октября 2022 г. № 1804 «О проведении эксперимента по предоставлению права использования программ для электронных вычислительных машин, алгоритмов, баз данных и документации к ним, в том числе исключительное право на которые принадлежит Российской Федерации, на условиях открытой лицензии и созданию условий для использования открытого программного обеспечения»
21.10.2022	Распоряжение Правительства Российской Федерации от 21.10.2022 № 3102-р
29.10.2022	Постановление Правительства Российской Федерации от 29.10.2022 № 1934 «О требованиях к адресам электронной почты, используемым государственными органами и органами местного самоуправления»

Продолжение таблицы Г. 3

1	2
08.11.2022	Распоряжение Правительства Российской Федерации от 08.11.2022 № 3363-р
08.11.2022	Постановление Правительства Российской Федерации от 08.11.2022 № 2006 «О внесении изменений в постановление Правительства Российской Федерации от 18 ноября 2020 г. № 1867»
22.12.2022	Распоряжение Правительства РФ от 22.12.2022 № 4088-р «Об утверждении Концепции формирования и развития культуры информационной безопасности граждан Российской Федерации»
28.12.2022	Постановление Правительства Российской Федерации от 28.12.2022 № 2461 «О внесении изменений в постановление Правительства Российской Федерации от 16 ноября 2015 г. № 1236 и признании утратившими силу отдельных положений некоторых актов Правительства Российской Федерации»
23.01.2023	Постановление Правительства Российской Федерации от 23.01.2023 № 72 «О внесении изменений в постановление Правительства Российской Федерации от 30 апреля 2022 г. № 805»
30.01.2023	Постановление Правительства Российской Федерации от 30.01.2023 № 127 «О внесении изменений в постановление Правительства Российской Федерации от 18 марта 2022 г. № 407»
22.02.2023	Постановление Правительства Российской Федерации от 22.02.2023 № 296 «О внесении изменений в Положение о государственной аккредитации российских организаций, осуществляющих деятельность в области информационных технологий»
28.04.2023	Распоряжение Правительства РФ от 28.04.2023 № 1105-р «Об утверждении Концепции информационной безопасности детей в Российской Федерации и признании утратившим силу Распоряжения Правительства РФ от 02.12.2015 № 2471-р»
06.05.2023	Постановление Правительства Российской Федерации от 06.05.2023 № 707 «О внесении изменений в Правила предоставления из федерального бюджета субсидий в целях обеспечения льготного кредитования проектов по цифровой трансформации, реализуемых на основе российских решений в сфере информационных технологий, и признании утратившими силу отдельных положений некоторых актов Правительства Российской Федерации»
06.05.2023	Постановление Правительства РФ от 05.12.2019 № 1598 (ред. от 06.05.2023) «Об утверждении Правил предоставления из федерального бюджета субсидий в целях обеспечения льготного кредитования проектов по цифровой трансформации, реализуемых на основе российских решений в сфере информационных технологий»
06.05.2023	Постановление Правительства РФ от 06.05.2023 № 707 «О внесении изменений в Правила предоставления из федерального бюджета субсидий в целях обеспечения льготного кредитования проектов по цифровой трансформации, реализуемых на основе российских решений в сфере информационных технологий, и признании утратившими силу отдельных положений некоторых актов Правительства Российской Федерации»
20.05.2023	Распоряжение Правительства РФ от 20.05.2023 № 1315-р «Об утверждении Концепции технологического развития на период до 2030 года>« (вместе с «Концепцией технологического развития на период до 2030 года»)
11.07.2023	Распоряжение Правительства РФ от 11.07.2023 № 1856-р «Об утверждении Концепции регулирования отрасли квантовых коммуникаций в Российской Федерации до 2030 года»

Продолжение таблицы Г. 3

1	2
01.08.2023	Распоряжение Правительства РФ от 1 августа 2023 г. № 2063-р О перечне программ для электронных вычислительных машин, странами происхождения которых являются РФ или другие государства - члены Евразийского экономического союза, которые должны быть предварительно установлены на отдельные виды технически сложных товаров в 2024 г.
08.08.2023	Постановление Правительства РФ от 08.08.2023 № 1295 «О внесении изменений в Правила предоставления субсидий из федерального бюджета кредитным организациям на возмещение недополученных доходов по кредитам, выданным на приобретение приоритетной для импорта продукции»
10.08.2023	Распоряжение Правительства Российской Федерации от 10.08.2023 № 2170-р
10.08.2023	Распоряжение Правительства РФ от 10 августа 2023 года №2170-р
31.08.2023	Постановление Правительства Российской Федерации от 31.08.2023 № 1411 «О внесении изменений в некоторые акты Правительства Российской Федерации и о приостановлении действия отдельных положений некоторых актов Правительства Российской Федерации по вопросам жилищного (ипотечного) кредитования граждан Российской Федерации»
31.08.2023	Постановление Правительства РФ ОТ 31 АВГУСТА 2023 Г. № 1411 «О внесении изменений в некоторые акты Правительства Российской Федерации и о приостановлении действия отдельных положений некоторых актов Правительства Российской Федерации по вопросам жилищного (ипотечного) кредитования граждан Российской Федерации»

Источник: составлено автором.

Таблица Г. 4 – Администрация Президента Российской Федерации, Нормативные правовые акты в сфере ИТ

Дата опубликования	Полное название документа
1	2
04.11.2020	Указ Президента Российской Федерации от 04.11.2020 г. № 668 О внесении изменений в состав Комиссии при Президенте Российской Федерации по вопросам развития авиации общего назначения и навигационно-информационных технологий на основе глобальной навигационной спутниковой системы ГЛОНАСС, утвержденный Указом Президента Российской Федерации от 10 февраля 2018 г. № 65
12.04.2021	Указ Президента Российской Федерации от 12.04.2021 г. № 213 Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности
17.05.2021	Указ Президента Российской Федерации от 17.05.2021 г. № 278 О признании утратившими силу пунктов 20 и 21 состава Межведомственной комиссии Совета Безопасности Российской Федерации по информационной безопасности по должностям, утвержденного Указом Президента Российской Федерации от 10 ноября 2018 г. № 64817 мая 2021 года
02.03.2022	Указ Президента Российской Федерации от 02.03.2022 г. № 83 О мерах по обеспечению ускоренного развития отрасли информационных технологий в Российской Федерации2 марта 2022 года

Продолжение таблицы Г. 4

1	2
30.03.2022	Указ Президента Российской Федерации от 30.03.2022 г. № 166 О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации
14.04.2022	Межведомственная комиссия СБ РФ по вопросам обеспечения технологического суверенитета Указ Президента РФ от 14.04.2022 № 203 «О Межведомственной комиссии Совета Безопасности Российской Федерации по вопросам обеспечения технологического суверенитета государства в сфере развития критической информационной инфраструктуры Российской Федерации» (вместе с «Положением о Межведомственной комиссии Совета Безопасности Российской Федерации по вопросам обеспечения технологического суверенитета государства в сфере развития критической информационной инфраструктуры Российской Федерации»)
01.05.2022	Указ Президента Российской Федерации от 01.05.2022 г. № 250 О дополнительных мерах по обеспечению информационной безопасности Российской Федерации 1 мая 2022 года
16.08.2023	Указ Президента Российской Федерации от 16.08.2023 г. № 612 О внесении изменений в Положение об Управлении Президента Российской Федерации по развитию информационно-коммуникационных технологий и инфраструктуры связи, утвержденное Указом Президента Российской Федерации от 14 июня 2018 г. № 33416 августа 2023 года
04.09.2023	Указ Президента РФ от 4 сентября 2023 г. № 660 «О внесении изменений в Положение о порядке рассмотрения вопросов гражданства Российской Федерации, утвержденное Указом Президента Российской Федерации от 14 ноября 2002 г. № 1325, и в Указ Президента Российской Федерации от 2 марта 2022 г. № 83 «О мерах по обеспечению ускоренного развития отрасли информационных технологий в Российской Федерации»

Источник: составлено автором.

Таблица Г. 5 – Федеральная служба безопасности Российской Федерации, Нормативные правовые акты в сфере ИТ

Дата	Полное название документа
1	2
24.10.2022	Приказ Федеральной службы безопасности Российской Федерации от 24.10.2022 № 524 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, с использованием шифровальных (криптографических) средств»
29.03.2023	Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, Федеральной службы безопасности Российской Федерации от 29.03.2023 № 321/147 «Об утверждении Типовых требований к плану мероприятий по внедрению собственниками или иными владельцами технологических сетей связи, имеющих уникальный идентификатор совокупности средств связи и иных технических средств в информационно-телекоммуникационной сети «Интернет», технических средств, обеспечивающих выполнение установленных действий при проведении оперативно-разыскных мероприятий»

Продолжение таблицы Г. 5

1	2
11.05.2023	Приказ ФСБ России от 11 мая 2023 г. № 213 «Об утверждении порядка осуществления мониторинга защищенности информационных ресурсов, принадлежащих федеральным органам исполнительной власти, высшим исполнительным органам государственной власти субъектов Российской Федерации, государственным фондам, государственным корпорациям (компаниям), иным организациям, созданным на основании федеральных законов, стратегическим предприятиям, стратегическим акционерным обществам и системообразующим организациям российской экономики, юридическим лицам, являющимся субъектами критической информационной инфраструктуры Российской Федерации либо используемых ими»
31.01.2022	Приказ ФСБ России от 31.01.2022 № 35 «Об утверждении форм документов, используемых Федеральной службой безопасности Российской Федерации в процессе лицензирования в соответствии с Федеральным законом от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности»
25.03.2023	Приказ ФСБ России от 25.03.2023 № 142 «Об установлении сроков и последовательности административных процедур при осуществлении органами федеральной службы безопасности лицензионного контроля за видами деятельности, предусмотренными пунктами 1 — 3 и пунктом 4 (в пределах компетенции ФСБ России) части 1 статьи 12 Федерального закона от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности»

Источник: составлено автором.

Таблица Г. 6 – Федеральная служба по техническому и экспортному контролю Российской Федерации, Нормативные правовые акты в сфере ИТ

Дата	Полное название документа
1	2
28.12.2021	Приказ ФСТЭК России от 28.12.2021 № 206 «Об утверждении формы оценочного листа, в соответствии с которым ФСТЭК России проводит оценку соответствия соискателя лицензии или лицензиата лицензионным требованиям при осуществлении деятельности по технической защите конфиденциальной информации»
28.12.2021	Приказ ФСТЭК России от 28.12.2021 № 207 «Об утверждении формы оценочного листа, в соответствии с которым ФСТЭК России проводит оценку соответствия соискателя лицензии или лицензиата лицензионным требованиям при осуществлении деятельности по разработке и производству средств защиты конфиденциальной информации»
20.12.2022	Приказ ФСТЭК России от 20.12.2022 № 226 «Об утверждении Программы профилактики нарушений обязательных требований, соблюдение которых оценивается при проведении ФСТЭК России мероприятий по контролю в рамках государственного контроля за соблюдением лицензионных требований при осуществлении деятельности по технической защите конфиденциальной информации и деятельности по разработке и производству средств защиты конфиденциальной информации, на 2023 год“
12.01.2023	Приказ ФСТЭК России от 12.01.2023 № 3 «Об утверждении форм документов, используемых Федеральной службой по техническому и экспортному контролю в процессе лицензирования деятельности по технической защите конфиденциальной информации, и признании утратившими силу приказа ФСТЭК России от 17 июля 2017 г. № 134 и внесенных в него изменений»

Продолжение таблицы Г. 6

1	2
12.01.2023	Приказ ФСТЭК России от 12.01.2023 № 4 «Об утверждении форм документов, используемых Федеральной службой по техническому и экспортному контролю в процессе лицензирования деятельности по разработке и производству средств защиты конфиденциальной информации, и признании утратившими силу приказа ФСТЭК России от 17 июля 2017 г. № 133 и внесенных в него изменений»

Источник: составлено автором.

Таблица Г. 7 – Министерство труда и социальной защиты Российской Федерации, Нормативные правовые акты в сфере ИТ

Дата опубликования	Полное название документа
09.07.2021	Приказ Минтруда России от 09.07.2021 № 462н «Об утверждении профессионального стандарта «Специалист по моделированию, сбору и анализу данных цифрового следа»
09.08.2021	Приказ Минтруда России от 09.08.2022 № 474н „Об утверждении профессионального стандарта «Специалист по технической защите информации»
14.09.2022	Приказ Минтруда России от 14.09.2022 № 525н «Об утверждении профессионального стандарта «Специалист по защите информации в автоматизированных системах»
14.09.2022	Приказ Минтруда России от 14.09.2022 № 533н «Об утверждении профессионального стандарта «Специалист по безопасности компьютерных систем и сетей»
14.09.2022	Приказ Минтруда России от 14.09.2022 № 536н «Об утверждении профессионального стандарта «Специалист по защите информации в телекоммуникационных системах и сетях»
03.10.2022	Приказ Минтруда России от 03.10.2022 № 609н «Об утверждении профессионального стандарта «Технический писатель (специалист по технической документации в области информационных технологий)»
28.11.2022	Приказ Минтруда России от 28.11.2022 № 739н «Об утверждении профессионального стандарта «Специалист по информационной безопасности в кредитно-финансовой сфере»
13.07.2023	Приказ Минтруда России от 13.07.2023 № 586н „Об утверждении профессионального стандарта «Специалист по информационным системам»

Источник: составлено автором.

Таблица Г. 8 – Министерство финансов Российской Федерации, Нормативные правовые акты в сфере ИТ

Дата опубликования	Полное название документа
1	2
24.08.2020	Письмо Минфина от 24.08. 2020 г. № 03-03- 07/74034
28.09.2020	Письма Минфина от 28.09.2020 г. № 03-03-10/84983
07.10.2020	Письма Минфина от 07.10. 2020 г. № 03-15-06/87608;
14.10.2020	Письмо Минфина от 14.10.2020 г. № 03-15-06/89541
16.10.2020	Письмо Минфина от 16.10.2020 г. № 03-15-06/90559

Продолжение таблицы Г. 8

1	2
21.10.2020	Письмо Министерства финансов РФ №03-15-06/91378 от 21.10.2020
21.10.2020	Письмо Минфина от 21.10.2020 г. № 03-15-06/91378
02.11.2020	Письма Минфина от 02.11.2020 г. № 03-15-06/95223
23.11.2020	Письмо Минфина РФ в письме от 23.11.2020 № 03-03-06/1/101948
07.12.2020	Письма Минфина от 07.12.2020 г. № 03-15-06/106519
10.12.2020	Письмо Минфина от 10.12.2020 г. № 03-03-10/108118
21.12.2020	Письмо Минфина от 21.12.2020 г. № 03-15-06/112636
22.12.2020	Письма Минфинаот 22.12.2020 г. № 03-01-10/112733
22.12.2020	Письма Минфинаот 22.12.2020 г. № 03-01-10/112704
24.12.2020	Письма Минфина от 24.12. 2020 г. № 03-15-06/114550
30.12.2020	Письма Минфина от 30.12. 2020 г. № 03-03-06/1/116093
03.02.2021	Письмо Минфина от 03.02. 2021 г. № 03-15-06/6834
17.02.2021	Письмо Минфина от 17.02.2021 г. № 03-15-06/10863
20.02.2021	Письма Минфина от 20.02.2021 г. № 03-15-06/12206;
25.02.2021	Письмо Минфина РФ от 25.02.2021 № 03-15-06/13084
11.03.2021	Минфина от 11.03.2021 г. № 03-15-06/17163
08.04.2021	Письмо Минфина от 08.04.2021 г. № 03-03-06/1/26170
19.04.2021	Письма Минфина от 19.04. 2021 г. № 03-15-06/29109
20.05.2021	Письма Минфина от 20.05. 2021 г. № 03-03-06/1/38715
29.10.2021	Письмо Минфина от 29.10.2021 № 03-03-06/1/87677
25.01.2022	Письмо Минфина РФ от 25.01.2022 № 03-15-07/4849.
22.03.2022	Письмо Минфина от 22.03.2022 № 03-03-06/1/22054
01.12.2022	Письмо Минфин от 01.12.2022 № 03-15-05/117730
22.12.2022	Письма Минфина от 22.12. 2022 г. № 03-03-05/12746
01.03.2023	Письмо Минфина России от 01.03.2023 № 03-03-06/1/17004

Источник: составлено автором.

Таблица Г. 9 – Федеральная налоговая служба Российской Федерации, Нормативные правовые акты в сфере ИТ

Дата опубликования	Полное название документа
1	2
27.11.2020	Письмо ФНС России от 27.11.2020 г. № СД-4-3/19545
25.12.2020	Письмо ФНС РФ от 25.12. 2020 г. № КВ-4-3/21367
21.01.2021	Письмо ФНС России от 21.01. 2021 г. № СД-4-2/561
27.01.2021	Письмо ФНС России от 27.01.2021 г. № СД-4-3/877
20.02.2021	Письмо ФНС России от 20.02.2021 г. № СД-4-3/2249
01.03.2021	Письмо ФНС России от 01.03. 2021 г. № СД-4-3/2495
09.04.2021	Письмо ФНС России от 09.04.2021 г. № СД-19-3/174
09.04.2021	Письмо ФНС России от 09.04.2021 г. № СД-19-3/173
04.08.2021	Письмо ФНС от 04.08.2021 №СД-4- 11/11036@
26.12.2021	Письмо ФНС России от 26.12.2021 г. № СД-4-3/2475
01.03.2022	Письмо ФНС России от 01.03.2022 г. № БС-4-11/2441@
17.03.2022	Письмо ФНС от 17.03.2022 №СД-4-2/3289@

Продолжение таблицы Г. 9

24.03.2022	<Письмо> ФНС России от 24.03.2022 № СД-4-2/3586@ «О назначении ВНП в отношении аккредитованных IT-организаций» (вместе с <Письмом> Минфина России от 18.03.2022 № 03-02-06/21331)
04.05.2022	Письмо ФНС от 04.05.2022 № ЕА-4-15/5416@
04.05.2022	Письмо ФНС от 04.05.2022 № ЕА-4-15/5416@
25.01.2023	<Письмо> ФНС России от 25.01.2023 № СД-4-3/763@ «О применении ставки 0% по налогу на прибыль организациями, осуществляющими деятельность в области информационных технологий»
22.02.2023	Письмо ФНС России от 22.02.2023 № СД-26-3/3@ <О налоговых льготах, предоставляемых при приобретении и внедрении передовых отечественных информационно-телекоммуникационных технологий>

Источник: составлено автором.

Таблица Г. 10 - Государственная дума Российской Федерации, Нормативные правовые акты в сфере ИТ

Дата опубликования	Полное название документа
1	2
31.07.2020	Федеральный закон «О внесении изменений в часть вторую Налогового кодекса Российской Федерации» от 31.07.2020 № 265-ФЗ
31.07.2020	Федеральный закон от 31 июля 2020 г. № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации»
26.03.2022	Федеральный закон от 26.03.2022 г. № 67-ФЗ «О внесении изменений в части первую и вторую Налогового кодекса Российской Федерации и статью 2 Федерального закона «О внесении изменений в часть вторую Налогового кодекса Российской Федерации».
28.06.2022	Федеральный закон «О внесении изменений в Федеральный закон «О правовом положении иностранных граждан в Российской Федерации» от 28.06.2022 № 207-ФЗ
14.07.2022	Федеральный закон «О внесении изменений в часть вторую Налогового кодекса Российской Федерации» от 14.07.2022 № 321-ФЗ
14.07.2022	Федеральный закон «О внесении изменений в часть вторую Налогового кодекса Российской Федерации» от 14.07.2022 № 323-ФЗ
14.07.2022	Федеральный закон от 14.07.2022 г. № 270-ФЗ О внесении изменений в Федеральный закон «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» и статью 10 Федерального закона «Об обеспечении доступа к информации о деятельности судов в Российской Федерации»

Продолжение таблицы Г. 10

1	2
14.07.2022	Федеральный закон от 14 июля 2022 г. № 266-ФЗ «О внесении изменений в Федеральный закон «О персональных данных", отдельные законодательные акты Российской Федерации и признании утратившей силу части четырнадцатой статьи 30 Федерального закона «О банках и банковской деятельности»
03.07.2023	Приказ Министерства здравоохранения РФ от 3 июля 2023 г. № 340н «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в сферах деятельности, нормативно-правовое регулирование которых осуществляется Министерством здравоохранения Российской Федерации»
04.08.2023	Федеральный Закон От 4 Августа 2023 Г. № 478-Фз «О Развитии Технологических Компаний В Российской Федерации»

Источник: составлено автором.

Таблица Г. 11 – Министерство науки и высшего образования Российской Федерации, Нормативные правовые акты в сфере ИТ

Дата	Полное название документа
06.03.2020	Распоряжение Минобрнауки России от 06.03.2020 № 148-р «Об утверждении результатов конкурсного отбора мероприятий, способствующих реализации инновационных проектов, направленных на создание и развитие производства высокотехнологичной промышленной продукции и (или) инновационных товаров и услуг в соответствии с приоритетными направлениями развития науки, технологий и техники Российской Федерации, на территориях которых расположены муниципальные образования, имеющие статус наукоградов Российской Федерации, проведенного в 2020 году»
11.08.2020	Распоряжение Министерства науки и высшего образования Российской Федерации от 11 августа 2020 г. № 298-р «О внесении изменений в распоряжение Министерства науки и высшего образования Российской Федерации от 6 марта 2020 г. № 148-р «Об утверждении результатов конкурсного отбора мероприятий, способствующих реализации инновационных проектов, направленных на создание и развитие производства высокотехнологичной промышленной продукции и (или) инновационных товаров и услуг в соответствии с приоритетными направлениями развития науки, технологий и техники Российской Федерации, представленных субъектами Российской Федерации, на территориях которых расположены муниципальные образования, имеющие статус наукоградов Российской Федерации, проведенного в 2020 году»
19.10.2020	Приказ Минобрнауки России от 19.10.2020 № 1316 «Об утверждении Порядка разработки дополнительных профессиональных программ, содержащих сведения, составляющие государственную тайну, и дополнительных профессиональных программ в области информационной безопасности» (Зарегистрировано в Минюсте России 02.11.2020 № 60696)
24.02.2021	Приказ Минобрнауки России от 24 февраля 2021 г. № 124 «Об обеспечении работы в государственной информационной системе «Официальный сайт Российской Федерации в информационно-телекоммуникационной сети «Интернет» для размещения информации об осуществлении государственного (муниципального) финансового аудита (контроля) в сфере бюджетных правоотношений»

Продолжение таблицы Г. 11

02.04.2021	Распоряжение Минобрнауки России от 2 апреля 2021 года № 100-р «Об утверждении результатов конкурсного отбора мероприятий, способствующих реализации инновационных проектов, направленных на создание и развитие производства высокотехнологичной промышленной продукции и (или) инновационных товаров и услуг в соответствии с приоритетными направлениями развития науки, технологий и техники Российской Федерации, представленных субъектами Российской Федерации, на территориях которых расположены муниципальные образования, имеющие статус наукоградов Российской Федерации, проведенного в 2021 году»
13.06.2023	Приказ Минобрнауки России от 13.06.2023 № 598 «Об упорядочении обращения со служебной информацией ограниченного распространения в Министерстве науки и высшего образования Российской Федерации и организациях, подведомственных Министерству науки и высшего образования Российской Федерации» (вместе с «Порядком передачи служебной информации ограниченного распространения другим органам и организациям», «Порядком снятия пометки «Для служебного пользования» с носителей информации ограниченного распространения») (Зарегистрировано в Минюсте России 28.08.2023 № 74982)

Источник: составлено автором.

Приложение Д

(информационное)

Данные SWOT-анализа российского сегмента ИТ-компаний

S (Strengths)

- Развита сфера разработки ПО, наличие компаний международного уровня (АО «Цифровые Закупочные Сервисы», АО «Лаборатория Касперского», ООО «Мтс Диджитал», ООО «Озон Технологии», АО «Производственная Фирма «Скб Контур», АО «Гринатом», АО «Позитив Текнолоджиз»);

- Рост общего вклада сферы ИТ в экономику страны, прибыльность сферы (Рост доли ИТ-сферы в ВВП России, которая с 1,32% в 2019 году достигла 1,96% в 2023 году. Объём реализации продуктов собственной разработки и ИТ-услуг с 2019 по 2023 год вырос в 2,5 раза и составил 3,1 трлн рублей.);

- Участие в секторе государственных корпораций, квазигосударственных компаний с финансовым и административным ресурсом (VK Group – 57,3% голосующих акций VK контролирует компания «МФ Технологии», 10% которой принадлежат Ростеху. Эффективная доля государства в компании, таким образом, составляет 5,7%. «Газпром автоматизация»; Госкорпорация «Росатом»; Госкорпорация «Роскосмос»; Госкорпорация «Ростех»; «Ростелеком»);

- Снижение налогов для компаний и облегченный режим проверок (ИТ-компании освободили от проверок и уплаты налога на прибыль – Постановление Правительства РФ от 24.03.2022 №448, Указ Президента РФ от 02.03.2022 №83, Письмо ФНС России от 24.03.2022 №СД-4-2/3586@);

- Дотации и отсрочки от военной службы для специалистов (льготная ипотека - Распоряжение Правительства от 01.04.2022 № 714-р, Постановление Правительства от 30.04.2022 № 805, Постановление Правительства от 30.06.2022 № 1177, Постановление Правительства от 30.09.2022 № 1729, Постановление Правительства от 23.01.2023 № 72, Постановление Правительства от 31.08.2023 № 1411; Постановление Правительства от 09.09.2023 № 1474; отсрочка от призыва – Постановление Правительства РФ от 28 марта 2022 года № 490 «Об утверждении Правил предоставления права на получение отсрочки от призыва на военную службу гражданам Российской Федерации, работающим в аккредитованных организациях, осуществляющих деятельность в области информационных технологий»);

- Повышенный интерес молодежи к карьере в сфере ИТ (в 2023 году на «цифровые кафедры» поступило 280 тыс. человек . В соответствии с исследованием VK Education и Профилум 53% молодежи планируют развиваться в ИТ).

W (Weaknesses)

- Неразвитая сфера производства АО, зависимость от импорта АО (По данным WTO, в 2022 году совокупный стоимостной объем импорта ИТ-оборудования в Россию составил 487,8 млрд рублей. В ИТ-сфере на 2022 компании зависят от иностранного оборудования и программного обеспечения на 94%.)

- Высокая степень зависимости от поддержки иностранного ПО (Проведенный компанией «Р7» опрос 530 российских компаний показал, что 100 из них по-прежнему используют зарубежное ПО. Восьмой пакет санкций Европейского Союза от 6 октября 2022 установил запрет на экспорт услуг по ИТ-консультациям);

- Нехватка специалистов, отток специалистов за рубеж (По оценке РАЭК в период с февраля по май 2022 года Россию покинуло от 50 до 70 тысяч ИТ-специалистов, 1,5% от общего числа работников этой сферы. Из покинувших в 2022 году страну 700 тыс. специалистов только 100 тыс. являются айтишниками. При этом около 80% из них продолжали работать на российские компании из-за рубежа. На конец 2023 года дефицит кадров в сфере составил 500–700 тыс. человек);

- Санкционные трудности в приобретении необходимых комплектующих элементов, технологий, компетенций (уход с российского рынка крупных компаний поставщиков АО и ПО (Cisco, Siemens, IBM и др.)), отключение лицензий, отсутствие обновлений и, как следствие, «баги» и уязвимости систем. Санкции негативно повлияли также на экспорт отечественных ИТ-продуктов за рубеж. Значительная часть зарубежных компаний сферы ИКТ ушла с российского рынка. Восьмой пакет санкций Европейского Союза от 6 октября 2022 установил запрет на экспорт услуг по ИТ-консультациям .

O (Opportunities)

- Рост отечественных компаний на внутреннем рынке в условиях отсутствия иностранных конкурентов и наличии государственных дотаций (В ИТ-сфере России, в соответствии с данными Института статистических исследований и экономики знаний НИУ ВШЭ, заметен позитивный тренд развития в период с 2019 по 2023 год, в который объем реализации собственных разработок ИТ-услуг отечественных компаний вырос в 2,5 раза и достиг 3,1 трлн рублей. Также активно растет доля ИТ-сферы в ВВП России, которая с 2019 года по 2023 год выросла с 1,32% до 1,96%);

- Выход российских компаний на рынки дружественных государств, также подвергшихся санкциям (По данным «Руссофт», в Российской Федерации не менее 4,8

тысяч компаний разработчиков ПО, из которых примерно 3 тысячи имеют опыт внешнеэкономической деятельности);

- Рост ниши импортозамещения в связи с сохранением запрета на иностранные ПО и АО в государственном секторе (6 октября 2022 года Восьмой пакет санкций ЕС установил запрет на экспорт услуг по ИТ-консультациям. В свою очередь, следует указать Постановление Правительства Российской Федерации от 16.11.2015 № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд» (вместе с «Правилами формирования и ведения единого реестра российских программ для электронных вычислительных машин и баз данных и единого реестра программ для электронных вычислительных машин и баз данных из государств - членов Евразийского экономического союза, за исключением Российской Федерации», «Порядком подготовки обоснования невозможности соблюдения запрета на допуск программного обеспечения, происходящего из иностранных государств (за исключением программного обеспечения, включенного в единый реестр программ для электронных вычислительных машин и баз данных из государств - членов Евразийского экономического союза, за исключением Российской Федерации), для целей осуществления закупок для обеспечения государственных и муниципальных нужд»));

- Наличие большого количества рабочих мест, престижность работы в российской сфере ИТ (В соответствии с исследованием hh.ru спрос на ИТ-специалистов в Российской Федерации с сентября 2022 года вырос на 18%);

- Возвращение уехавших специалистов (По данным Минцифры, две трети уехавших в 2022 году специалистов вернулись на территорию России);

- Увеличение количества ИТ специалистов, а также повышение их качества за счет новых образовательных программ (По данным Росстата, количество ИТ-специалистов в отрасли за 2023 год увеличилось на 13% и составило 857 тыс. человек);

- Рост компаний в сфере АО (Благодаря активной государственной поддержке наиболее крупные российские ИТ компании не только продолжают функционировать, но и демонстрируют активный рост. Так, в 2023 году прибыль анализируемых компаний составила 85,2, а в 2024 году - 64,0 миллиарда рублей)

T (Threats)

- Возможность введения новых санкций, присоединение к антироссийским санкциям новых государств, что затрудняет доступ к импортному ПО, АО, комплектующим (16.12.2024 был принят уже Пятнадцатый пакет Санкций Европейского Союза);

- После окончания СВО прекратится государственная поддержка ИТ компаний (все меры поддержки имеют свои ограничения по времени. Так, в отношении аккредитованных ИТ-организаций было приостановлено проведение выездных налоговых проверок до 3 марта 2025 года. Остается под вопросом, какие из введенных мер поддержки будут продлеваться. В частности, доле компаний в сфере АО требуется долговременная поддержка по развитию производства);

- Перенос акцента с импортозамещения на механизм параллельного импорта (Вся продукция компаний, принадлежащих области электроники и бытовой техники, поставляется в Россию по программе параллельного импорта. Это создаёт конкуренцию отечественным производителям. Но при этом российский рынок электроники, бытовой техники восполнил дефицит товаров);

- Захват отечественного рынка компаниями из стран, не поддержавших санкции (Экспорт из Китая в Россию в 2023 году вырос на 46,9%, составив около $110,97 млрд);

- Продолжение оттока специалистов (события 2022 года показали возможность оттока специалистов за рубеж, и хоть с того момента ситуация стабилизировалась, Россия по-прежнему находится в состоянии геополитической напряжённости, которая может обустроить уже существующие или вызвать новые кризисы);

- Экономический кризис и внедрение ИИ снизят спрос на ИТ специалистов, что приведет к падению прибыли зарплат (Развитие генеративного ИИ с большой вероятностью в будущем затронет сферу программирования. По мере того, как эти технологии будут совершенствоваться, спрос на программистов и разработчиков может снизиться, что, вероятно, приведет к снижению среднего уровня их заработной платы в данной области);

- Появление компаний монополистов из-за того, что именно государство является одним из наиболее крупных заказчиков и инвесторов (Мировой рынок программного обеспечения захвачен монополистами, такими как Microsoft, Google, Cisco-Webex, Apple и др. При этом в 2022 году доля госзакупок составляла около 20% оборота сферы ИТ Российской Федерации, что может привести к развитию монополий на территории России);

- Сохранение диспропорции между компаниями производителями ПО и АО (Диспропорции в экономике – это нарушение согласованности и соответствия взаимосвязанных процессов и показателей. Вероятнее всего, даже с учетом роста компаний в сфере АО им в среднесрочной перспективе не удастся достичь уровня разработчиков ПО)

Приложение Е

(информационное)

Данные SWOT-анализа российской политики в сфере ИТ

S (Strengths)

- Выбор курса на максимальное импортозамещение (Приказ Минцифры России от 18.01.2023 № 21 «Об утверждении Методических рекомендаций по переходу на использование российского программного обеспечения, в том числе, на значимых объектах критической информационной инфраструктуры Российской Федерации, и о реализации мер, направленных на ускоренный переход органов государственной власти и организаций на использование российского программного обеспечения в Российской Федерации»; Указ Президента Российской Федерации от 30 марта 2022 года № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации; Постановление Правительства Российской Федерации от 16.11.2015 № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд» (вместе с «Правилами формирования и ведения единого реестра российских программ для электронных вычислительных машин и баз данных и единого реестра программ для электронных вычислительных машин и баз данных из государств - членов Евразийского экономического союза, за исключением Российской Федерации», «Порядком подготовки обоснования невозможности соблюдения запрета на допуск программного обеспечения, происходящего из иностранных государств (за исключением программного обеспечения, включенного в единый реестр программ для электронных вычислительных машин и баз данных из государств - членов Евразийского экономического союза, за исключением Российской Федерации), для целей осуществления закупок для обеспечения государственных и муниципальных нужд»));

- Выделение ресурсов на поддержание устойчивости киберпространства (В 2022 году Правительство России выделило 21,5 млрд рублей на меры поддержки ИТ-сферы. На национальный проект «Цифровая экономика» на 1 января 2025 года было потрачено 3,31 триллиона рублей);

- Финансовое и законодательное обеспечение цифровизации политики, экономики (в декабре 2024 сумма контракта «Ростелеком» по работе над инфраструктурой электронного правительства составила 1,3 млрд руб.);

- Поддержка российских ИТ компаний и ИТ специалистов (Налоговые льготы, льготные кредиты, гранты, стимулирование спроса, льготная ипотека, отсрочка от армии, освобождение от проверок, трудоустройство иностранцев, включение в реестры, аккредитация, ИТ-образование, привлечение финансирования);

- Снижение налоговой нагрузки на ИТ-компании, дотации, льготы сектору (ставка налога на прибыль 0% до 31 декабря 2024 года; 5% – начиная с 2025 года; пониженные ставки при УСН; освобождение от НДС для разработчиков ПО; пониженный тариф страховых взносов – 7,6%; нет проверок госорганов, включая налоговые и валютные; кредиты с пониженной ставкой; другие льготы – гранты, упрощенные госзакупки, упрощенный наем иностранных сотрудников);

- Политическое и экономическое сотрудничество с Китаем (Объем российского рынка трансграничной электронной коммерции в 2020 году составил 440 млрд руб., торговля с Китаем 70% от общего объема трансграничной электронной коммерции . По данным главного таможенного управления Китая, товарооборот с Россией за 2022 год вырос почти на 30%, превысив 190 млрд долларов. «Соглашение между Правительством Российской Федерации и правительством китайской народной республики о сотрудничестве в области обеспечения международной информационной безопасности»).

W (Weaknesses)

- Реактивность политики как ответа на реализовавшиеся риски (Подавляющее количество законов прводились параллельно с мировыми политическими событиями и являлись, в основном, реакцией на них, в частности на СВО. В ИТ-сфере в 2022 году продемонстрировано ухудшение динамики показателей «финансовый результат», «количество конкурсных производств», «инвестиции в основной капитал»);

- Отсутствие единой долгосрочной программы развития и поддержки;

- Отсутствие значимого эффекта от программ развития сферы АО, игнорирование подмены импортозамещения серым импортом (Основным документом программы импортозамещения является Постановление правительства РФ от 15 апреля 2014 года №328 «Об утверждении государственной программы Российской Федерации «Развитие промышленности и повышение ее конкурентоспособности». Хотя данные тенденции появились еще в 2014 году, урон, нанесенный санкциями, продемонстрировал малоэффективность программ);

- Сокращённые налоговые поступления в государственный бюджет от ИТ-компаний (Объем налоговых поступлений от ИТ-компаний в 2021 году составил 87 млрд рублей. 6 февраля 2023 года Минфин России отчитался об исполнении

федерального бюджета в январе 2023 года. По сравнению с январем 2022 года, доходы сократились более, чем на треть, а расходы выросли на две трети).

O (Opportunies)

- Расширение цифровизации всех сфер жизни общества (Россия является одним из мировых лидеров по внедрению цифровизации в повседневную жизнь людей. В России используются сотни электронных разнопрофильных систем, в том числе, банковских приложений и сервисов покупок и общественного транспорта. Электронные системы также регулируют многие вопросы здравоохранения и образования);

- Формирование стабильного пула дружественных стран с возможностью сотрудничества в сфере ИТ (По данным Аналитической записки №54 / 2024 БРИКС, успешно выполняет роль международной переговорной платформы. В частности активно обсуждаются вопросы развития ИКТ и цифровой экономики. Россией в рамках БРИКС создано множество механизмов многостороннего сотрудничества в сфере ИТ);

- Создание и укрепление цифрового суверенитета России (Россия является один из глобальных центров силы в информационном пространстве. Так, Российские компании в сфере информационной безопасности стали лидерами на глобальных рынках (Kaspersky)).

T (Threats)

- Сокращение программ поддержки после окончания СВО (На современном этапе остается под вопросом, какие из введенных мер поддержки будут продлятся. В частности, для компаний в сфере АО требуется долговременная поддержка по развитию производства);

- Уменьшение финансирования и льготирования ИТ сектора из-за бюджетного дефицита (Бюджет РФ в 2024 году исполнен с дефицитом 3,485 трлн руб., около 1,7% ВВП);

- Оптимизация государственной политики импортозамещения для открытия рынка зарубежным акторам (В России 2022–2031 гг. были объявлены десятилетием науки и технологий. Однако геополитические события повлекли за собой ряд недружественных санкций. Эффективность нивелирования последствий санкций зависит от степени зависимости отрасли от импортных ИТ-продуктов. Необходимо определить, какие товары и услуги отечественные компании могут предоставить на современном этапе, а какие возможны только в долгосрочной перспективе. И, как следствие, необходимо понять, какие товары должны поставляться компаниями дружественных государств);

- Отказ от курса на цифровой суверенитет и встраивание в поле киберпространства страны геополитического лидера (Альтернативой создания суверенного сегмента киберпространства на территории одного государства является его создание на

территории союза государств. У Китая данное пространство уже функционирует, и теоретически возможна сначала полная зависимость от китайских компаний, затем переход к их методам регулирования, а затем частичное присоединение к их системе).

Приложение Ж

(информационное)

Данные SWOT-анализа российского сегмента киберпространства

S (Strengths)

- Политический курс на суверенитет национального сегмента киберпространства (Федеральный закон от 01.05.2019 № 90-ФЗ «О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации». В России политика обеспечения цифрового суверенитета ставит во главу угла вопросы информационной безопасности, при этом Россия выступает в роли лидера формирования международного режима в данной области.);

- Финансовое и законодательное обеспечение цифровизации всех сфер общественной жизни (На национальный проект «Цифровая экономика» на 1 января 2025 года было потрачено 3,31 триллиона рублей. В национальный проект «Цифровая экономика Российской Федерации» входят следующие федеральные проекты: «Нормативное регулирование цифровой среды» ; «Кадры для цифровой экономики» ; «Информационная инфраструктура» ; «Информационная безопасность» ; «Цифровые технологии» ; «Цифровое государственное управление» ; «Искусственный интеллект» ; «Обеспечение доступа в Интернет за счет развития спутниковой связи» ; «Развитие кадрового потенциала ИТ-сферы»);

- Участие в секторе государственных корпораций, квазигосударственных компаний с финансовым и административным ресурсом (VK Group – 57,3% голосующих акций VK контролирует компания «МФ Технологии», 10% которой принадлежат Ростеху. Эффективная доля государства в компании, таким образом, составляет 5,7%. «Газпром автоматизация»; Госкорпорация «Росатом»; Госкорпорация «Роскосмос»; Госкорпорация «Ростех»; «Ростелеком»);

- Относительно высокий уровень развития в сфере разработки ПО (АО «Цифровые Закупочные Сервисы», АО «Лаборатория Касперского", ООО «Мтс Диджитал», ООО «Озон Технологии», АО «Производственная Фирма «Скб Контур», АО «Гринатом», АО «Позитив Текнолоджиз»);

- Политико-экономическое сотрудничество с Китаем как страной производителем дефицитной продукции ИТ сектора. Объем российского рынка трансграничной электронной коммерции в 2020 году составил 440 млрд руб., торговля с Китаем – 70% от общего объема трансграничной электронной коммерции. По данным главного

таможенного управления Китая, товарооборот с Россией за 2022 год вырос почти на 30%, превысив 190 млрд долларов. «Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности».

W (Weaknesses)

- Преимущественно реактивный характер государственной политики; (Подавляющее количество законов проводились параллельно с мировыми политическими событиями и являлись, в основном, реакцией на них, в частности на СВО. В ИТ-сфере в 2022 году продемонстрировано ухудшение динамики показателей «финансовый результат», «количество конкурсных производств», «инвестиции в основной капитал»);

- Высокий уровень серого и черного импорта, использования нелицензионной продукции как результат недостаточного импортозамещения (На 2024 год на объектах КИИ доля иностранного ПО составляет от 30 до 40%. Только 15–20% госкомпаний успевали заменить иностранное ПО на отечественное до конца 2024 года. Если учесть, что импортозамещение стартовало в 2014 году, показатели слабые. Из-за неэффективности систем параллельного импорта происходит их сокращение. За 2023 год было завезено всего 2 млн ноутбуков посредством параллельного импорта, что на 41% меньше, чем по итогам 2022 года);

- Недостаток ИТ специалистов (По оценке РАЭК, в период с февраля по май 2022 года Россию покинуло от 50 до 70 тысяч ИТ-специалистов, 1,5% от общего числа работников этой сферы. Из покинувших в 2022 году страну 700 тыс. специалистов только 100 тыс. являются айтишниками. При этом около 80% из них продолжали работать на российские компании из-за рубежа. На конец 2023 года дефицит кадров в сфере составил 500–700 тыс. человек);

- Технологическое отставание российского АО от иностранных аналогов (Отставание заметно в сфере микроэлектроники. В 2022 году передовые отечественные производители микроэлектроники осваивали технологии уровня 65 нм на пластинах 200 мм, а в развитых странах уже применяется технология уровня 16 нм на пластинах до 300 мм, и начата разработка уровня 10-7 нм и переход на пластины размером 450 мм);

- Прямые и косвенные санкционные ограничения затрудняют или блокируют доступ к технологиям, элементам материально-технической базы ИТ сектора. (Уход с российского рынка крупных компаний поставщиков АО и ПО (Cisco, Siemens, IBM и др.), отключение лицензий, отсутствие обновлений и, как следствие, «баги» и уязвимости систем. Санкции негативно повлияли также на экспорт отечественных ИТ-продуктов за рубеж. Значительная часть зарубежных компаний сферы ИКТ ушла с российского рынка.

Восьмой пакет санкций Европейского Союза от 6 октября 2022 г. установил запрет на экспорт услуг по ИТ-консультациям)

O (Opportunities)

- Рост запроса политических, экономических акторов, граждан России на трансформацию киберпространства в формат максимально автономного национального сегмента как составной части государственного суверенитета (Россия не только формирует международно-политическую составляющую суверенитета киберпространства, но и активно формирует собственные цифровые границы. Политика, направленная на развитие российского программного и аппаратного обеспечения с целью снижения зависимости от зарубежных технологий, является основным направлением в условиях санкций);

- Рост доли ИТ-сектора в экономике страны в связи с ростом спроса на товары услуги сектора со стороны всех сфер общества (Рост доли ИТ-сферы в ВВП России, которая с 1,32% в 2019 году достигла 1,96% в 2023 году. Объём реализации продуктов собственной разработки и ИТ-услуг с 2019 год по 2023 год вырос в 2,5 раза и составил 3,1 трлн рублей. Ускоренное внедрение цифровых технологий в экономике и социальной сфере создаст условия для бизнеса);

- Увеличение и углубление связей с постсоветскими дружественными странами, и расширение российской экосистемы ИТ-коммуникаций (Несмотря на сильное санкционное давление, существуют широкие возможности для осуществления внешнеполитической деятельности в области ИТ. В первую очередь, это касается развития и укрепления связей с дружественными государствами – Китаем, Республикой Белорусь, Индией, Кубой, Арменией);

- Выстраивание сотрудничества с дружественными странами для получения технологий и дефицитной продукции ИТ сектора (С учетом текущей геополитической ситуации наиболее приоритетными направлениями для экспорта ИТ являются страны ЕАЭС, БРИКС, страны Латинской Америки, Ближнего Востока, Африки и Юго-Восточной Азии).

T (Threats)

- В среднесрочном периоде подменить реальное импортозамещение, особенно в сфере АО, серым и черным импортом (Продукция ИТ-компаний из недружественных стран поставляется в Россию по программе параллельного импорта, что создает проблемы отечественным производителям);

- Расширение пула стран, поддержавших санкции, что затруднит или блокирует получение технологий и дефицитных товаров ИТ сектора (16.12.2024 был принят уже Пятнадцатый пакет Санкций Европейского Союза);

- Открытие российского рынка крупным зарубежным акторам из дружественных стран (Россия активно развивет сотрудничество с партнерами из стран БРИКС. Множество компаний из Китая, Индии, Бразилии и других дружественных стран вышли на российский рынок или значительно усилили свое присутствие);

- Отказ от курса на цифровой суверенитет и встраивание в поле киберпространства страны геополитического лидера (Россия и КНР пытаются использовать многосторонние форумы, чтобы достичь обязывающих международных соглашений о поведении государств в киберпространстве);

- Недостаток квалифицированных кадров в ИТ секторе в связи с релокацией и невысоким уровнем компетенций новых специалистов (По данным Росстата, количество ИТ-специалистов в отрасли за 2023 год увеличилось на 13% и составило 857 тыс. человек);

- Неэффективное или нецелевое расходование бюджетных средств на программы поддержки ИТ сектора (Проблема в том, что люди, принимающие законы о киберпространстве и о поддержке компаний в данной сфере, не всегда достаточно погружены в вопрос и осведомлены об актуальных проблемах данной области, что может вести к ошибкам при распределении бюджетных средств).

Приложение И

(информационное)

Данные матрицы исходов стратегий взаимодействия государства и бизнеса сегмента ПО

- Государство стратегия развития / бизнес стратегия развития – Российский бизнес в сфере ПО обладает значительным потенциалом для роста, а также многие отечественные компании представлены на международном рынке. Уход иностранных компаний дает возможность провести замещение иностранной продукции отечественной и не только в рамках российского рынка, но и рынков дружественных государств, также подверженных санкциям. Для реализации стратегии развития бизнеса ПО требуется активная поддержка со стороны государства. Средства на поддержку развития ПО идут как на привлечение высококлассных специалистов, так и на оплату нового оборудования, что сочетается со стратегией развития со стороны государства, которая также стремится к повышению независимости в технологическом аспекте на международной арене. Взаимовыгодная поддержка бизнеса государством приводит к получению максимального роста прибыли для бизнеса, а также к значительному повышению степени независимости российского сегмента киберпространства.

- Государство стратегия развития / бизнес стратегия выживания – Стратегия выживания для российского бизнеса в сфере ПО позволит сохранить свои позиции в российском сегменте за счет накопленных ресурсов и контроля над значительной частью российского рынка, при любом варианте развития стратегии государства. При этом при стратегии развития у государства – позволит постепенно заместить иностранные компании на российском рынке, но не позволит распространиться активно на рынки дружественных государств. Сочетание данных стратегий приведет к постепенному естественному росту сферы ПО, что не позволит иностранным компаниям занять значительную часть российского рынка, а также к постепенному росту суверенитета киберпространства России.

- Государство стратегия развития / бизнес стратегия зависимости – Стратегия зависимости бизнеса в сфере ПО, а именно восстановление старых связей с иностранными компаниями при государственном курсе на развитие, а, как следствие, замещение иностранной продукции на отечественную невыгодно для бизнеса, так как накладывает серьезные ограничения в поиске иностранных поставщиков продукции и услуг. Может привести к захвату значительной доли российского рынка компаниями из Китая. С одной

стороны, данная система позволит российскому сегменту киберпространства функционировать, но приведёт в той или иной степени к зависимости киберпространства России от иностранных поставщиков;

- Государство стратегия выживания / бизнес стратегия развития – Минимальная поддержка со стороны государства не позволит бизнесу в сфере ПО реализовать весь свой потенциал, но при этом сохранится отсутствие конкуренции внутри страны со стороны бизнеса из стран, поддержавших санкции, что позволит постепенно развивать российский сегмент киберпространства даже без активной государственной поддержки. Но при этом на российский рынок активно будут входить компании из дружественных стран и в основном из Китая, которые составят конкуренцию отечественным разработчикам;

- Государство стратегия выживания / бизнес стратегия выживания – Стратегия выживания позволит сохранить состояние компании, что в сочетании стратегии выживания у государства породит общую ситуацию застоя в сфере ИТ. Бизнес сохранит свои преимущества, связанные с уходом иностранных компаний, но при этом государство не улучшит состояние суверенитета и стабильности киберпространства;

- Государство стратегия выживания / бизнес стратегия зависимости – Позволит бизнесу без противодействия со стороны государства проводить действия по восстановлению международных систем поставок (чему будут противостоять системы санкций, которые не будут отменены без капитуляции российского государства). В свою очередь, данная стратегия не позволит государству повысить степень независимости сегмента киберпространства, но позволит поддержать его функционирование при помощи иностранных компаний, в частности компаний из Китая;

- Государство стратегия зависимости / бизнес стратегия развития – Стратегия развития у бизнеса противоречит стратегии зависимости государства. Отечественным компаниям придётся бороться с вернувшимися иностранными компаниями без государственной поддержки. Но при этом у российского ПО все равно будет преимущество, обусловленное подрывом доверия российского потребителя к иностранным вендерам и уже нарушенными международных системами поставок. Как следствие, понижение степени стабильности российского сегмента киберпространства и незначительное сокращение доли рынка, контролируемого российскими компаниями;

- Государство стратегия зависимости / бизнес стратегия выживания – Стратегия выживания бизнеса позволит сохранить значительную часть российского рынка под контролем российских компаний при возвращении иностранных компаний. Произойдет ухудшение стабильности и независимости киберпространства;

- Государство стратегия зависимости / бизнес стратегия зависимости – Стратегия позволит активно восстановить международные системы поставок. Компании смогут извлечь значительную выгоду при поддержке данных процессов со стороны государства, но при этом все равно не позволит распространить поле своего влияния. В свою очередь, данные стратегии негативно повлияют на стабильность российского сегмента киберпространства за счет перехода к иностранным вендерам, и с высокой вероятностью приведет к вытеснению/слиянию отечественных компаний с международными компаниями.

Приложение К

(информационное)

Данные матрицы исходов взаимодействия государства и бизнеса сегмента АО

- Государство стратегия развития / бизнес стратегия развития – Стратегия развития для бизнеса в сфере АО характеризуется потребностью как в финансовых вложениях, так и в государственной поддержке модификации кластеров производства на территории страны для максимального замещения иностранной продукции, чего требует аналогичная государственная стратегия. Процесс перестройки систем производства невозможно осуществить в краткие сроки, что не позволит оперативно решить потребности сферы ИТ России. Максимальный отказ от иностранной продукции приведет к серьезной ее нехватке из-за неспособности российских компаний все обеспечить, но при этом ведет к их значительным ростам прибылей из-за отсутствия конкуренции;

- Государство стратегия развития / бизнес стратегия выживания – Стратегия выживания, в данном случае умеренного роста, позволит АО постепенно расширяться, наращивая свой технический потенциал и сферы влияния, с другой стороны, государство, применяя стратегию развития сможет активно поддерживать сферу АО как материально, так и с точки зрения ограничения иностранных поставок. В долгосрочной перспективе государство получит развитую сферу АО, а также повышение степени стабильности киберпространства;

- Государство стратегия развития / бизнес стратегия зависимости – Стратегия развития государства противоречит концепции зависимости бизнеса. Государство, поддерживая свой политический курс, который подразумевает сохранение санкционных ограничений, не позволит бизнесу восстановить свои международные связи. В свою очередь, бизнес АО не сможет удовлетворить потребности государственного сегмента киберпространства в оборудовании. Таким образом, данные стратегии приводят к взаимному негативному влиянию;

- Государство стратегия выживания / бизнес стратегия развития – Отсутствие активной поддержки со стороны государства по развитию бизнеса в сфере АО приведет к серьезной нестабильности в сфере АО, а также к возможному сокращению производства отечественного оборудования, но даст частичного его замещение иностранной продукцией из дружественных стран;

- Государство стратегия выживания / бизнес стратегия выживания – Сочетание стратегий выживания позволит бизнесу как сохранить свои позиции на отечественном

рынке, так и развить связи с дружественными государствами, а власти сохранить уровень стабильности в сфере киберпространства;

- Государство стратегия выживания / бизнес стратегия зависимости – Бизнес не сможет активно восстанавливать связи с иностранным бизнесом, а также не сможет получать активные субсидии. Данное сочетание стратегий приведет к потере стабильности российского сегмента киберпространства, а также к частичному переходу его обеспечения посредством АО из Китая;

- Государство стратегия зависимости / бизнес стратегия развития – Приведет к полному провалу бизнеса по развитию своей продукции, в итоге рынок будет взят под контроль вернувшимися иностранными компаниями и будет значительно понижена как сфера влияния бизнеса, так и устойчивость российского сегмента киберпространства;

- Государство стратегия зависимости / бизнес стратегия выживания – Произойдет возвращение иностранных компаний либо приток компаний из дружественных стран, что во многом займет ниши, которые потенциально смогли бы занять российские компании, но стратегия выживания позволит им только сохранить свои позиции. Как результат, нет роста отечественных компаний, и российский сегмент киберпространства продолжит функционировать за счет иностранной продукции;

- Государство стратегия зависимости / бизнес стратегия зависимости – Приведет как к переходу российских компаний под контроль иностранных корпораций, так и значительно понизит степень суверенитета киберпространства.