

*Охрименко С.А., Силаков А.В.,  
Орлова Д.Р., Сенков В.А., Черней В.А.*



## ЭКОНОМИЧЕСКИЕ САНКЦИИ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ



*Монография*

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ  
РОССИЙСКОЙ ФЕДЕРАЦИИ**

---

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ им. А.Н. Косыгина  
(ТЕХНОЛОГИИ. ДИЗАЙН. ИСКУССТВО)»  
(ФГБОУ ВО «РГУ им. А.Н. Косыгина»)**

**Охрименко С.А., Силаков А.В., Орлова Д.Р.,  
Сенков В.А., Черней В.А.**

# **ЭКОНОМИЧЕСКИЕ САНКЦИИ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ**

**Монография**

**Москва – 2024**

УДК 339  
092

Охрименко С.А., Силаков А.В., Орлова Д.Р., Сенков В.А., Черней В.А.  
Экономические санкции в сфере информационных технологий:  
монография – М.: ФГБОУ ВО «РГУ им. А.Н. Косыгина», 2024. – 163 с.

В монографии систематизированы различные аспекты санкций, включая их исторический контекст, текущие тенденции, а также многообразие подходов к оценке их эффективности. Особое внимание уделено анализу современных киберсанкций и их влиянию на международные отношения и глобальную экономику. Содержание данной монографии является логическим продолжением проведенных исследований авторов.

Материал предназначен для широкого круга читателей, включая преподавателей, студентов, аспирантов экономических специальностей, научных сотрудников, работников организаций и предприятий.

#### Рецензенты

*Карп М.В.* - заведующий кафедрой «Бухгалтерского учета, аудита и налогообложения», ФГБОУ ВО «Государственный университет управления», Москва, Россия, профессор, д-р экон. наук;

*Карамова О.В.* - профессор кафедры экономической теории ФГБОУ ВО «Финансовый университет при Правительстве РФ», Москва, Россия, профессор, д-р экон. наук.

ISBN 978-5-00181-656-0

© Федеральное государственное бюджетное образовательное учреждение высшего образования «Российский государственный университет им. А.Н. Косыгина (Технологии. Дизайн. Искусство)», 2024

© Охрименко С.А., Силаков А.В., Орлова Д.Р., Сенков В.А., Черней В.А., 2024

© Обложка. Дизайн. Николаева Н.А., 2024

## СОДЕРЖАНИЕ

Введение .....	4
Глава 1. Литературные источники по проблеме санкций и их эффективности..	7
Глава 2. Анализ исторического развития санкций и их преобразований.....	44
Глава 3. Международные санкции как объект исследований.....	59
Глава 4. Санкции: политический и экономический аспекты.....	72
Глава 5. Особенности санкций в сфере IT.....	92
Глава 6. Анализ рынка печатных плат в РФ.....	134
Выводы.....	160

## ВВЕДЕНИЕ

*«Что было, то и теперь есть, и что будет, то уже было –  
и Бог воззовет прошедшее»* Екклезиаст 3:15-15

Экономические санкции, направленные на ограничение торговли и финансовых операций, часто используются как средство давления на государства для достижения политических целей. Однако их эффективность остается предметом дискуссий среди экспертов. С одной стороны, они могут привести к значительному экономическому ущербу для целевых стран, с другой – вызывать нежелательные гуманитарные последствия и усиление антизападных настроений.

История показывает, что санкции могут иметь разнообразные последствия. Например, санкции, введенные против Югославии в 1990-х годах, или Ирана в начале 2000-х, привели к серьезным экономическим трудностям в этих странах, но не всегда достигли своих политических целей. Важно изучать эти примеры для понимания механизмов и последствий санкционной политики. Перед исследователями стоит задача не только анализировать исторические и современные примеры санкций, но и прогнозировать их будущее развитие. Важно учитывать меняющийся международный ландшафт, развитие технологий и изменение мирового экономического порядка.

Санкции не являются изолированным инструментом, их эффективность и последствия тесно связаны с международными политическими процессами. Взаимодействие санкционной политики с глобальными экономическими и геополитическими тенденциями определяет их реальное влияние на мировую арену.

Санкции, как инструмент международной политики, имеют давние исторические корни. В современном мире санкции стали более сложными и многогранными. В последние десятилетия они приобрели новые измерения в контексте глобализации и развития информационных технологий. Они включают не только традиционные экономические ограничения, но и такие разновидности, как киберсанкции, которые оказывают влияние на информационные системы стран. Эти меры могут варьироваться от хакерских атак на критически важные инфраструктуры до целенаправленных киберкампаний против конкретных лиц или организаций. Технологический аспект санкций приобретает особое значение. Киберсанкции, как инструмент воздействия на информационные системы и технологическую инфраструктуру стран, открывают новые горизонты для политического давления, но также несут в себе риски эскалации конфликтов в киберпространстве.

Оценка эффективности санкций требует комплексного подхода, включая анализ экономических, политических, социальных и технических факторов. Это включает в себя изучение как непосредственных последствий санкций, так и их косвенного влияния на международные отношения, внутреннюю политику и общественное мнение в целевых странах.

В данной работе мы систематизировали различные аспекты изучения санкций, включая их исторический контекст, текущие тенденции, а также многообразие подходов к оценке их эффективности. Особое внимание уделено анализу современных киберсанкций и их влиянию на международные отношения и глобальную экономику. Анализируя многообразие примеров международных санкций, мы поставили цель - исследовать исторический опыт реализации и противостояния санкциям и спрогнозировать будущее развитие этого сложного и многогранного инструмента международных отношений.

Содержание данной монографии является логическим продолжением проведенных исследований авторов и нашедших отражение в следующих работах [ 1-6].

По нашему мнению, монография прежде всего будет интересна исследователям проблем эффективности политических и экономических санкций, экономической безопасности, кибербезопасности. Преподавателям и аспирантам научных специальностей 5.2.3. «Региональная и отраслевая экономика», 5.2.1. «Экономическая теория». Студентам, обучающимся в высших учебных заведениях по УГСН 38.00.00 «Экономика и управление».

## **Литература**

1. Ohrimenco S., Orlova D., Cernei V. Cyber Threats Modeling: An Empirical Study // Business Management/Biznes Upravlenie. – 2023. – №. 3.
2. Охрименко С.А., Черней В.А. Теневая цифровая экономика и её основные сегменты. În: Человеческий капитал в модели устойчивого экономического роста России: Монография / О.В.Карамова, Г.А.Терская, Н.Н.Соловых [и др.]; под науч. Ред. О.В.Карамовой. Г.А.Терской, Н.В.Цхададзе. –М.: Прометей, 2022. -514 с. ISBN 978-5-00172-372-1
3. Охрименко С.А., Орлова Д.Р., Черней В.А. Анализ концепции «этичный хакинг» (на примере платформы HackerOne). În: Государство и рынок: евразийская доминанта развития в условиях формирования многополярного мира: коллективная монография / под ред. д-ра экон. наук, проф. С.А.Дятлова, д-ра экон. наук, Д.Ю. Миропольского, д-ра экон. наук, Т.А. Селищевой. – СПб.: Изд-во СПбГЭУ, 2023. – 2023. – 632 с. ISBN 978-5-7310-6264-0

4. Serghei Ohrimenco, Grigori Borta, Valeriu Cernei. Estimation of the Key Segments of the Cyber Crime Economics. În: 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T). 05-07 October 2021, Kharkiv, Ukraine. (0,5 с.а.) DOI: 10.1109/PICST54195.2021.9772165
5. Охрименко С. А., Орлова Д. Р. Экономические санкции против России в сфере информационных технологий. În: Материалы XI Международного научного конгресса «Новый смысл развития предпринимательства: модель опережения, технологии, кадры». 19-20 мая 2023 года. Москва, Финансовый университет при Правительстве Российской Федерации / под науч. Ред. д.э.н., проф. А.В.Шарковой. – Москва: Издательско-торговая корпорация «Дашков и К», 2023. с. 87-95. (0,25 с.а.). ISBN 978-5-394-05540-9 DOI 10.29030/978-5-394-05540-9-2023
6. Пескова Д.Р., Евсеева О.А. "Санкционированное" развитие российского предпринимательства // Экономика и управление: научно-практический журнал. – 2015. - №3 (125). – С 94-97.

# ГЛАВА 1. ЛИТЕРАТУРНЫЕ ИСТОЧНИКИ ПО ПРОБЛЕМЕ САНКЦИЙ И ИХ ЭФФЕКТИВНОСТИ

Важной задачей исследования является обобщение литературных источников, относящихся к теме изучения проблематики санкций. После предварительного анализа было отобрано свыше 120 работ монографической литературы и несколько, наиболее значимых статей.

Все источники по содержанию были объединены в следующие укрупненные группы:

- 1.1 Исторические аспекты санкций;
- 1.2 Санкции, введенные Советом безопасности ООН;
- 1.3 Санкции в рамках Системы экспортного контроля;
- 1.4 Санкции в области ИТ (киберконфликт, киберсанкции, киберблокады);
- 1.5 Система экономических санкций;
- 1.6 Эффективность санкций;

Рассмотрим содержание приведенных групп. Для каждой группы в скобках приведено количество источников, использованных при написании данной книги. Проанализированы наиболее значимые и интересные, с точки зрения авторов, исследования.

## 1.1. Исторические аспекты санкций (7)

**1. Рональд Сегал «Санкции против Южной Африки» (Ronald Segal (1964). *Sanctions Against South Africa*. Penguin Books. ASIN: B000LDSU2Q).** Книга содержит материалы Международной конференции по экономическим санкциям против Южной Африки, против апартеида. Книга содержит экспертные документы по экономическим, расовым и политическим стратегическим аспектам санкций. На основании этих доказательств эксперты сочли, что были обоснованы необходимость, законность и осуществимость организованных международным сообществом экономических санкций против Южной Африки, политика которой, как считалось, стала прямой угрозой миру и безопасности в Африке и во всем мире.

**2. Питер Ян Кайпер «Реализация международных санкций. Нидерланды и Родезия». (Pieter Jan Kuiper (1974). *The Implementation of International Sanctions: The Netherlands and Rhodesia*. Springer. ISBN 90 286 0888 5).** Книга содержит анализ санкций в муниципальном и международном праве, описаны провал централизованных санкций, а также политика Нидерландов против южноафриканского апартеида, ограничения, введенные Генеральным соглашением по тарифам и торговле, экономическим союзом Бенилюкс, Европейским экономическим сообществом и др.



**3. Салим Ламрани «Экономическая война против Кубы: историко-правовой взгляд на блокаду США». (Salim Lamrani (2013). *The Economic War Against Cuba: A Historical and Legal Perspective on the U.S. Blockade*. Monthly Review Press. ISBN 978-1-58367-341-6).** Книга посвящена анализу более полувековых санкций против Кубы. Показано, что введенные санкции полностью провалились и не достигли основной задачи – свержения кубинского правительства. Автор указывает, что Куба не представляет угрозы США. За время проведения санкционной политики США нормализовали свои отношения с Китаем, Вьетнамом и рядом бывших противников, но упорно отказываются сделать тоже самое с Кубой. Автор исследует комплекс экономических санкций, введенных Президентами США, от Дуайта Эйзенхауэра до Барака Обамы, а также противодействие американского общества экономическим санкциям.

**4. Ирина Богданова, глава «История экономического принуждения: от экономической войны к обеспечению общественных интересов» в книге «Односторонние санкции в международном праве и обеспечение прав человека». (Iryna Bogdanova (2022). In: *Unilateral Sanctions in International Law and the Enforcement of Human Rights*. (2022). Brill | Nijhoff. ISBN: 9789004507890 DOI: [https://doi.org/10.1163/9789004507890\\_003](https://doi.org/10.1163/9789004507890_003)).** Работа начинается с исторического обзора и прекрасного по наполнению анализа экономического принуждения до 20 века. Затем следует обзор экономических санкций и их применения в межвоенный период во времена Лиги Наций. Следующим разделом является материал, содержащий обзор экономических санкций после Второй Мировой Войны, в том числе санкции ООН против Родезии, Южной Африки, «десятилетие санкций» и поиск «умных» санкций. Важным является раздел, содержание которого посвящено рассмотрению войны с терроризмом и целевым действиям СБ ООН после событий 9/11. Следующий раздел посвящен росту использования односторонних экономических санкций и новому геоэкономическому мировому порядку. Второй раздел данной главы содержит описание эффективности экономических санкций, с выделением целей, преследуемых экономическими санкциями, открытости международной торговли и ее влиянию на эффективность экономических санкций, многостороннему сотрудничеству и его влиянию на эффективность экономических санкций, финансовым санкциям как новому рубежу эффективности экономических санкций, стратегии обхода негативных последствий экономических санкций. Автор приводит ссылки на более чем три сотни источников.

**5. Хиба Хафиз «За свободой: к истории и теории экономического принуждения». (Hafiz, Hiba, *Beyond Liberty: Toward a History and Theory of Economic Coercion* (December 11, 2016). *Tennessee Law Review*, Vol. 83, 2016, Available at SSRN: <https://ssrn.com/abstract=2992978> (дата обращения 24.12.2023).** Материал состоит из четырех частей. В первой части «Развитие философских взглядов о принуждении», рассматривается материал о

философских взглядах о принуждении в 19 веке, о принуждении и законе в современной аналитической философии сквозь призму публичного и частного права, а также ограничения философских теорий. Вторая часть объединяет развитие юридических взглядов на принуждение с выделением правового реализма и ограничениями парадигмы юридического реализма. Международные правовые взгляды на экономическое принуждение являются содержанием третьей части: регулирование системного экономического принуждения со стороны государственных субъектов и частных субъектов, а также ограничения международного подхода к правам человека в экономическом принуждении. Заключительная, четвертая часть работы рассматривает теорию и практику экономического принуждения, с выделением теории реляционных прав и измерение защиты от экономического принуждения.

**6. Отчет, подготовленный Евразия Групп Колумбийского университета «Торговое оружие. Исследование современных торговых конфликтов с середины 1900-х годов до настоящего времени». *The Weaponization of Trade. A study of modern trade conflicts from the mid-1900s to present.*** Для получения представления о внедрении, эволюции и развитии торгового оружия в данном отчете проанализированы торговые конфликты с 1940-х годов. Страны используют торговые инструменты в качестве оружия для оказания экономического давления на страны-мишени ради достижения политических целей. В отчете представлены результаты тематических исследований по следующим направлениям: руководство страны как субъект давления, административная и государственная политика, политические и геостратегические цели в сравнении с экономическими проблемами и последствиями для технического развития. При анализе результатов использовались такие индикаторы как: связи внутри альянсов и между ними, симметричные и асимметричные экономические, политические и военные возможности. Была рассмотрена возможность использования торговых инструментов ВТО и ГАТТ. Были определены факторы, которые обеспечивают преимущества для оценки текущих и будущих войн. Авторы представили анализ геополитических событий, таких как взаимоотношения между США и Японией в 40-е годы 20 века, куриная война 1960-х годов, нефтяной кризис 1970-х годов, взаимоотношения США-Япония 1980-х годов, конфликты вокруг природного газа и энергетики 1980-х годов, редкоземельных элементов 2010-х годов. Этот материал дополнен анализом экономических событий: макаронные войны 1980-х годов, текстильный конфликт 1980-х годов, банановая война 1990-х годов, тарифы на сталь 2000-х годов.

**7. Франсиско Родригес «Гуманитарные последствия экономических санкций». (Francisco Rodríguez (2023). *The Human Consequences of Economic Sanctions.* <https://cepr.net/wp-content/uploads/2023/04/FINAL-The-Human-Consequences-of-Economic-Sanctions-Rodriguez-7.pdf>).** Автор приводит результаты тематических исследований по следующим

направлениям: исторический обзор и экономические и социальные последствия для Ирана (1979-2021 г.г.), Афганистана (1999-2021 г.г.), Венесуэлы (2017-2021 г.г.). Представлен материал, позволяющих переосмыслить последствия экономических санкций.

## **1.2. Санкции, введенные Советом безопасности ООН (10)**

**1. Голнуш Хакимдавар «Стратегическое понимание экономических санкций ООН: международные отношения, право и развитие» (Golnoosh Hakimdavar (2014). A Strategic Understanding of UN Economic Sanctions: International Relations, Law, And Development. Routledge. ISBN: 978-0-203-10946-5).** В начале книги приведены высказывания двух представителей американских университетов относительно содержания данной книги. Х.Сабери, из Йорского университета, указывает: «Стратегическое понимание экономических санкций ООН требует поддержки от различных дисциплин для формирования новой оценки формы международного принуждения, реальный вред которой часто затмевается предполагаемыми потенциальными выгодами. Настоящее исследование выходит за рамки дебатов относительно против или в пользу экономических санкций как эффективного инструмента наказания и предполагает пересмотр фундаментальных предпосылок подобных дебатов». Соответственно, Муно Ндуло, из Корнуэльского университета, указывает: «Эта книга представляет собой глубокий и ясный анализ и оценку роли санкций в международной политике. Это важный ресурс для ученых и политиков, заинтересованных в эффективности санкций как политического инструмента, позволяющего изменить поведение государства».

Во введении книги указывается, что после десятилетия санкций, в результате которых погибло более миллиона иракцев, экономические санкции в отношении Ирака были частично отменены 22 мая 2003 года, через два месяца после военного нападения на страну. Возмущение, которое осталось после санкций, привело к расследованию использования санкций в качестве меры принуждения. Достигнутый консенсус заключался в том, что иракские санкции не были эффективными и существует необходимость в новом, более продвинутом виде санкций, который не причинит вреда населению. Таким образом ученые и политики начали вводить новую формулу «целевых санкций» в качестве нового метода борьбы с угрозами миру. Эта новая форма санкций была нацелена на правящую элиту и минимизировала воздействие на население в целом.

В книге последовательно рассматриваются такие вопросы, как ООН и односторонние санкции, СБ ООН и защита мира, реализация санкций и внутренняя политика, реализация санкций и внутренняя политика, реализация от теории к практике, меры успеха и неудачи и политические рекомендации.

В заключении книги автор указывает на растущий интерес к использованию санкций ООН и измерению экономических санкций с привлечением множества дисциплин социальных наук, права, экономики, политологии, международных отношений, бизнеса и т.д. Однако многообразие методологических подходов к оценке санкций не прояснило основные проблемы. Основная цель – переориентировать внимание на цели санкций. Без четкого обозначения цели введения санкций невозможно измерить успех или неудачу эффективного внедрения санкций. То, что когда-то использовалось в форме наказания государств-изгоев, теперь используется в качестве главного оружия против отдельных лиц. Сегодня, как и в прошлые годы, используются те же политически заряженные идеологии и санкции превратились в, прежде всего, политическое явление. Современные политики сталкиваются с новыми проблемами в отношении санкций: глобализация и прогресс в экономических отношениях, контр идеологии, достижения в области науки и технологий, поэтому было бы неразумно полагаться на старые методы и методологии разработки новых схем санкций.

**2. Андреа Чаррон «Санкции ООН и конфликты: реагирование на угрозы миру и безопасности», (Andrea Charron (2011). UN Sanctions and Conflict: Responding to Peace and Security Threats. Routledge. ISBN: 978-0-203-80756-9).** В книге освещаются санкции, введенные Советом Безопасности ООН за 20 лет. Автор сосредоточил внимание на адаптациях и тенденциях, которые получили развитие в данном важном механизме СБ ООН. Проведена документация и интерпретация каждого случая введения санкций, а также связи между ними, а также то, что политика СБ ООН в использовании этих инструментов принуждения обладает и имеет больше содержания и направленности, чем пустые дискуссии в прессе. Андреа Чаррон представляет эмпирическую базу исследований и широкий контекст для поиска ответов на два критических замечания. Во-первых, санкции представляют собой навязывание действий сильными против слабых с учетом невысказанного нюанса – санкции вводятся довольно произвольно. Частью критики автора по отношению к вводимым санкциям является то, что санкции непропорционально часто применяются в странах Африки к югу от Сахары. Во-вторых, санкции просто не работают. Автору удалось продемонстрировать то, что существовали веские причины, по которым СБ действовал посредством санкций в Африке и этот инструмент являлся элементом нового империализма. Содержание книги демонстрирует тот факт, что Африка была местом, где возникли самые большие угрозы миру. Описав случаи введения санкций, а затем проведя сравнительный анализ санкций, введенных в целях контроля над конфликтами и поддержания мира, автор выделяет несколько центральных моментов – СБ всегда сначала вводил эмбарго на поставки оружия, за которыми следовали целевые санкции в отношении субъектов и секторов, а затем эти меры вступали в контакт с другими (иногда успешно, иногда менее успешно). Предоставляя полное описание мер реагирования ООН на угрозы миру, ключевым компонентом которых является санкции,

автор демонстрирует, что санкции были введены как инструмент миротворчества ООН с некоторыми разумными успехами в Африке.

**3. Андреа Чаррон и Клара Портела «Многосторонние санкции: новый взгляд на уроки, извлеченные Маргарет Докси», (Andrea Charron, Clara Portela (2022). Multilateral Sanctions Revisited Lessons Learned from Margaret Doxey. McGill-Queen's University Press. ISBN 978-0-2280-1261-0)**

Произошел возврат санкций, причем с новой силой, новыми целями и мерами, вызовами и возможностями. В книге отмечается, что канадский исследователь Маргарет Докси предвосхитила и проанализировала эти проблемы, заново открыла предыдущие уроки и их результаты применительно к новым практикам, которые формируются в условиях геополитической противоречивой среды. Данная книга написана международной группой, исследует меры ООН, региональные санкции, автономные меры и их взаимосвязь. Опираясь на идеи Маргарет Докси, авторы прослеживают эволюцию научных исследований, относящихся к многосторонним санкциям. Книга состоит из двух разделов. В первом разделе проведен анализ действий различных субъектов, таких как великие державы и региональные организации, применяют многосторонние санкции. Вторая часть книги посвящена применению и последствиям многосторонних санкций, включая нормы, которые они обеспечивают, а также проблеме уклонения от санкций и будущим вызовам, таким как санкции в отношении использования криптовалют.

Международные институты, такие как ООН, редко проводят глубокий и беспристрастный анализ своих прошлых действий. Их устремления и энергия сосредоточены на решении проблем текущего момента. Кроме того, решения о введении санкций зачастую является весьма деликатным вопросом. Пересмотр прошлого может означать возобновление старых дебатов и возрастание напряженности среди членов СБ ООН. Авторы высказывают мысль, суть которой заключается в следующем – они сомневаются в том, что когда-нибудь СБ ООН снова прибегнет к полномасштабным санкциям, наподобие тех, которые он применял к Ираку в конце войны в Персидском заливе, учитывая ужасные последствия и человеческие жертвы. Всесторонний и независимый анализ, результаты которого представлены в этой книге, должны помочь политикам принимать наиболее подходящие решения на основе выводов и практического опыта, сделанных в этой книге.

**4. Сачико Яшимура «Финансовые санкции ООН», (Sachiko Yoshimura (2021). United Nations Financial Sanctions. Routledge. ISBN: 978-0-429-26031-5).** Финансовые санкции используются достаточно давно, со времен Лиги Наций. В начальный период своей деятельности ООН, финансовые санкции рассматривались в качестве дополнения к торговым эмбарго. В книге представлены глубокие взгляды на введение, реализацию и применение одобренных ООН финансовых санкций и связанных с этим вопросов. Эксперты предлагают анализ того, как развивались финансовые санкции ООН, различные роли различных крупных международных игроков в

их согласовании и применении, а также их успехи в достижении желаемых результатов.

В настоящее время важность финансовых санкций многократно возросла, поскольку замораживание активов рассматривается в качестве мощной меры в составе «умных санкций». По сравнению с торговым эмбарго и другими средствами экономического воздействия, финансовые санкции являются уникальными во многих отношениях, например, из-за необходимости участия частного сектора и сложных методов реализации. Что касается односторонних и других типов финансовых санкций, в книге анализируются финансовые санкции, принятые ООН. Книга начинается с описания и истории ООН и финансовых санкций, а также «умных санкций». Затем проводится анализ сферы реализации с акцентом на крупнейшие мировые экономики (Япония, США, и ЕС). Представлены тематические исследования финансовых санкций ООН против Северной Кореи и Ирана.

**5. Джереми Мэтам Фаролл «Санкции ООН и верховенство закона». (Jeremy Matam Farrall (2007). United Nations Sanctions and the Rule of Law. Cambridge University Press. ISBN-13 978-0-511-37729-7).** Книга преследует две основные цели – описать эволюцию санкций ООН и изучить взаимосвязь между санкциями и верховенством закона. Практическая цель книги – продвигать политические предложения по улучшению соблюдения принципа верховенства права при выполнении санкций ООН. Автор описывает процесс введения санкций ООН и прагматическую модель верховенства права для этих санкций. Приведена эволюция санкций ООН с выделением предыстории санкций. Значительный объем книги посвящен реализации санкций ООН на практике, в том числе: установление правовой основы для санкций, выявление угроз, определение сферы санкций и определение целей, постановка целей, применение временных ограничений и минимизация негативных последствий, делегирование ответственности за санкции. Автор выявляет слабые стороны верховенства права в системе санкций ООН и определяет укрепление верховенства закона в санкционной системе. Интересными по содержанию являются приложения, в которых приведено краткое изложение политических рекомендаций и режимов санкций.

**6. Микаэль Эрикссон «Нацеленность на мир: понимание целевых санкций ООН и ЕС». (Mikael Eriksson (2011). Targeting Peace : Understanding UN and EU Targeted Sanctions. Routledge. ISBN 9781409419327).** Материал книги содержит описание нацеленности санкций на мир, переосмысление целевых санкций, оценку санкций в сфере нефтепереработки, тенденции в адресных санкциях ООН и ЕС, их принятие, восприятие и сложность, эпизоды целевых санкций ООН против УНИТА, принятие решений по санкциям ЕС, эпизоды целевых санкций против руководства Зимбабве и переосмысление санкций. Представляют интерес приложения, в которых описано введение в действие и определение целевых санкций и эпизоды санкционного режима по отношению к Белоруссии,

бывшей Югославской Республике Македония, Сербии и Черногории, Молдовы (Транснистрия), Ирак, Иран, Сиерра-Леоне, Либерии, Кот-д'Ивуар, Демократической Республики Конго, Судан, Зимбабве, Узбекистан, Бирма.

**7. «Целевые санкции: последствия и эффективность действий Организации Объединенных Наций Targeted Sanctions: The Impacts and Effectiveness of United Nations Action / Edited by Thomas J. Biersteker, Sue E. Eckert, Marcos Tourinho. New York: Cambridge University Press, 2016. ISBN 978-1-107-59309-1).** Коллектив авторов последовательно описывает цели адресных санкций ООН, их динамику и дизайн, а также другие инструменты политики – дипломатию, юриспруденцию, применение силы. Исследуются такие вопросы, как взаимосвязь между санкциями ООН и региональными режимами, координация санкций ООН с другими субъектами и инструментами, непредвиденные последствия действий санкций ООН, эффективность адресных санкций ООН и институциональное обучение в области введения санкций.

**8. Дэвид Кортрайт, Джордж А. Лопес, Линда Гербер «Санкции и поиск безопасности: вызовы действиям ООН». (David Cortright, George A. Lopez, Linda Gerber (2002). Sanctions and the Search for Security: Challenges to UN Action. Lynne Rienner Publishers, Inc. ISBN 1-58826-078-X).** Авторы обозначили цель данной книги как изложение общих выводов о типах санкций, которые кажутся эффективными или неэффективными, а также стратегий, необходимых для повышения эффективности действий ООН с помощью данного инструмента. Последовательно представлен материал, характеризующий основные тенденции санкций, описание санкций для Ирака, «умные» санкции и их ограниченное воздействие в Афганистане, эволюция санкций ООН в Анголе, санкции и кризис в Западной Африке, целевые финансовые санкции, борьба с терроризмом, комплекс санкций в отношении путешествий и авиации, эмбарго на поставки оружия, жизнеспособность сырьевых санкций и будущее санкционной политики ООН. Таким образом, основные темы исследования включили следующие: разработка эффективных инноваций и введение более целенаправленных и избирательных санкций, резкое усиление контроля за соблюдением санкций посредством использования независимых следственных комиссий и группы экспертов, устранение двусмысленности и несоответствия между теорией санкций и их реализацией, изменяющийся характер целей и условий санкций, трудности, связанные с наложением санкций на объект при условии, что экономика объекта пострадала от дезинтеграции, теневой экономики и криминализации. Отдельным пунктом выступает положение о росте известности неправительственных организаций (НПО) в качестве внешних критиков, наблюдателей за санкциями в процессе реформирования санкционной политики.

**9. Лариса ван ден Херик «Справочник по исследованиям санкций ООН и международного права». (Larissa van den Herik (2017). Research Handbook on UN Sanctions and International Law. Edward Elgar Publishing**

**Limited. ISBN 978 1 78471 303 4 DOI 10.4337/9781784713034).** В этом исследовательском справочнике рассматривается комплекс проблем, связанных с умножением и диверсифицированием санкций ООН, в частности, проводятся различия между тремя типами режимов санкций: антитеррористические санкции, санкции по борьбе с распространением и санкции по разрешению конфликтов. Наблюдаются определенные изменения в составе режимов санкций – увеличение количества ссылок на международно-правовые стандарты при разработке санкций, заметное взаимодействие с другими процессами и режимами, а также неформальными договоренностями. В первой части работы рассматриваются санкции и контрмеры в международно-правовых рамках. Во второй части рассматриваются функции санкций ООН, в том числе такие, как санкции ООН и стратегии борьбы с терроризмом, распространением оружия массового уничтожения, как инструмента защиты прав человека и гуманитарного права. Третья часть работы содержит материал, описывающий структуру и процедуры регулирования санкций ООН – разработка санкций ООН посредством взаимодействия с неформальными договоренностями, гласностью в Совете Безопасности, санкции СБ и политика прекращения действия санкций ООН. В следующей части книги рассматривается взаимодействие с другими режимами – санкции ООН и международные финансовые институты, Всемирная торговая организация, международный арбитраж, договорные споры между частными операторами и преследование нарушителей санкций. В последнем разделе представлены региональные перспективы, в том числе такие, как санкции ООН и региональные организации, интерпретация и пересмотр санкций ООН европейскими судами, взгляды Китая и Японии на санкции ООН, восприятие санкций ООН в Африке, санкции ООН и мирное строительство в Западной Африке.

**10. Энрико Кариш, Лорейн Рикард-Мартин, Шона Р. Мейстер «Эволюция санкций ООН: из инструмента ведения войны в инструмент мира, безопасности и прав человека» (Enrico Carisch, Loraine Rickard-Martin, Shawna R. Meister (2017). The Evolution of UN Sanctions: from a Tool of Warfare to a Tool of Peace, Security and Human Rights. Springer. ISBN 978-3-319-60005-5 DOI 10.1007/978-3-319-60005-5).** В качестве ключевых моментов данной книги авторы выделяют следующие – для выяснения используются ли санкции ООН в соответствии с основополагающими ценностями благосостояния человека, которые закреплены в Уставе ООН, описывается создание системы санкций ООН и ее постоянное изменение в мирное время и в ходе войны. Переход от традиционного инструмента экономической войны к современной системе превентивных, защитных и принудительных санкций ООН начался задолго до создания ООН. Книга состоит из трех частей. Первая часть включает материал об эволюции системы санкций ООН, вторая часть посвящена рассмотрению самих санкций, и третья часть содержит анализ, выводы и рекомендации. Во второй части книги приведен анализ состава санкций ООН, начиная от ввода санкций против



Родезии и апартеида Южной Африки, Ирак, Югославия, Гаити, и до Южного Судана. Данная часть книги представляет собой комплексное описание политического контекста санкций, санкционной политики, сфальсифицированного вмешательства, борьбы с насилием и т.д. Следует отметить, что книга отражает все виды санкционной политики по отношению к всем странам, против которых были введены санкции ООН.

### **1.3. Санкции в рамках Системы экспортного контроля (3)**

**1. Дэниелс, Марио, Крайдж, Джон «Регулирование знаний и национальная безопасность в послевоенной Америке». (Daniels, Mario, Krige, John (2022). Knowledge Regulation and National Security in Postwar America. The University of Chicago Press. ISBN-13: 978-0-226-81752-1 DOI: <https://doi.org/10.7208/chicago/9780226817521.001.0001>)** В книге последовательно излагается материал, связанный с анализом целей экспортного контроля, его связь с национальной безопасностью и изменения системы экспортного контроля. Приводятся примеры попыток нескольких администраций президентов США (Рейган, Буш, Клинтон, Трамп) контролировать передачу технологий несекретного характера и приобретение знаний в академических кругах. Авторы связывают политику экспортного контроля с экономической безопасностью при передаче технологий в разные страны, в том числе в Японию, Россию, Китай.

**2. О.Л. ван Даален, Дж.В.Дж. ван Хобокен, М. Кут, М. Руч. «Новые правила экспортного контроля предметов кибернаблюдения в ЕС». (O.L. van Daalen, J.V.J. van Hoboken, M. Koot, M. Rucz (2021). The New Rules for Export Control of Cyber-Surveillance Items in the EU. Institute for Information Law. <https://www.ivir.nl/publicaties/download/Report-on-cybersurveillance-items.pdf> (дата доступа 27.12.23).** В отчете описано регулирование предметов кибернаблюдения двойного назначения с выделением законодательной истории определения данных объектов, правила в отношении объектов кибернаблюдения, политика экспортного контроля, основанная на соблюдении прав человека, конституционная основа для интеграции прав человека во внешнюю политику ЕС и инструменты торговой политики, синергия о двойном использовании и другими политиками ЕС. Часть отчета посвящена внутренним репрессиям и нарушению прав человека, в том числе такие, как оценка нарушений прав человека для экспортного контроля, кибернаблюдение и международное гуманитарное право, а также оценка нарушений международного гуманитарного права. Специальный раздел описывает использование предметов кибернаблюдения, таких как, технологии искусственного интеллекта для распознавания лиц и эмоций и возможности злоупотреблений, технологии и устройства отслеживания местоположения, технологии аналитического программного обеспечения с открытым исходным кодом и возможности злоупотреблений, технологии

перехвата связи и возможности злоупотреблений, технологии программного обеспечения для взлома и возможности злоупотреблений. В заключительном разделе приведен синтез новых правил – перечисленные элементы кибернаблюдения, попадающие под определение (технологии распознавания лиц и эмоций, технологии отслеживания местоположения, аналитическое программное обеспечение с открытым исходным кодом), комплексная проверка и разрешение на экспорт, выделение вопросов координации и прозрачности, а также национального законодательства.

**3. Хиршхорн Эрик, Иган Брайан, Крауланд Эдвард. «Экспортный контроль и экономические санкции США». (Hirschhorn Eric, Egan Brian, Krauland Edward (2022). U.S. Export Controls and Economic Sanctions. Oxford University Press. ISBN 9780190068288).** В книге отмечается, что экспортный контроль и экономические санкции США имеют долгую историю. Первый пример относится к октябрю 1774 года. Авторы рассматривают четыре режима лицензирования экспорта в США, а именно, контроль над товарами «двойного назначения», программного обеспечения и технологий, предметы оборонного назначения, ядерное оборудование и технологии, а также радиоактивные материалы. Книга состоит из четырех разделов. Первый, описывает контроль министерства торговли за экспортом военных товаров «двойного назначения», программного обеспечения и технологий. Во втором разделе описан контроль государственного департамента над экспортом оборонных товаров и услуг. Третий раздел посвящен составу и структуре экономических санкций. Заключительный раздел описывает контроль за экспортом ядерной продукции и содействие иностранной ядерной деятельности. Данная книга может быть использована исследователями в качестве справочного материала.

#### **1.4. Санкции в области информационных технологий (киберсанкции, киберблокады, киберконфликты) (12)**

**1. Юлия Мядзвецкая «Проблемы режима киберсанкций в рамках общей внешней политики и политики безопасности (ОВПБ). Miadzvetskaya, Yuliya. (2019). Challenges of the Cyber Sanctions Regime under the Common Foreign and Security Policy (CFSP). Security and Law, 277–298. ISBN: 9781780688909 doi:10.1017/9781780688909.012.** Столкнувшись с широкомасштабными кибератаками и тупиком в глобальном переговорном процессе, ЕС поставил задачу разработки собственной системы борьбы со злонамеренной кибердеятельностью и укрепления кибербезопасности на основе кибердипломатии. Приведена текущая структура санкций ЕС, которая представляет собой важнейший инструмент, направленный на поддержание и восстановление международного мира и безопасности, борьбу с терроризмом и распространением оружия массового поражения, а также на обеспечение уважения прав человека, демократии и

верховенства закона. Рассматривается проблема атрибуции кибератак, указывается на существующие риски того, что практическая реализация будет ограничена. Выделяются несколько существенных аспектов атрибуции – техническая, правовая, политическая и контекстуальная. Вводимые санкции должны основываться на веских убедительных доказательствах и выдерживать тест на фундаментальные права. В то же время, конфиденциальный характер доказательств, подтверждающих режим киберсанкций, включая секретную или частично секретную информацию, должен храниться в тайне. Описана задача предоставления доказательств, которые должны иметь правдоподобную фактическую основу. Однако конфиденциальный характер информации, на которой основаны санкции, может быть поставлена под угрозу ее раскрытием. И в этом состоит основная трудность соблюдения требования об изложении причин и достаточном их доказательственном обосновании. В заключении приведен обзор киберсанкций США, которые более эффективно применяли, вместе с уголовным обвинением, против спонсируемых правительством хакеров. Программа санкций США, связанная с кибербезопасностью, вступила в силу в 2015 году и предусматривала также блокировку собственности определенных лиц, занимающихся значительной злонамеренной кибердеятельностью. Киберсанкции являются серьезной мерой, учитывая, что атака приведет или будет способствовать возникновению значительной угрозы национальной безопасности, внешней политике или экономическому здоровью или финансовой стабильности США. Сюда может входить «нанесение вреда» или иным образом существенно ставить под угрозу предоставление услуг в критически важном секторе инфраструктуры, нарушая доступность компьютера или сети компьютеров, что приводит к значительному незаконному присвоению средств или экономических ресурсов, коммерческой тайны, личных идентификаторов, вмешательства или подрыва избирательных процессов или институтов. Американские санкции также включают в себя ряд мер: от всеобъемлющих, блокирующих деятельность всего правительства или введение торговых ограничений, до сокращенной программы санкций, нацеленных только на конкретных физических и юридических лиц.

**2. «Законодательное руководство по киберсанкциям (опубликовано 3 ноября 2020 г.)». Statutory guidance Cyber sanctions: guidance. Published 3 November 2020. <https://www.legislation.gov.uk/uksi/2020/597/contents/made> (дата доступа 28.12.23)** Документ состоит из 7 частей и является нормативным актом Великобритании «Положение о киберсанкциях и проблема принадлежности кибератак». Последовательно излагается материал об обозначении лиц, вовлеченных в соответствующую кибердеятельность, замораживание активов в отношении обозначенных лиц, вопросы иммиграции, исключения и лицензии, информация, характеризующая полномочия запрашивать информацию, информационные преступления, раскрытие информации и вопросы правоприменения.

**3. Николас Михаил Самбалюк «Конфликт в 21 веке: влияние кибервойны, социальных сетей и технологий». (Nicholas Michael Sambaluk (2019). Conflict in the 21st Century: The Impact of Cyber Warfare, Social Media, And Technology. ABC-CLIO, LLC. ISBN 9781440860010).** В книге описаны аспекты технологий 21 века и их влияние на характер конкретных конфликтов. Материал разделен на три раздела, охватывающих кибервойну, социальные сети и собственно технологии. В целом кибервойна может быть определена как возможность использования цифровых инструментов и методов для нанесения какого-либо ущерба цели в связи с поставленной политической задачей. Более того, с точки зрения жертвы, различные формы киберагрессии бывает трудно отличить друг от друга. Кроме того, кибервторжения часто не идентифицируются до того момента, пока это не произойдет (манипулирование данными и или их удаление, а также другие эффекты). Неопределённость в развитии событий добавляют использование специальных технологий (шпионское оборудование) и социальных сетей. Распространение кибероружия подтверждает утверждение о том, что кибероружие дешево и широко доступно. Наличие ботнетов, рынка зловредных программных злоупотреблений подтверждает этот вывод. Каждый раздел включает описание соответствующих инструментов. Приведена хронология действий с 2002 по 2018 г.г., связанных с использованием инструментов кибервойны. Представлен подробный список литературных источников по кибервойне.

**4. Виктор Шеймов «Киберпространство и безопасность: принципиально новый подход». (Victor Sheymov (2021). Cyberspace and Security: A Fundamentally New Approach. Third Revised Edition. Cyberbooks Publishing. ISBN: 978-0-9858930-8-8).** В книге обсуждаются проблемы киберпреступлений и указывается, что повреждение критически важной инфраструктуры может привести к выходу из строя нефтеперерабатывающих и химических предприятий, выключают из работы службы экстренной помощи, оставляют дома без отопления и кондиционированного воздуха и т.д. В качестве целей кибератак выступают: финансовый сектор и финансы корпораций, системы промышленного контроля, энергосистемы, системы связи, системы добычи и распределения нефти и газа, криптовалюта и другие компоненты критической инфраструктуры. Книга состоит из 4 частей, в которых последовательно рассматриваются такие вопросы, как безопасность доступа, киберпространство (структура и среда, законы и правила киберпространства, инфраструктура киберпространства), кибербезопасность (безопасность киберпространства, злоумышленники и цели). Автор выделяет в отдельную главу материал, относящийся к анализу устаревших методов компьютерной безопасности, например, системы контроля доступа на основе пароля, системы обнаружения вторжений, виртуальные частные сети, системы защиты от вредоносного программного обеспечения. В последней части книги рассматривается материал, относящийся к защите суверенных систем,

защитной роли правительства, режимам пассивной и активной защиты, суверенитета в киберпространстве и др.

**5. Карстен Фриис, Йенс Рингсмос. «Конфликт в киберпространстве: теоретические, стратегические и правовые перспективы».** (Karsten Friis, Jens Ringsmose (2016). *Conflict in Cyber Space: Theoretical, Strategic and Legal Perspectives*. Routledge. ISBN 9781315669878). Рассматривается широкий круг проблем, относящихся к киберконфликтам. Приведен анализ академических подходов к определению кибербезопасности, эмпирический анализ категорий соперничество и киберконфликт, вопросы управления кибербезопасностью, кибервойна со стороны социальных сетей, развитие правовых норм в киберпространстве и др. Авторский коллектив рассматривает, в первую очередь, проблемы национальной безопасности. Все информационные системы (военные и гражданские) сильно компьютеризированы и эти процессы будут продолжаться. Уже сейчас каждый киберконфликт имеет киберизмерение. Высказывается предположение о том, что лидерство отдельных стран в киберпространстве обеспечит победу в будущем. Хотя этот тезис является спорным. Проводится сравнение действий в военной сфере и в киберпространстве. Для «реального мира» злоумышленник может оценить уровень болевого порога (пересечение границы, нападение на судно противника и т.д.). Но какую реакцию противника следует ожидать, в том случае, если хорошо спланированная кибератака выведет из строя компоненты национальной критической инфраструктуры? Какой ответ будет выбран, даже если жертв не было? Многонациональный контекст киберконфликта усиливает необходимость в общих стандартах киберзащиты. Если атака осуществляется против самого слабого звена сети, группа стран должна настоять на принятии всеми определенных мер защиты. Если это не произойдет, то некоторые страны почувствуют, что им лучше жить в одиночестве, а те, кто серьезно относится к риску и тратит значительные ресурсы на его смягчение, не захотят платить за тех союзников, которые доверяют свою киберзащиту случаю. Еще одним последствием для национальных правительств и альянсов является необходимость государственно-частного партнерства, поскольку большая часть киберинфраструктуры принадлежит частному сектору. И именно там сосредоточена большая часть опыта в области киберзащиты. И данная проблема ждет своего решения! Компании могут иметь общий интерес в защите от кибератак, но они по-прежнему остаются конкурентами. Одновременно, компаниям необходимо сбалансировать свои обязательства перед правительствами (например, раскрывать все данные) и соблюдать свои обязательства перед клиентами (т.е. защищать конфиденциальность от слежки со стороны правительства). В качестве основного вывода авторы предлагают следующее: развитие киберпространства открывает самую неудобную истину – то, что когда-то было почти абсолютной безопасностью, стало относительной безопасностью. Необходим новый общественный договор. Поскольку жертвой кибератаки может стать любой, в любое время и в любом

месте. Правительствам придется признать, что в эпоху кибератак (и терроризма) они не могут больше защищать своих граждан так же всесторонне, как в прошлом – и, тем не менее, в то же время, этим гражданам придётся дать государству разрешение на применение силы, в том числе наступательной киберсилы.

**6. Ричард А. Кларк, Роберт К. Кнейк «Пятая сфера: защита нашей страны, наших компаний и самих себя в эпоху киберугроз». (Richard A. Clarke, Robert K. Knake (2019). The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats. Penguin Press. ISBN 9780525561972).** В первую очередь, авторы отталкиваются от тезиса, что любой сценарий между противниками в киберпространстве – это баланс между нападением и защитой. В случае, если отмечается технологическое преимущество при низких затратах – говорят о конфликте. При обратной ситуации, слабой защите и высоких шансах поражения будет стремление к преобладанию большей стабильности. Данные положения полностью применимы к действиям между хакерами и корпорациями, тайному шпионажу национальными государствами и потенциальной будущей кибервойне между государствами. Традиционная мудрость, накопленная в области информатики, информационных технологий и нетворкинга (полезные связи - социальная и профессиональная деятельность, направленная на то, чтобы с помощью круга друзей и знакомых, работающих или имеющих связи в той или иной сфере, максимально быстро и эффективно решать сложные жизненные задачи), позволяет сделать вывод о том, что существует огромное преимущество в атаке. Будущие войны будут начинаться с кибератак. Эта книга о том, как найти баланс между изменяющимися нападением и защитой, как увеличить скорость изменений и найти путь к стабильности. Рассматривается и обсуждается категория киберустойчивости, т.е. способности организации работать в условиях кибератаки или другого кибер-инцидента. Можно снизить риски, возникающие за счет использования наступательных кибертехнологий и субъектами в мирное время и во время кризисных ситуаций. Это подтверждает тлеющий киберконфликт с Россией, Китаем и Ираном. Отмечается рост расходов на кибербезопасность, инвестиций в технологии кибербезопасности для разработки новых решений, рост киберстрахования. Выделен тезис о том, что киберпространство - есть, в значительной степени частная сфера, и оно, по сути, связано с обменом информацией, большая часть которой является частной. Анализируется проблема, суть которой заключается в следующем – кто несет фундаментальную ответственность за кибербезопасность на национальном уровне. За защиту сетевых систем несут ответственность владельцы и операторы частного сектора при поддержке правительства. Правительственные структуры оказывают помощь, например, при расследовании компьютерных преступлений, сбору разведанных или ведении наступательных операций. Частные компании в ответе за отражение атак типа «отказ в обслуживании», фильтрации вредоносного трафика и т.д. Правительственные органы будут находить и арестовывать

киберпреступников и своими усилиями выравнять киберсанкции. Описанный подход подвергается критике, эксперты утверждают, что кибербезопасность является частью национальной безопасности, правительство несет ответственность за это направление. Высказывается мнение о том, что частные компании занимаются бизнесом и не имеют должного стимула. Приведенные аргументы кажутся заслуживающими внимания, но не обеспечивают действенного решения для национальной кибербезопасности.

**7. Майкл Секстон, Элиза Кэмпбелл «Кибервойна и кибермир: цифровой конфликт на Ближнем Востоке». Michael Sexton, Eliza Campbell (2022). Cyber War And Cyber Peace: Digital Conflict In The Middle East. I.B. Tauris. ISBN 978-0-7556-4602-9.** Книга Представлена Институтом Ближнего Востока (Middle East Institute (MEI)). Ближний Восток является домом, в котором развивается одно из технологически продвинутых в мире общество. Ближний Восток стал ареной большого количества сражений в киберпространстве, чем любой другой регион. Необходимо понимание динамики киберактивности в регионе, который имеет решающее значение для мировой экономики и который погряз в геополитической напряженности. Анализируется состав участников MENA (Middle East and North Africa), их состав, возможности. Приведен материал, который характеризует негосударственных участников событий в данном регионе и их политическая и информационная активность. Приведен исторический обзор киберпространства в регионе Ближнего Востока и Северной Африки, злоумышленные кибератаки и международные последствия. Устоявшаяся практика традиционной дипломатической деятельности дополнена «кибердипломатией», которая сосредоточена вокруг контроля и управления взаимосвязанной цифровой средой и ресурсами. Выделен параграф, в котором киберстрахование рассматривается как кибердипломатия. Представлен материал по анализу санкционированному государственному хактивизму (сирийская электронная армия), дезинформации в Персидском заливе, росту цифрового авторитаризма на Ближнем Востоке, безопасного регионального киберпространства.

**8. Брэндон Валериано, Райан К. Мэнесс. «Кибервойна против киберреальности: Киберконфликт в международной системе». (Brandon Valeriano, Ryan C. Maness (2015). Cyber War Versus Cyber Realities: Cyber Conflict in the International System. Oxford University Press. ISBN 978-0-19-020479-2).** Данная книга посвящена киберконфликтам и процессу международного взаимодействия в условиях изменяющегося ландшафта международной безопасности. Авторы разделяют две категории – киберхайп вместе с инфляцией угроз, с одной стороны, и эмпирическими реалиями кибервзаимодействия с другой. И эти разногласия важны, поскольку они представляют две точки зрения в дебатах о кибербезопасности. Отмечается, что сейчас в международной системе доминирует чувство страха. С наступлением цифровой эпохи киберкоммуникаций процесс создания страха

продолжает формировать диалог в международных отношениях, поскольку киберпространство становится новой областью споров в международных взаимодействиях. Авторы отмечают, что старые парадигмы, ориентированные на силовую политику, демонстрацию силы и сдерживание, применяются к новым тактикам и технологиям, при этом мало учитывается, как новая тактика может привести к другим средствам и целям. Возникающий страх, которому мы стремимся противостоять, заключается в том, что кибероружие станет доминировать в системе и изменит способы взаимодействия государств и отдельных лиц. Авторы раскрывают, как на самом деле работают киберконфликты между отдельными игроками, раскрывают внешнеполитические последствия новой области конфликта, а также как данный тип конфликта регулируется с помощью международных норм и режимов. Предлагается теория киберсдерживания, которая зависит от четырех процессов: характера оружия и его во производимости, что делает его одноразовым оружием ограниченной эффективности; возможность обратного удара, учитывая, что государства-инициаторы часто слабее государства, в которое они стремятся проникнуть; естественный потенциал сопутствующего ущерба в киберпространстве, поскольку технология не ограничивается военным пространством; потенциальный вред гражданскому населению. В книге последовательно рассматриваются следующие вопросы: контуры мира киберконфликтов; киберсила, кибероружие и кибероперации; теории киберконфликта (сдержанность, регионализм, шпионаж и кибертерроризм в цифровую эпоху); динамика киберконфликта между соперничающими антагонистами; влияние кибердействий (киберсобытия и связь между конфликтом и сотрудничеством); киберконфликт и негосударственные субъекты; киберправила – поощрение справедливости и пропорциональности в кибероперациях.

**9. Рассел, Элисон Лоулор. «Киберблокады». (Russell, Alison Lawlor (2014). *Cyber blockades*. Georgetown University Press. ISBN 978-1-62616-113-9).** Данная книга является самой представительной в данном разделе и базируется на докторской диссертации Элисон Рассел «Киберблокады: к теории информационной войны в цифровую эру» (*Cyber Blockades: Towards a Theory of Informational Warfare in the Digital Era*. <http://hdl.handle.net/10427/011661> (дата доступа 03.01.24), которая была защищена в университете Тафтса в 2012 году. Кибератакам и кибервойнам уделяется значительное внимание из-за угрозы, которую они представляют для государственного и коммерческого секторов. Кибератаки происходят регулярно и крупные учреждения становятся объектами для получения информации по проблемам дипломатии, безопасности и финансов. Киберпространство превратилось в центр тяжести не только военных операций, но и для всех аспектов национальной безопасности, включая экономические операции, дипломатические транзакции и т.д. Автор книги в качестве цели выделила следующие моменты – каким образом кибератаки могут привести к отключению, закрытию киберпространства и превращению



его в довесок информационного общества; может ли быть отказано в доступе к киберпространству по желанию какой-либо стороны и какие могут быть последствия. Целью исследования является развитие понимания категории «киберблокада», когда и в каких условиях она может быть использована и как она может повлиять на национальную безопасность, а также ее последствия для науки и политики. Киберблокада — это ситуация, возникающая в результате атаки на киберинфраструктуру или систему, которая препятствует доступу государства к киберпространству, тем самым предотвращая передачу (вход и выход) данных за пределы географических границ. Киберблокады потенциально могут нанести политический, экономический, военный и социальный ущерб государству и могут рассматриваться как военные действия. Киберблокады и кибератаки являются политически и экономически разрушительными формами войны, но мы мало что о них понимаем, отчасти потому, что у нас нет теории, которая могла бы обосновать их использование или защиту от них. Два основных вопроса этого исследования направлены на определение киберблокады и понимание условий, при которых они могут возникнуть. Первый вопрос — что такое киберблокады, их структура и компоненты (необходимо определить понимание участников, ресурсов, потенциальных последствий). Второй вопрос — почему акторы используют киберблокады как инструмент международных отношений. Последовательно анализируются такие важные вопросы, как сети органов власти, эволюция блокад в различных сферах, примеры кибератак, сравнение киберблокад. Представлен обзор уникальных особенностей киберпространства и того, как оно согласуется с традиционными теориями международных отношений. Рассматривается анализ блокад в четырех сферах — на суше, на море, в воздухе и в космосе для выявления общих черт и различия между разными типами блокад и оценки какие функции будут применяться с наибольшей вероятностью.

**10. Лэнс Э. Дэвис, Стэнли Л. Энгерман «Морские блокады в мире и войне: экономическая история с 1750 года». (Lance E. Davis, Stanley L. Engerman (2006). *Naval Blockades in Peace and War: An Economic History Since 1750*. Cambridge University Press. ISBN 978-0-511-24537-4).** Во время войны существует ряд альтернативных военных и военно-морских стратегий, которые воюющая страна может использовать для победы над врагом. Одной из таких стратегий является завоевание силой оружия в прямом бою. Подобная стратегия предполагает осаду или вторжение на территорию противника и направлена на уничтожение, захват или капитуляцию противника и, возможно оккупацию его территории. В свою очередь, экономическая война, ослабляя способность противника вести военные действия, может заменить или дополнить стратегию прямого боя. Такая экономическая стратегия призвана разорвать торговые связи между противником и его союзниками или с нейтральными государствами и тем самым снизить уровень военных и гражданских товаров, доступных для поддержки его военных предприятий. Исторически блокада (морская и

наземная) была наиболее распространённой формой экономической войны, но использовались и другие формы экономической войны. К ним относятся введение более высоких тарифов, нетарифные исключения, ограничения на движение капитала и политика, направленная на поощрение производства заменителей странами-мишенями и нейтральными странами. Кроме того, масштабы прямой экономической войны были расширены и теперь включают воздушные бомбардировки экономических объектов, санкции, направленные на ограничения торговли, саботаж экономических целей, упреждающие закупки стратегических материалов и т.д. Законы международных экономических отношений предусматривают три категории действий между странами или четыре, если один из вариантов состоит в том, чтобы ничего не делать и сохранять текущую ситуацию. Этими тремя категориями являются следующие: дружественные меры, исключающие войну; недружественные меры, за исключением войны; и война. Эта политика, называемая «санкциями», включает меры экономического, политического или дипломатического характера, которые вводятся в одностороннем порядке одной страной или коалицией стран. Среди экономических санкций – блокады и другие формы ограничений на торговлю, финансовые потоки и передвижение людей. В этой книге для нас наибольший интерес представляет УШ глава «Блокады без войны. От тихоокеанских блокад к санкциям» (с.383-417). В ней последовательно рассматриваются вопросы определения блокад и санкций, санкций в мирное время, эффективность санкций и санкции, введенные ООН. Авторы анализируют статистические данные, характеризующие введенные санкции в период 1914-1990 г.г. по разным аспектам.

**11. Понимание киберконфликта: четырнадцать аналогий / Джордж Перкович и Ариэль Э. Левит, редакторы. *Understanding Cyber Conflict : Fourteen Analogies* / George Perkovich and Ariel E. Levite, Editors. (2017). Georgetown University Press. ISBN 9781626164994.** Международное сообщество и правительства только сейчас начинают понимать атрибуты кибервозможностей и возможную природу конфликтов кибербезопасности. Авторы в основу своих исследований киберконфликта положили метод аналогий. Основная ценность аналогий состоит в том, что позволяет выяснить какие особенности кибервозможностей потенциального конфликта наиболее важны для анализа и понимания, а какие менее актуальны в целях предотвращения конфликтов и проведения киберопераций. Книга состоит из трех взаимосвязанных частей: определение кибероружия (интеллект в киберпространстве и в разведке, нелетальное оружие и кибервозможности, кибероружие и высокоточные боеприпасы); какими могут быть кибервойны (кибервойна и информационная война, кризисная нестабильность, стратегия экономической войны); предотвращение и управление киберконфликтами (киберугрозы и ядерные аналогии, новые технологии двойного назначения, активная киберзащита и применение противоздушной обороны в киберпространстве). В первом разделе рассматриваются характеристики

кибервозможностей и способы их использования в разведывательных целях. Второй раздел исследует возможность применения или неприменения эпизодов политических и тотальных войн к киберконфликтам XXI века. Третий раздел проверяет какие идеи могут быть использованы государствами при управлении киберпространства опираясь на опыт управления грозными субъектами и технологиями. Приведено одно из получивших распространение определений киберпространства – связанное оборудование, программное обеспечение и человеческие ресурсы, причем проблема человеческих ресурсов постоянно остается актуальной. Информация и коммуникационные технологии служат множеству мирных целей, а также предоставляют законные и незаконные средства создания богатства и обогащения. Авторы исходят из предположения, что в контексте только одного межгосударственного конфликта можно привести сотни аналогий и провести анализ между кибероружием и его предшественниками. Авторы указывают, что общество находится на ранней стадии изучения наступательных операций и киберконфликтов. Наблюдения, анализ и предположения, которые присутствуют в книге предназначены для стимулирования дальнейшего анализа и дебатов, опираясь на соответствующие аналогии прошлого для формирования будущего.

**12. Брантли, Аарон Франклин «Решение о нападении: принятие киберрешений военными и разведчиками». (Brantly, Aaron Franklin (2016). The Decision to Attack: Military and Intelligence Cyber Decision-Making. University of Georgia Press. ISBN 9780820349190).** Споры о важности киберпространства привели к формированию подхода, в соответствии с которым определено что новая сфера деятельности является жизненно важной для национальной безопасности государства. Ландшафт, структура и виды угроз постоянно изменяются и это приводило к недопониманию того, как должны приниматься решения в этом аморфном домене под названием киберпространство. Остается до конца не исследованным вопрос – способно ли государство рационально участвовать в наступательных кибероперациях базируясь на системной модели принятия решений, основанной на рациональных ожиданиях полезности. Книга включает 10 глав, в которых последовательно рассматриваются следующие вопросы: введение в систему принятия киберрешений; ключевые концепции киберпространства; цифровая власть; анонимность и атрибуция в киберпространстве; кибер и традиционные операции и динамика конфликта; определение роли разведки в киберпространстве; использование кибербезопасности и выбор подхода; когнитивные процессы и принятие решений в киберпространстве; ожидаемая полезность международного киберконфликта. Авторы отмечают еще одно важное обстоятельство – поскольку опыт борьбы с киберконфликтами пока весьма ограничен, любое государство, которое рассматривает нападение как часть стратегии сдерживания, принуждения или упреждающего применения силы – создает прецедент. В качестве примера используется Stuxnet и его предшественники. И еще одно важное обстоятельство – относительно легкое

вхождение субъекта в мир киберконфликтов практически гарантирует, что после получения значительного преимущества от определенного вида атаки, другие будут склонны делать подобное. Во-первых, несмотря на имеющуюся неопределенность в отношении будущего киберконфликтов, динамика интенсивности и частоты являются достаточно ясными. Во-вторых, возможности проведения кибератак гораздо более масштабных, чем те, которые были проведены ранее, находятся в распоряжении всего нескольких государств. В-третьих, обладатели стратегических киберпотенциалов по-прежнему сознательно воздерживаются от их максимального использования, и такая осторожность признана справедливой.

## 1.5. Экономические санкции (13)

1. Роберт Эйлер «Экономические санкции. Международная политика и политическая экономия в действии». (Robert Eyster (2007). *Economic Sanctions International. Policy and Political Economy at Work*. Palgrave Macmillan. ISBN-13: 978-1-4039-7463-1). В предисловии указывается, что данная книга может использоваться как политологами, так и экономистами для оценки санкций и их экономического эффекта. Этот союз между политикой и экономикой, возможно, в конечном итоге станет заменой войне. Высказывается тезис, что перераспределение богатств в результате политических решений и их экономические эффекты определяют предмет политической экономии. Санкции стали немедленной дипломатической реакцией на происходящие процессы. Независимо от того, являются ли санкции односторонними или универсальными, потенциальная прибыль влечет за собой нарушение санкций, используя для этого более высокие цены в другой стране и потерянные рынки. Несмотря на то, что санкции стали более целенаправленными и появилось новое законодательство, призванное экономически наказать страны, которые помогают и содействуют странам, находящимся под санкциями, последние с трудом достигают заявленных целей. Высказывается предположение о том, что ученые должны договориться о модели или наборе моделей для прогнозирования и анализа последствий санкций. Подобный консенсус поможет правительствам рекомендовать варианты санкционной политики, которые одновременно позволят сбалансировать экономическую, гуманитарную и политическую эффективность. Санкции в конечном итоге являются макроэкономическим явлением, и их последствия необходимо тщательно анализировать и прогнозировать. В книге последовательно рассматриваются следующие вопросы: базовый анализ санкций, начало и продолжение санкций с использованием теории игр, теория общественного выбора и «умные санкции», макроэкономика открытой экономики, математическая модель санкций, эмпирический анализ эффективности санкций, выводы и политические рекомендации. Одним из достоинств данной книги является

использование макромоделей новой открытой экономики, разработка которой является весьма трудоемкой, но полученные эмпирические решения можно использовать для оценки влияния санкций на экономику. Эффективность санкций является серьезной проблемой в научной литературе и средствах массовой информации. Высказывается прогноз о том, что использование экономических санкций, вероятно со временем увеличится. В приложении приведены краткие истории отдельных санкций.

**2. Уильям Х. Кемпфе, Антон Д. Ловенберг. «Политическая экономия экономических санкций». (William H. Kaempfe, Anton D. Lowenberg (2007). The Political Economy of Economic Sanctions. Chapter 27. Handbook of Defense Economics, Volume 2. Elsevier B.V. DOI: 10.1016/S1574-0013(06)02027-8).** Материал содержит комплекс вопросов, посвященных исследованию политической экономии экономических санкций. Последовательно рассматриваются следующие вопросы: экономические последствия санкций; политические детерминанты санкционной политики в государствах-отправителях; политические последствия санкций для страны-объекта, монорациональный актор и подходы теории игр к санкциям; эмпирические исследования санкций; политические институты и санкции; выводы и направления дальнейших исследований. Исследование экономических последствий санкций начинается с рассмотрения последствий торговых санкций. Масштаб торговли между санкционирующей стороной и объектом санкций до введения санкций является важным фактором, определяющим легкость, с которой объект может найти альтернативные источники поставок и альтернативные рынки для своих товаров. Используя кривые предложения для изучения последствий торговых санкций, можно показать не только влияние санкций на условия торговли соответствующих стран, но также сделать выводы о влиянии санкций на благосостояние. Экономисты и политологи пришли к выводу, что рассмотрение политических процессов посредством которых политика санкций возникает в странах-отправителях, а также политических процессов, посредством которых санкции приводят к результатам политики в целевой стране, является ключом к решению двух основных вопросов политической экономии санкций: а) какие факторы определяют, когда санкции будут использоваться в качестве предпочтительного инструмента оказания влияния в международных отношениях; б) какие факторы определяют вероятность успеха или неудачи санкций в достижении их политических целей? Фундаментальная трактовка санкций способствовала четкому пониманию того, что эти два вопроса неразрывно связаны и большинство стратегий санкций фактически заканчивается навязыванием. Эксперты все чаще признают важность политических институтов как в странах, подвергающихся санкциям, так и в странах-объектах санкций. Приведен емкий список анализируемой литературы по теме исследования экономических санкций.

**3. Хуфбауэр Г.К., Шотт Дж.С., Эллиотт К.А., Барбара Оэгл «Экономические санкции пересмотрены». (Hufbauer G.C., Schott J.S., Elliott**

К.А., Barbara Oegg (2007). *Economic Sanctions Reconsidered*. 3rd Edition. Peter G. Peterson Institute for International Economics. ISBN 978-0-88132-407-5). Данная книга выдержала 3 издания и считается базовой при изучении проблем оценки эффективности экономических санкций. Книга включает 6 глав, 3 приложения и обширный список литературы. Авторы последовательно изложили следующие вопросы: введение (страны-отправители и их мотивы, ограничения на применение санкций, исторический обзор); анализ полезности санкций (анатомия санкций, структура санкций, цели внешней политики, обзор переменных, влияющих на стоимость неповиновения); политические переменные (смена режима, нарушающие военные авантюры, ухудшение военного потенциала, другие важные изменения в политике, политика, холодная война и цели санкций); экономические переменные (размеры отправителей и целевых стран, торговые связи, экономическое здоровье и политическая стабильность целевых стран, стоимость санкций для целей, стоимость санкций для отправителей); санкции после холодной войны (эволюция санкционной политики США, ООН и политика послевоенных санкций, вмешательство Конгресса в политику санкций, санкции государства и местного самоуправления, невероятная легкость «умных санкций», новые вызовы санкционной политике); выводы и политические рекомендации (эффективны ли санкции?, политические рекомендации по более эффективному использованию санкций). Авторы исследования концентрируются на четырех центральных вопросах: каковы были экономические санкции в достижении иностранных политических целей? Какие факторы – как политические, так и экономические – повышают шансы на то, что санкции внесут положительный вклад в желаемый исход внешней политики? Какова цена санкций как для страны-мишени, так и для страны-отправителя? Какие уроки можно извлечь из этого опыта, чтобы они могли служить руководством для политиков? Отправной точкой для анализа является список из 174 случаев экономических санкций. В аннотации к каждому делу подводятся итоги, ключевые события эпизода, цели отправителя, реакция цели, отношение третьих стран, а также экономические издержки как для получателя, так и для отправителя. В заключение приводится общая оценка эпизода. Заслуживает пристального внимания материал трех приложений: А «Эконометрический анализ экономических санкций», Б «Влияние экономических санкций США на торговлю» и В «Методология, используемая для оценки стоимости санкций для целевой страны».

**4. Питер А.Г. ван Бергейк «Справочник по исследованиям экономических санкций».** (Peter A.G. van Bergeijk (2021). *Research Handbook on Economic Sanctions*. Edward Elgar Publishing Limited. ISBN 9781839102721 <http://dx.doi.org/10.4337/9781839102721>). Материалы, представленные в этом справочнике, свидетельствуют о том, что широта и глубина исследований в области экономических санкций расширяются. Авторы объединили две дисциплины, которые изучают санкции – экономику и

политологию/международные связи. Исследуются санкции разных форм. Появились новые формы, которые охватывают, например, путешествия, финансы и все чаще частных лиц. Сделан вывод о том, что некоторые меры представляются как санкции, но де-факто являются символическими, в то время как другие ограничения на международные обмены остаются скрытыми и лишь недавно были признаны санкциями. Важным вопросом является то, что все торговые ограничения влекут за собой издержки как для отправителя, так и для получателя. Поэтому отправитель может разработать санкционные меры таким образом, чтобы убытки для собственного бизнеса были сведены к минимуму. На практике это означает, что санкции будут менее эффективными. Так в главе 13 «Санкции ЕС против России и российские контр санкции» приведены результаты анализа различных последствий санкций ЕС против РФ в 2014 году и российских контр санкций (с.249-263). Были использованы две методологические инновации: а) гибридный подход, сочетающий VAR и моделирование «разница в различиях» (статистический метод, используемый в эконометрике и количественных исследованиях) для проверки структурных сдвигов во время введения экономических санкций; б) прогнозы вне выборки для оценки потерь в торговле для ЕС и России. Анализ результатов оценки показал, что в 2014 г. санкции на экспорт в Россию вводились выборочно, вызывая незначительные сбои. Санкции ЕС сохраняют видимость и сводятся к простым жестам. Сделан вывод о том, что напротив, российские контрсанкции против импорта из ЕС вызвали серьезные потери для торговли ЕС. Полученные результаты подчеркивают сложность навязывания санкций на экспорт и подтверждают ценность санкций как сигнального устройства, а не экономического оружия. Справочник включает три взаимосвязанных раздела, в которых последовательно рассматриваются следующие вопросы: экономические санкции в XXI веке; база данных о глобальных санкциях; целевые санкции ООН; экономические санкции, политическая стабильность и насилие; эффект внутренней оппозиции международных санкций; приостановление торговых преференций как экономическая санкция; экономические санкции ВТО; негативные и позитивные санкции; туризм и санкции и др. В целом книга представляет интересный материал для специалистов, изучающих эффективность экономических санкций и их последствий.

**5. Брайан Р. Эрли «Отмененные санкции: Объяснение, почему экономические санкции терпят неудачу». (Bryan R. Early (2015). Busted Sanctions: Explaining Why Economic Sanctions Fail. Stanford University Press. ISBN 978-0-8047-9432-9).** Данная книга объясняет почему экономические санкции, введенные самой могущественной страной мира, имеют плохой послужной список. Это является демонстрацией провала США по санкциям и связано с поведением внешних игроков, нарушающих торговые санкции и иностранную помощь. Коммерческие мотивы, в первую очередь, побуждают третьи страны расширять свою торговую деятельность, несмотря на политические мотивы. Анализ свидетельствует, что нарушение санкций, в

конечном счете, подрывает усилия международного сообщества. Реакция третьих стран на экономические санкции может варьироваться в широком диапазоне. Экономические санкции могут дать сбой и привести к дополнительным затратам на торговлю третьих стран с целевыми государствами. В тоже время, могут создаваться дополнительные прибыльные коммерческие возможности и многие государства готовы воспользоваться ими. Санкционные споры имеют, прежде всего, политический характер и побочные эффекты, которые тоже оказывают влияние на реакцию третьих стран. Третьи государства могут получить существенную выгоду от торговли, нарушающей санкции. Государства, которые, скорее всего, станут нарушителями торговых санкций, это те, которые предлагают фирмам наиболее выгодные возможности для отмены санкций. Противоречивый вывод из всего этого заключается в том, что политическое прикрытие, предлагаемое союзническими отношениями, также может помочь другим союзникам государств-отправителей сформировать выгодные площадки для фирмы, нарушающей санкции.

**6. Масахико Асада «Экономические санкции в международном праве и практике» (Masahiko Asada (2020). *Economic Sanctions in International Law and Practice*. Routledge. ISBN: 978-0-429-05298-9).** Книга состоит из 3 разделов. В первом разделе рассматриваются определение и юридическое обоснование санкций, ООН и санкции, последствия санкций для прав человека и законность экстерриториальных санкций. Второй раздел объединяет следующие вопросы: история применения санкций, реализация санкций США, реализация санкций ЕС, реализация санкций Японией. Третий раздел объединяет следующие тематические исследования с привязкой к конкретным странам-мишеням: Северная Корея: проектирование, реализация и уклонение, Иран: роль и эффективность санкций ООН, Сирия: вопрос химического оружия и автономия санкций, Россия: Крымский вопрос и автономные санкции. В данной книге обсуждаются текущие правовые и политические проблемы, с которыми столкнулось международное сообщество при создании и осуществлении экономических санкций, которые являются одним из самых мощных инструментов. Книга возникла в результате серии небольших симпозиумов, проведенных в 2015-2017 года в Японии и во Франции. Наибольший интерес представляет третья часть книги, где собраны тематические исследования, имеющие современную актуальность. В качестве первых санкций в целях ядерного нераспространения были выдвинуты против Северной Кореи, и специалисты отмечают, что санкции были самыми строгими при наличии серьезных пробелов. Относительно санкций против Ирана, эксперты отмечают что внутривнутриполитическая система стала ключом к успешным санкциям. Относительно санкций против Сирии, эксперты отмечают уникальность случая в этом отношении, поскольку СБ ООН не смог принять резолюцию из-за российского вето, что неизбежно привело к введению автономных санкций. Санкции против России представляет собой уникальный случай санкций против одного из постоянных членов СБ ООН. В



целом, книга представляет собой очерков по теории и практике экономических санкций.

**7. Агата Демарэ «Обратный эффект: как санкции меняют мир вопреки интересам США».** (Agathe Demarais (2022). *Backfire: How Sanctions Reshape the World Against U.S. Interests*. Columbia University Press. ISBN 9780231553339). Автор книги работала финансовым атташе в казначействе Франции в Москве, во Французском посольстве в Бейруте. Эта книга не за и не против санкций. В предисловии книги описывается ситуация, сложившаяся в Судане в 2002 году, Конгресс США обсудил введение санкций в отношении энергетических фирм, работающих в этой африканской стране. Рассуждения американских законодателей были просты – угрозы санкций может быть достаточно, чтобы убедить суданское правительство пойти на переговоры с повстанцами. Скептики оценили это, будто Вашингтон собирался выстрелить себе в ногу. Структурно книга объединяет три раздела. В первом разделе представлен следующий материал: краткая история санкций; эра финансовых санкций; почему санкции иногда работают, но чаще неудачно. Второй раздел включает следующее: побочный ущерб; когда иностранные фирмы попадают под перекрестный огонь; когда санкции рушат мировые товарные рынки; когда российские газопроводы разделяют союзников. В заключительной части излагаются следующие вопросы: нарушение санкций; снижение доллара – рост цифровых валют и других резервных валют; будущее высоких технологий – является ли экспортный контроль завтрашними санкциями; когда санкции работают слишком хорошо. Неудивительно, что санкции стали столь популярны в последние два десятилетия, поскольку они обладают множеством преимуществ. С одной стороны, они являются быстрым способом для США продемонстрировать решимость и наказать плохое поведение. С другой, санкции являются дешевым политическим инструментом. Для разработки санкций нужны услуги небольшой группы экспертов. Бремя санкций США ложится на транснациональные корпорации и банки, которые несут затраты на соблюдение требований. Прямые издержки санкций также кажутся низкими, что делает их более привлекательными, чем другие формы принуждения, например, военное вмешательство. Санкции заполняют пустоту в дипломатическом пространстве между неэффективными декларациями и потенциально смертоносными действиями. Дополнительным бонусом является то, что санкции, как правило, усиливают рейтинги одобрения деятельности политиков, которые их навязывают. У политиков есть избиратели, которым нужно угодить, и решительные действия по защите своих интересов обычно поддерживают голосование. Автор отмечает, что настоящая история санкций еще не рассказана: дни односторонних санкций США сочтены и Америке понадобится другое оружие помимо санкций.

**8. Марк Дэниел Джегер «Принудительные санкции и международные конфликты: социологическая теория».** (Mark Daniel Jaeger (2018). *Coercive Sanctions and International Conflicts: A Sociological Theory*. Routledge. ISBN: 978-1-315-52243-2). Книга состоит из двух

взаимосвязанных частей. В первой части рассматривается комплекс вопросов, связанных с концептуализацией международных санкционных конфликтов, в том числе: санкции, теория санкций, концептуализация санкций, теории международных санкций как инструментов принуждения, социологическая теория принудительных международных санкций, санкции, риск и опасность, секьюритизация как причинный механизм, структурный анализ и отслеживание процессов и др. Вторая часть книги охватывает следующие вопросы: кнут и пряник конфликта, конфликты с тремя разными стратегиями санкций, поляризация комбинированных санкций, эскалация и деэскалация конфликта, развитие стратегий санкций и т.п. Исследование теоретизировало социальные условия на основе представления о принудительных санкциях как социальных фактах. Санкции приобретают значение в рамках конфликта и в конечном счете способствуют его трансформации, но не передают логику «затраты/выгоды» по простой модели коммуникации «отправитель-получатель». Концептуально исследование предполагает, что при изучении санкционных конфликтов следует переориентировать внимание на социальные процессы и практики, что предполагает разработку возможных сценариев будущего. В процессе исследования была развернута триада взаимосвязанных элементов, каждый из которых затрагивал более конкретный вопрос: во-первых, какое значение санкции приобретают в конфликте; во-вторых, как санкционные конфликты конструируются в обществе; в-третьих, относительно трансформации конфликта и влияния конкретных стратегий санкций. Детальное рассмотрение компонентов, которые потенциально могут повлиять на возможности трансформации конфликта, позволили бы создать более точную аналитическую модель санкций и конфликтов, а также трансформации конфликтов.

**9. А. Купер Друри «Экономические санкции и президентские решения: модели политической рациональности».** (A. Cooper Drury (2005). *Economic Sanctions and Presidential Decisions: Models of Political Rationality*. ISBN 978-1-4039-7695-6 DOI 10.1057/9781403976956). Автор определил цель книги, как устранение пробела в понимании природы экономических санкций и поиск ответа на вопрос: какие условия заставляют президента США инициировать, а потом изменять экономические санкции? Первым шагом является переоценка эффективности санкций. Она показала, что общепринятые взгляды неспособны объяснить эффективность санкций, поэтому следующим логическим шагом стало исследование условий, которые приводят к использованию санкций. Отмечается, что большинство экспертов неточно понимают экономические санкции, поскольку не считают их нормальным типом внешней политики, воспринимают их как экономические проблемы, а не инструменты внешней политики. Лицо принимающее решение располагает следующими вариантами – пропаганда, дипломатические, экономические санкции и военные санкции. Автор объясняет условия, при которых президент США применяет экономические санкции, опираясь на принудительную дипломатию, внутренние императивы и когнитивные

процессы. Содержание книги представляет последовательность следующих тем: экономическое принуждение в теории и практике; оценка эффективности санкций; почему президент США применяет санкции; когда президент вводит санкции; существует ли предвзятость целей; внутренние ограничения и стимулы. Автор определил пять условий эффективности санкций: 1) проблемные объекты чаще поддаются санкциям; 2) санкции, дорогостоящие для цели, обычно оказываются более эффективными; 3) при сотрудничестве нескольких стран при вводе санкций против объекта без помощи международной организации, санкции менее эффективны; 4) если отправитель при введении санкций беспокоится о национальной безопасности, вероятность успеха этих усилий снижается; 5) экономическое принуждение против демократических целей, как правило, более эффективно, чем недемократических целей.

**10. Тамаш Сабадос «Экономические санкции в международном частном праве ЕС». (Tamás Szabados (2019). *Economic Sanctions in EU Private International Law*. HART PUBLISHING. ISBN 978-1-50993-353-2).**

Экономические санкции – это «аномалии» в логике свободной торговли и некоторые авторы ставят под сомнение их эффективность и подвергают критике. Европейский Парламент еще в 1982 году установил, что: а) экономические санкции имеют историю неудач; б) экономические санкции оказались совершенно неудовлетворительными в качестве средства достижения внешнеполитических целей, хотя они могут быть подходящими для дополнения других форм воздействия; в) вряд ли какое-либо государство может быть побуждено экономическим давлением к радикальным изменениям в своей политике. Такое давление с гораздо большей вероятностью приведет к ужесточению политических отношений, в то время как национальная экономика государства, вводящего санкции, и третьих стран, не вовлеченных напрямую, очень часто подвергается столь же серьезному воздействию и серьезному ущербу, как и национальная экономика государства, налагающего санкции; г) существует множество способов обойти и подорвать экономические санкции. Как бы строго они не контролировались, невозможно гарантировать, что они будут выполняться абсолютно последовательно и без исключений. Автор составил и использует таблицу обширных правовых источников по экономическим санкциям, включающих Резолюции Генеральной Ассамблеи ООН, Совета Безопасности ООН, решения Международного Суда, решения Суда Европейского Союза, законодательство ЕС, акты других международных организаций, инструменты национального законодательства (Франции, Германии, Ирака, Ирландии, Испании, Швейцарии, Великобритании, США), а также примеры национального прецедентного права. В качестве основного вывода, автор выделяет то, что последовательное применение экономических санкций в частноправовых спорах необходимо для того, чтобы гарантировать правовую определенность для договаривающихся сторон, а также единый внешнеполитический подход на уровне ЕС.

**11. Сесиль Фабр «Управление экономическим государством: права человека, санкции и условия». (Cécile Fabre (2018). *Economic Statecraft: Human Rights, Sanctions, and Conditionality*. Harvard University Press. ISBN 9780674979635).** В структуру книги входят следующие вопросы: права человека; экономические санкции; вторичные санкции; условная помощь; суверенное кредитование и прощение долгов. Экономическое государственное управление является ключевым инструментом реализации геополитических целей. Оно регулярно использовалось и продолжает использоваться как средство обеспечения прав человека. Введение торговых и финансовых санкций и тем самым вмешательство в свободную торговлю, находится в противоречии с правом человека на частную собственность. Таким образом, эффективность экономических санкций можно обозначить следующим образом: 1) первичные и вторичные всеобъемлющие санкции (против всех агентов и/или всех товаров – **нет**. 2) первичные и вторичный целевые санкции (в отношении некоторых агентов и/или некоторых категорий товаров: а) **да**, фактически является обязательным в отношении: - узко специализированных товаров (например, оружие); - товаров специального назначения; - косвенно способствующих товаров, льготных (частных) кредитов; - широких стратегических товаров. б) **предположительно нет**, в большинстве случаев в отношении товаров двойного назначения (например, нефти). Автор указывает, что более всеобъемлющих санкций против широкого круга кубинских, российских и северокорейских агентов нет.

**12. Нефью Ричард «Искусство санкций: взгляд с места событий». (Nephew Richard (2017). *The Art of Sanctions: A View from the Field*. Columbia University Press. ISBN 9780231542555 DOI 10.7312/neph18026).** Автор последовательно описывает события, связанные с введением санкций против Ирака и Ирана. Содержание книги представлено следующими разделами: после введения, автор тщательно анализирует и определяет термины предметной области, затем рассматривает Ирак и борьбу с Ираном, связывает введение санкций со страданием населения государств-мишеней, интенсивное давление на Иран и поворот к реальным переговорам, в поисках переломных моментов. Книга заканчивается главой, где приведена точка зрения автора на взгляд в будущее. Книга начинается с напоминания о том, насколько ощутимы современные санкции по сравнению с изменениями в прошлом веке. Результатом исследований выступает шестиэлементный процесс развития индивидуального подхода к введению санкций: определение цели и минимально необходимых мер по исправлению ситуации; необходимо понять природу цели, включая его уязвимости, последовательность интересов, приверженность и готовность поглотить страдания; разработка стратегии тщательного, методического и эффективного усиления страданий населения в тех областях, которые являются уязвимыми; контроль исполнения стратегии и постоянный пересмотр первоначальных предложений о целевом состоянии, эффективности страданий и улучшения стратегии; формирование целевого состояния с четким изложением условий, необходимым для снятия части

санкций и ведения переговоров, необходимых для заключения соглашения; не исключена возможность того, что, несмотря на тщательную разработку стратегии, государство, использующее санкции может потерпеть неудачу из-за неэффективности стратегии, непонимания цели усиление способности сопротивления.

**13. Хаппольд Мэтью, Иден Пол «Экономические санкции и международное право». (Happold Matthew, Eden Paul (2016). *Economic Sanctions and International Law*. Hart Publishing. ISBN 9781782254737).**

Книга рассматривает использование санкций и эмбарго в качестве инструментов внешней политики или экономической войны. В настоящее время действуют 17 режимов санкций ООН и 37 режимов санкций Европейского Союза, а также другие режимы, введенные государствами, действующими в одностороннем порядке или под эгидой других международных организаций. Однако в то же время подобная практика редко вызывает споры или оспаривается. Целевые или «умные» санкции против физических и юридических лиц, в частности, замораживание активов и запрет на поездки, введенные СБ ООН и государствами-членами, действующие с его санкции, подвергаются постоянному оспариванию. Это происходит потому, что они сводят тех, на кого они распространяются, до состояния нищеты. Потому что они основаны на нераскрытых доказательствах и не подлежат судебному пересмотру. Санкции подвергаются критике как противоречащие международному праву и нарушают права государств, против которых они направлены такие меры. Авторы указывают на важное обстоятельство, что широкомасштабные экономические санкции, введенные против Ирана и Сирии со стороны ООН и ЕС, являются частью одного из главных правовых и политических противоречий нашего времени. Они также поднимают важные вопросы о соотношении между общим международным правом и универсальными и региональными механизмами коллективной безопасности. С 2006 года ООН и ЕС приняли программы санкций в отношении Ирана, ссылаясь на иранскую программу ядерного обогащения в качестве причины. В отношении Сирии, где с 2011 года идет война, СБ ООН не принял ни одной резолюции о введении санкций против Сирии, в то время как Совет ЕС ввел свои собственные санкции против этого государства. Книга состоит из 9 разделов, в которых рассматриваются следующие проблемы: экономические санкции и международное право; санкции и фундаментальные права государств; сфера действия санкций ООН и ЕС против Ирана и Сирии; взаимодействие между санкциями, их полномочиями и фундаментальными правами государств; правовая основа санкций ЕС и коллективная безопасность; дела о санкциях в европейских судах; санкции США и заявления об исключении из перечня, судебный контроль и секретные доказательства; санкции и коммерческое право. Авторы указывают, что санкции имеют долгую историю. Современные санкции и меры, используемые для их обеспечения, являются прямыми наследниками мер, применяемых во время войны или репрессий и соответствующих норм международного и

внутреннего права о торговле с врагом, торговых эмбарго, блокады, контрабандные меры, репрессалии, призовые и торговые договоры. Санкции препятствуют торговле и могут дать конкурентам из других юрисдикций, которые не ввели такие же санкции, преимущество. Однако они являются неизбежным фактом политической и коммерческой жизни, поскольку они являются одним из немногих инструментов правоприменения и предотвращения, доступных в международном праве.

## **1.6. Эффективность санкций (5)**

**1. Элизабет Розенберг, Закари К. Голдман, Дэниел Дрезнер, Джулия Соломон-Штраусс «Новые инструменты воздействия экономической войны и эффективность современных финансовых санкций США» (Elizabeth Rosenberg, Zachary K. Goldman, Daniel Drezner, Julia Solomon-Strauss (2016). The New Tools of Economic Warfare Effects and Effectiveness of Contemporary U.S. Financial Sanctions. <https://www.lawandsecurity.org/wp-content/uploads/2016/04/FINAL-CNASReport-EconomicWarfare-160408v02.pdf> (дата доступа 14.01.24).** Материал состоит из 5 глав в следующей последовательности: введение, современный ландшафт санкций; новые данные о последствиях санкций, направленных против государств; эффекты санкций против транснациональных угроз; вызовы современных санкций для США и мировая финансовая система; политические рекомендации относительно будущего применения санкций США. Авторы отмечают, что целевые финансовые санкции переместились в центр национальной политики безопасности США. Они стали применяться как в борьбе с терроризмом, так и против распространения оружия массового уничтожения и территориальной агрессии. Санкции часто являются тем инструментом, к которому политики США обращаются в первую очередь при реагировании на кризисы и постоянное управление угрозами. Но также быстро, как и сами санкционные инструменты, развивались показатели их воздействия и оценки эффективности. В результате финансовые санкции часто не интегрируются в рамках общих стратегических подходов к проблемам политики иностранных государств. Авторы приходят к выводу, что санкции 21-го века не оказывают существенного влияния на целевой ВВП страны-мишени. Однако они оказывают мощное влияние на иностранные инвестиции, коррупцию, простоту ведения бизнеса и другие меры взаимодействия с международным финансовым сообществом. Но существенно сложнее измерить воздействие санкций на негосударственные субъекты, такие как торговля наркотиками, террористы и киберпреступники. Поскольку данные о их деятельности недоступны, но тем не менее, неофициальные данные на всех уровнях международного сообщества служат доказательством того, что санкции оказывают влияние и на них. Авторы сделали ряд выводов об эффективности

санкций с использованием трех общих критериев: а) способность осмысленно формировать политическую среду и баланс политических рычагов; б) стимулирование соответствующих сообществ (внутренних и международных) к согласованным действиям, в том числе путем обмена сообщениями относительно цели санкций; в) достижение отдельных политических целей в поддержку общей политики США. Предложенные критерии должны определять разработку и введение санкций США в будущем. Эффективная политика санкций должна учитывать также негативные последствия, которые могут появиться. На фоне усиления таких стран, как Россия и Китай, фонды международной финансовой системы напоминают, что размер, ликвидность и целостность финансовой системы США относят к числу наиболее важных стратегических активов.

**2. Саид Гассеминжад «Финансовая анатомия экономических санкций» (Saeed Ghasseminejad (2018). A Financial Anatomy of Economic Sanctions. Social Science Electronic Publishing; Publons; Research Square; Elsevier BV (ISSN 1556-5068), SSRN Electronic Journal, 2018. DOI: 10.2139/ssrn.3214012).** Материал содержит комплексный анализ экономических санкций по отношению к Ирану ввиду наличия у него развитых финансовых рынков, разнообразных и продолжительных санкций. Сделана попытка измерить эффект введения и снятия санкций с биржевых фирм целевой страны и исследовать влияние санкций на деятельность компаний с государственным участием. Особое внимание направлено на исследование влияния санкций на события ядерной сделки 2015 года, которое привело к отмене некоторых введенных санкций. Сделан вывод о том, что прямые санкции приводят к совокупным краткосрочным и долгосрочным отрицательным последствиям, создают отрицательную доходность. В случае введения нескольких санкций со стороны различных юрисдикций, эффект от первой санкции считается самым сильным. Это указывает на то, что широко распространенное мнение о том, что односторонние санкции неэффективны, не соответствуют действительности. В свою очередь, снятие санкций приводит к положительной аномальной доходности. Таким образом, фирмы, подвергшиеся экономическим санкциям, сталкиваются с возросшим риском, ухудшением показателей рентабельности. Приведена расширенная статистика, характеризующая деятельность фирм до ввода и снятия санкций.

**3. Франческо Джумелли, Пол Иван «Эффективность санкций ЕС. Анализ Ирана, Беларуси, Сирии и Мьянмы (Бирмы)». (Francesco Giumelli, Paul Ivan (2013). The effectiveness of EU sanctions an Analysis of Iran, Belarus, Syria and Myanmar (Burma). EPC Issue Paper no.76. ISSN 1782-494X).** В данной работе исследуются способы оценки эффективности ограничительных мер. Для этого предлагается четырехэтапный процесс оценки, который рассматривает: роль санкций в общей внешнеполитической стратегии; цель и задачи политики с точки зрения принуждения, ограничения и сигнализации; влияние санкций и понесенные затраты; сравнительная

полезность санкций. Применение четырехэтапной модели (процедуры) позволяет оценить эффективность ограничительных мер. Утверждается, что существует необходимость тщательной оценки того, чего должны достичь санкции, чтобы построить надлежащие ожидания, на основании которых можно будет судить об их эффективности. Фазу разработки санкций рекомендуют дополнить контрольным списком целей и ожиданий в отношении принуждения, ограничения и сигнализации.

**4. «Справочник Рутледжа по политической экономии санкций. Под редакцией Ксении Киркхэм». (The Routledge Handbook of the Political Economy of Sanctions. Edited by Ksenia Kirkham. (2024). Routledge. ISBN 9781003327448 DOI: 10.4324/9781003327448).** Книга состоит из 5 разделов. В первом разделе «Теоретические и исторические аспекты санкций» рассматриваются: оценка эффективности санкций, краткий обзор исторического и текущего использования односторонних санкций, теоретические аспекты санкций, теоретическая идентификация механизмов санкций, сдерживание и случай России. Второй раздел «Политическая экономия санкций» включает: международные санкции в отношении нефти; почему некоторые целевые государства способны их избежать, финансовые черные списки и возврат к неизбирательному подходу санкций, прекращение санкций; действующие лица, процессы и последствия, насилие на расстоянии: исправление недальновидности международного права и видение экономического принуждения, когда санкции терпят неудачу, односторонние санкции как тормоз устойчивого развития, В третьем разделе «Целевые государства: голоса государств, подвергшихся санкциям» предлагается следующий материал: случай современного вестерна – санкции против России, санкции США и китайская политическая экономия, иранские дискурсы и практика в отношении санкций США, политическая экономия санкций: пример Кубы, непредвиденные последствия санкций Африканского союза. Четвертый раздел «Третьи стороны: влияние вторичных санкций» содержит: последствия изменения политики санкций Японии и Кореи, санкционное наступление США: последствия для «третьих сторон» и трансатлантические отношения, влияние западных санкций на глобальные цепочки поставок, как третьи страны реагируют на сырьевые санкции, обзор вторичных санкций: Турция под прикрытием западных экономических санкций, развивающаяся Индия и санкции: баланс норм и интересов. В заключительном, пятом разделе «Горячие дебаты: правовые аспекты санкций», рассматриваются следующие вопросы: гуманитарное воздействие односторонних санкций, законность вторичных санкций США. Экономические санкции появлялись в разных типах и формах на протяжении всей истории, государства использовали различные инструменты невоенного принуждения, чтобы заставить противников сменить свой курс. Санкции и сегодня остаются очень мощным инструментом внешней политики. Целью данного справочника является отслеживание всех новых явлений в санкционной политике, оценки их эффективности и побочных эффектов для



отправителей санкций, стран-целей и «третьих» сторон. Последовательность различных кризисов указала на ограниченность неолиберальной модели роста, кризис еврозоны, многочисленные экологические катастрофы, вспышку пандемии COVID-19 и новые военные конфликты – изменили обычные модели глобализации и способствовали эскалации напряженности во всем мире. Хотя санкции кажутся правдоподобным и эффективным политическим и экономическим оружием, их многочисленные подобные эффекты заставляют пересмотреть существующие подходы, планы и политику.

**5. Ксения Киркхэм «Политическая экономия санкций: устойчивость и трансформация в России и Иране». (Ksenia Kirkham (2022). The Political Economy of Sanctions: Resilience and Transformation in Russia and Iran. Palgrave Macmillan. ISBN 978-3-031-04055-9 <https://doi.org/10.1007/978-3-031-04055-9>).** Это еще одна книга Ксении Киркхэм, посвященная экономическим санкциям. Структура книги состоит из 5 частей и 11 разделов. Последовательно рассматриваются следующие вопросы. Часть 1 «Теоретическая идентификация механизмов санкций» включает следующие вопросы: режим государства всеобщего благосостояния как теоретическое объяснение; режим государства всеобщего благосостояния как аналитический инструмент. Часть 2 «Институциональный дизайн»: Россия – институциональный дизайн; Иран: институциональный дизайн. Часть 3 «Материальные возможности»: Россия – материальные возможности; Иран – материальные возможности. Часть 4 «Культурное лидерство»: Россия – культурное лидерство, Иран – культурное лидерство. Часть 5 «Воспроизводство режима государства всеобщего благосостояния»: введение, контррелегемонистские тенденции, некоторые мысли для будущих исследований и рекомендации. Утверждается, что использование санкций в международной политической экономии значительно возросло. Санкции являются наиболее важными инструментами внешней политики США по отношению к государствам-соперникам, таким, как Россия, Иран, Китай, Венесуэла и Куба и др. Данная книга базируется на сравнительном анализе России и Ирана в условиях санкций. Несмотря на продолжающееся введение санкций, целевые государства стали более демократичными и заняли более агрессивную позицию по отношению к Западу. В книге представлен широкий список использованной литературы.

## **1.7. Оценки санкций против России (4)**

**1. Ричард Коннолли «Ответ России на санкции: как западное экономическое управление меняет политическую экономию в России». (Richard Connolly (2018). Russia's Response to Sanctions: How Western Economic Statecraft is Reshaping Political Economy in Russia. Cambridge University Press. ISBN 978-1-108-41502-6 DOI: 10.1017/9781108227346).**

Книга написана Ричардом Коннолли, ассоциированным исследователем программы «Россия и Евразия» Королевского института международных отношений (Chatham House), он представил первый углубленный анализ воздействия санкций на российскую политическую и экономическую ситуацию. Он подробно описывает западные санкции, направленные против энергетического, оборонного и финансового секторов, а также исследует как западные санкции заставили сформулировать новую политику и меры реагирования, которые позволили адаптироваться к новым вызовам и обстоятельствам. Это привело к росту роли государства в экономике и ускорить усилия по изменению внешнеэкономических связей в сторону Азии. Автор проводит анализ того, как политическая экономия в России и природа интеграции в мировую экономику фундаментально изменила форму, и это является свидетельством зарождения новой системы политической экономии. И это является весьма важным элементом для понимания будущей траекторией развития России. Материал книги изложен в следующей последовательности: санкции и политическая экономия; Российская система политической экономии; западные санкции и ответ России; санкции и энергетика; санкции и оборонная промышленность; санкции и финансовая система. Санкции, введенные западными державами и их союзниками, оказали мощное влияние на эволюцию политической экономии в России, заставили пересмотреть характер взаимоотношений с мировой экономикой. Значительные усилия направлены на построение экономики, основанной на развитии внутреннего потенциала в стратегических отраслях, а также путем развития более тесных связей с альтернативными источниками технологий и капитала. Политики сократили влияние введенных санкций на функционирование и результативность российской экономики и это смягчило экономическое и политическое давление. Автор высказывает мысль о том, что долгосрочное воздействие российского стратегического ответа на санкции – в лучшую или худшую сторону – еще предстоит выяснить. То, что кажется почти несомненным, заключается в том, что политическая экономия в России значительно изменила форму. Самый важный вывод заключается в том, что первоначально санкции вызвали некоторые сбои, воздействие на целевые сектора уменьшилось после относительно короткого периода. В энергетической отрасли санкции не оказали заметного негативного влияния на производство нефти и газа. Использование государственных ресурсов и доступа к альтернативным источникам иностранного капитала позволили не только выжить, но и начать беспрецедентную программу инвестиций и приобретений. В оборонной промышленности санкции нанесли определенный ущерб, но Россия добилась значительного прогресса во внутренней военной модернизации и выполнила свои экспортные обязательства. Финансовая система испытала значительные потрясения, однако решения монетарных властей позволили смягчить санкционные последствия и тем самым были созданы условия для более самостоятельной финансовой системы.

**2. Клэр Миллс «Санкции против России. Исследовательский брифинг, 16 ноября 2022 г.».** (Claire Mills (2022). *Sanctions against Russia. Research Briefing* 16 November 2022. <https://researchbriefings.files.parliament.uk/documents/CBP-9481/CBP-9481.pdf> (дата доступа 16.01.24)). Содержание документа представлено следующей последовательностью: режим санкций Великобритании до 2022 года; что послужило причиной новых санкций?; какие санкции вводит Великобритания?; координация с союзниками; наложение вторичных санкций третьих стран. Подробно рассматривается состав санкций вводимых Великобританией: первый и второй пакеты санкций; переходящая программа санкций; Путин, Лавров и члены их семей попали под санкции; финансовые санкции; транспортные санкции; дальнейшие торговые санкции и т.д. Пункт, посвященный координации действий с союзниками, подробно описывает взаимодействие с США, Европейским Союзом и другими странами. Речь идет о введении первоначальных санкций, введенных США и ответ на российскую аннексию, а также уклонение от санкций. Подробным образом перечисляются санкции, последовательно введенные против юридических и физических лиц. Упоминается также режим киберсанкций Великобритании за кибератаки на офисы Организации по запрещению химического оружия в 2018 году и парламент Германии в 2015 году.(с.9),

**3. Сюзанна Оксеншерна, Пер Олссон «Экономические санкции против России: последствия и перспективы успеха».** (Susanne Oxenstierna, Per Olsson (2015). *The Economic Sanctions Against Russia: Impact and Prospects of Success*. September 2015. FOI-R--4097—SE. ISSN1650-1942. <https://www.foi.se/rest-api/report/FOI-R--4097--SE> (дата доступа 17.01.24)). Основной целью данного отчета является качественная оценка последствий экономических санкций, введенных ЕС и США против России. В докладе исследуется влияние санкций и выполнение ими своих задач по навязыванию издержек российской экономике в целях изменения политики России. Главный вывод заключается в том, что целевые экономические санкции ЕС и США внесли свой вклад в увеличение стоимости российской экономики в сочетании с другими факторами, но они до сих пор не убедили Россию изменить свою политику. Факторами, усиливающими эффект санкций, являются следующие: падение цен на нефть, обесценивание рубля и ослабление условий торговли и политизированная экономическая система. Отмечается, что политическая система распределения ресурсов и ренты гарантирует выживание режима и представляет собой угрозу успеху санкций. Для решения этой проблемы необходимо использовать стратегии выхода.

**4. Политика санкций: цели, стратегии, инструменты: хрестоматия.** Издание 3-е, переработанное и дополненное / [сост. И.Н. Тимофеев, П.И. Чуприянова, К.В. Троцкая]; Российский совет по международным делам (РСМД). —М.: НП РСМД, 2023. — 536 с. ISBN 978-5-6048843-3-1. Невозможно не указать ценный информационный ресурс, каким является сборник материалов, подготовленный экспертами РСМД

Сейчас важно осознать происходящее в попытке заглянуть в будущее. В 2014–2021 гг. Россия фактически приспособлялась к западным санкциям, стремясь избежать дополнительных и вторичных санкций. Крупный бизнес избегал рисков (например, большие банки отказывались работать в Крыму). Были введены регуляторные точечные исключения в раскрытии информации. Создавались обособленные «санкционные» структуры. Однако после 2022 г., когда большое количество крупного российского бизнеса и подавляющая по активам доля банков оказались под массивными рестрикциями Запада, прежняя политика утратила смысл. Требуется реформирование государственной политики в области санкций. В 2022 г. стало ясно, что санкции Запада не такие всемогущие. Массивное давление не смогло сломать и изолировать экономику России. Возникает шанс изменения сложившейся системы, при которой в международных расчетах доминируют доллар и евро (с долями порядка 40% каждая). Это основной фактор, который давал и дает США, а теперь и ЕС, возможность экстерриториального насаждения своего санкционного диктата.

## ГЛАВА 2. АНАЛИЗ ИСТОРИЧЕСКОГО РАЗВИТИЯ САНКЦИЙ И ИХ ПРЕОБРАЗОВАНИЙ

Экономические санкции начали использовать задолго до I Мировой войны и задолго до XX века [1-4 и др.]. Первым упоминанием об экономических санкциях принято считать Мегарскую псефизму (Мегарский указ) – решение народного собрания Древних Афин 433-432 годов до н.э., которое запрещало купцам Мегары торговать на рынках Аттики, а их кораблям – заходить в порты Афинского морского союза. По сути Мегаре была объявлена морская блокада [5].

Особый интерес для нас представляет литература, в которой рассматриваются санкции, введенные Советом Безопасности ООН [6-13]. Глава «История и эффективность экономических принуждений (The History and Effectiveness of Economic Coercion)» автора Ирины Богдановой [14] в монографии «Unilateral Sanctions in International Law and the Enforcement of Human Rights», содержит исторический обзор используемых санкций в международном праве и защите прав человека. Временной охват истории экономического принуждения включает античную Грецию, Римскую и Византийскую империи, средние века, Первую мировую войну, период между Первой и Второй мировыми войнами, холодную войну и т.д.

Дополнительным источником исследования исторических аспектов санкций является книга “Economic Sanctions: Examining Their Philosophy and Efficacy” [15]. Приведем таблицу истории экономических санкций в следующей таблице.

Таблица 1. История экономических санкций

Отправитель	Цель	Активные годы	Проблемы
Афины	Мегара	432 г. до н.э.	Мегарское посягательство на священную афинскую землю и похищение афинян
Рим	Иерусалим	72 г. н.э.	Римское завоевание Иерусалима
Король Англии Стефан	Болдуин де Редверс	1138	Восстание против короля Англии Стефана
Джеффри Анжуйский	Руан	1144 г.	Завоевание Нормандии Джеффри Анжуйским

Отправитель	Цель	Активные годы	Проблемы
Монголия	Багдад	1257 г.	Отказ Багдада на требование Монголии о почтении
Американские колонии	Британия	1765 г.	Колониальный бойкот британских товаров в ответ на Закон о гербовых марках
Американские колонии	Британия	1767-1770 гг.	Колониальный бойкот британских товаров в ответ на британское регулирование американской торговли
Британия Франция	Франция Британия	1792-1815 гг.	Морская блокада британцами и самоблокада континента французами
США	Великобритания	1812-1814 гг.	Эмбарго США на британские товары в ответ на воинственные действия британцев
Соединенные Штаты	Конфедеративные Штаты	1861-1865 гг.	Приказ Линкольна о морской блокаде Конфедеративных Штатов
Пруссия	Франция	1870 г.	Прусская осада Парижа в рамках франко-прусской войны
Версаль	Париж	1871 г.	Гражданская война между Парижской Коммуной и Версалем

*Источник:* Hossein Askari, John Forrer, Hildy Teegen, Jiawen Yang (2003). Economic Sanctions: Examining Their Philosophy and Efficacy. Praeger Publishers.p. 6. ISBN 1-56720-542-9

Рассмотрим инициированные санкции в период с 1915 по 2000 г.г, приведенные в следующей таблице.

Таблица 2. Инициированные эпизоды санкций, их стоимость и мировой экспорт (1915–2000 гг.) [16]

Год	Количество дел, возбужденных за последние пять лет	Сумма годовых расходов на текущие дела (млрд долларов)	Общий мировой экспорт (млрд долларов)
1915	1	0,84	15
1920	2	0,45	Н.д
1925	2	0	25
1930	0	0	30
1935	3	0,09	Н.д.
1940	3	0,40	25
1945	1	0,72	50
1950	8	1,09	65
1955	5	1,11	90
1960	10	1,74	125
1965	15	2,28	180
1970	4	2,44	300
1975	13	2,41	820
1980	25	6,81	1,880
1985	15	4,97	1,840
1990	20	28,90	3,330
1995	34	30,75	4,945
2000	13	27,21	6,375

*Источник:* Economic sanctions reconsidered / Gary Clyde Hufbauer . . . [et al.].—3rd ed 2007. P.17 ISBN 978-0-88132-407-5

Анализ данных таблицы позволяет сделать главный вывод – с ростом количества объявленных санкций, возрастают годовые затраты на поддержку санкций. Если в 1960 году затраты на поддержку санкций по отношению к общему мировому экспорту составляли 0,01 %, то в 1995 году это соотношение составило только 0,006 % при росте мирового экспорта до 4945 млрд. дол.

В следующей таблице приведен хронологический обзор экономических санкций, имеющих отношение к СССР и РФ (1914-2000 г.г.)

Таблица 3. Хронологический обзор экономических санкций, имеющих отношение к СССР и РФ (1914-2000 г.г.) [16]

Основной отправитель санкций	Целевая страна-получатель санкций	Годы активности	Цели страны отправителя
Великобритания	Россия	1918-1920	1) Возобновить поддержку союзников в Первой мировой войне. 2) Дестабилизировать большевистский режим
Великобритания	СССР	1933	Освобождение двух граждан Великобритании
СССР	США, Великобритания, Франция	1948-1949	1) Предотвратить образование Правительство Западной Германии 2) Ассимилировать Западный Берлин в Восточную Германию.
СССР	Югославия	1948-1955	1) Вернуться в советский лагерь 2) Дестабилизировать правительство Тито
США (CoCom)	СССР	1948-1994	1) Запрет на стратегические материалы 2) Ослабить военный потенциал советского блока
СССР	Австралия	1954	Репатриация советского перебежчика
СССР	Финляндия	1958-1959	Принятие про-Советской политики
СССР	Китай	1960-1970	1) Отомстить за разрыв с советской политикой 2) Ухудшить китайскую экономический и военный потенциал
СССР	Албания	1961-1965	1) Возмездие за союз с Китаем 2) Дестабилизировать правительство Енвера Ходжа



Основной отправитель санкций	Целевая страна-получатель санкций	Годы активности	Цели страны отправителя
СССР	Румыния	1962-1963	Ограничение экономической независимости
США	СССР	1975-1994	Либерализация еврейской эмиграции
США	СССР	1978-1980	Либерализировать обращение с диссидентами. например, Щаранский
США	СССР	1980-1981	1) Вывести советские войска из Афганистана 2) Ослабить советский военный потенциал
США	СССР	1981-1982	1) Отменить военное положение в Польше 2) Отменить проект газопровода СССР-Европа 3) Ослабить советский экономический и военный потенциал
США	СССР	1983	Возмездие за сбитый корейский авиалайнер
СССР	Литва	1990	Отменить декларацию о независимости
США, ЕС	СССР	1991	Блокирование переворота, восстановление правительства Горбачева
СССР/Россия	Туркменистан	1991-1995	Расширить права русского меньшинства
СССР/Россия	Эстония	1992-1999	Расширить права русского меньшинства
СССР/Россия	Латвия	1992-1999	Расширить права русского меньшинства
СССР/Россия	Украина	1993-1997	1) Признать контроль Российского флота над Черным морем 2) Отказаться от ядерного оружия
СССР/Россия	Казахстан	1993-1996	1) Обезопасить ядерное оружие и военные базовые права

Основной отправитель санкций	Целевая страна-получатель санкций	Годы активности	Цели страны отправителя
			2) Автономия для этнических русских 3) Права в отношении казахстанских энергоресурсов

*Источник:* выборка, составленная авторами на основе Gary Clyde Hufbauer, Jeffrey J. Schott, Kimberly Ann Elliott, Barbara Oegg (2007). *Economic Sanctions Reconsidered*. 3rd Edition. p.20-42.

Таблица 4 Среднее количество наложенных санкций по десятилетию [17]

Годы	Торговля	Финансы	Путешествия	Другие	Всего
1950-е	17	6	6	10	38
1960-е	25	16	9	35	85
1970-е	36	29	8	46	118
1980-е	39	49	10	53	151
1990-е	49	77	19	96	241
2000-е	51	72	41	115	279
2010-е	93	138	83	168	482

*Примечание:* категория «другие» включает, среди прочего, санкции в отношении оружия и военной помощи.

*Источник:* Peter A. G. van Bergeijk (Editor). (2021). *Research Handbook on Economic Sanctions*. Edward Elgar Publishing Limited. ISBN 978 1 83910 272 1 <http://dx.doi.org/10.4337/9781839102721>

Беглый анализ данных таблицы свидетельствует о значительном количественном росте наложенных санкций. В частности, количество санкций по разделу торговли возросло в 7,7 раз (с 17 случаев в 1950-е годы до 93 в 2010-е годы). По разделу финансов картина такая же: рост в 23 раза (с 6 случаев до 138), по разделу путешествий – рост в 13,8 раза (с 6 до 83), по разделу других санкций рост составил 16,8 раза (с 10 до 168). И в целом, за указанный период количественный рост составил 12,6 раза.

Первоначальная цель, стоящая перед творческим коллективом, заключалась в исследовании возможных потерь и нанесенном ущербе, последовавших после ввода политических и экономических санкций по отношению к СССР и РФ в области информационных технологий (ИТ). Планировались исследования по определению недопоставок или отказов в поставках вычислительной техники и программного обеспечения в адрес СССР и братских социалистических государств, и их влияния на валовый продукт.

Длительная подготовительная работа по поиску статистических данных, фактов о нереализованных проектах, сведений о контрактах не увенчались

успехом. Статистические сборники Центрального статистического управления СССР (ЦСУ СССР) не содержали подобную информацию. Подобную информацию не удалось найти и в статистических и справочных материалах Государственного планового комитета СССР (Госплан СССР). Просмотр статистических сборников «СССР в цифрах», «Народное хозяйство СССР (статистический ежегодник)» и др., не дало результатов. Изучение мемуаров советских руководителей партии и правительства, известных экономистов, архивных материалов не продвинуло нас ни на йоту к намеченной цели. В конце концов, многие аналитические обзоры, докладные записки и частные обращения в высшие партийные и государственные органы были закрытыми и имели гриф секретности.

После продолжительного анализа была выдвинута гипотеза о невозможности проведения оценки потерь по следующим причинам:

- существующая в то время методология статистического учета не предполагала расчет и фиксацию потерь или упущенной выгоды в случае срыва поставок;

- отыскать следы несостоявшихся сделок по покупке вычислительной техники практически невозможно. Предполагаем, что подобная информация могла фигурировать в закрытых документах, которая использовалась в процессе проведения дипломатических переговоров на уровне послов и делегаций высокого ранга, формирования планов работ Госкомитета по науке и технике СССР (ГКНТ СССР), фигурировать в качестве заданий для технических служб органов разведки и т.д.;

- существование списка товаров, запрещенных к экспорту в СССР и социалистические страны, однозначно исключало обсуждение их содержания во время ведения переговоров по линии Торгово-промышленной палаты (ТПП СССР) и торговых представительств за рубежом;

- министерство радиопромышленности СССР, в чьем ведении находились научные разработки по проектированию и выпуску широкого спектра вычислительной техники, в силу своей закрытости не оставило соответствующих доступных архивных данных.

Вышеприведенные аргументы заставили нас пересмотреть структуру и содержание настоящей книги и сосредоточить основное внимание на рассмотрении и анализе оценок американских и европейских ученых-аналитиков и специалистов эффективности своих санкционных мероприятий. Несомненно, представляет интерес анализ моделей, подходов и инструментария, которые использовались для оценки достижения основных целей санкций. Авторы преднамеренно оставили за рамками исследования работы политической и политологической направленности, а также государственную пропаганду, уделив основное внимание работам, имеющим отношение к фундаментальным основам экономической теории. Доступные литературные источники описывают и обобщают несколько десятков геополитических, экономических, экологических, географических, военных, правовых и информационных тенденций, которые будут определять будущее

развитие. Нас больше всего интересовали теоретическое обоснование, практические оценки и выводы американских специалистов по широкому спектру введенных санкций. Отправной точкой можно считать книгу известного экономиста Ричарда Конолли (Richard Connolly), директора Центра русского, европейского и евразийского исследований (CREES - Centre for Russian, European and Eurasian Studies) в Бирмингемском университете. Его исследования направлены главным образом на изучение изменений теоретических основ экономики России. Первая глава его книги «Ответ России на санкции. Как западное экономическое государственное управление меняет форму политической экономики в России (Russia's Response to Sanctions. How Western Economic Statecraft is Reshaping Political Economy in Russia)» носит название «Санкции и политическая экономика (Sanctions and Political Economy)» [ 18].

Некоторые случаи противостояния санкциям советского периода были описаны в СМИ [19- 24]. Но, в основном, информация относится к санкционным действиям по договору о поставках стальных труб для строящихся газопроводов. Например, в начале 1960-х годов СССР стал вторым в мире производителем энергоносителей, для добычи и последующей транспортировки газа в Европу. Для этого требовались мощные газопроводы, а значит, и стальные трубы большого диаметра. Координационный комитет, контролирующий экспорт, запретил продавать Советскому Союзу технологии, способствующие добыче, переработке или поставке нефти. Осенью 1962 года страны в составе НАТО одобрили запрет на дальнейшую поставку труб большого диаметра, которые используются при строительстве трубопроводов. Вашингтон убеждал европейцев в том, что, помогая Союзу, они способствуют созданию военной инфраструктуры Варшавского блока. В результате Западная Германия начала аннуляцию уже заключенных контрактов с компаниями, которые составили с СССР соглашение о ввозе около 135 тыс. тонн стальных труб.

Одна из ведущих английских фирм по производству газовых турбин – John Brown Engineering – оказалась в патовом положении: ей грозили штрафные санкции за невыполнение обязательств по контракту, которые могли достигнуть 400 млн фунтов, что повлекло бы в дальнейшем массовые увольнения сотрудников. В случае если корпорация выполнила свои обязательства перед Советским Союзом, она бы потеряла свой рынок в Америке, возможность использовать технологии компании General Electric, потерпев многочисленные убытки. Маргарет Тэтчер, в то время являясь премьер-министром, не осталась в стороне от решения конфликтной ситуации, успешно вмешавшись в переговоры с США относительно интересов британских компаний. В результате John Brown Engineering, а впоследствии и несколько других компаний, были выведены из-под действия наложенных санкций. Это подтверждение русской пословицы – «Своя рубашка ближе к телу».

Британская корпорация ICL достаточно охотно сотрудничала с Советским Союзом и другими странами социалистического лагеря, пользуясь поддержкой собственного правительства [25]. ICL — единственный крупный производитель компьютерной техники в Великобритании того времени — не выдерживал конкуренции американцев и находился в постоянном поиске новых рынков сбыта, власти же были заинтересованы в сохранении перспективной отрасли национальной промышленности. В 1970 году ICL выручила от продажи компьютеров в Восточную Европу \$ 10 млн: сумма была относительно небольшой, но британцы верили в перспективы дальнейшего сотрудничества.

В августе 2023 года отмечали 100-летие известного советского ученого Виктора Михайловича Глушкова (24.08.1923- 30.01.1982). Благодаря его исследованиям, получила развитие кибернетика, как наука, и вычислительная техника в СССР. Именно он стоял у начала работ по разработке первой в СССР персональной ЭВМ «Мир-1» (машина для инженерных расчетов). Следует отметить существенный вклад академика В.М.Глушкова в развитие следующих направлений:

- теория топологических групп и топологическая алгебра в целом;
- теория цифровых автоматов;
- теория программирования и системы алгоритмических алгебр;
- теория проектирования электронных вычислительных машин;
- создание средств вычислительной техники: новые архитектуры вычислительных машин и систем, управляющие вычислительные машины широкого назначения;
- кибернетика как наука об общих закономерностях, принципах и методах обработки информации и управления в сложных системах;
- создание автоматизированных систем управления технологическими процессами и промышленными предприятиями;
- разработка основ построения общегосударственной автоматизированной системы управления народным хозяйством;
- основы безбумажной информатики.

В 1962 году академик В.М. Глушков предложил концепцию Общегосударственной автоматизированной системы учета и обработки информации (ОГАС), которая предполагала использование сети с компьютерным центром в Москве, 200 центров среднего уровня — в других крупных городах и до 20 000 локальных терминалов в экономически значимых местах. Для связи должна была использоваться существующая телефонная сеть. Каждый терминал мог взаимодействовать с любым другим [26-29]. На создание сети отводилось 10 лет (1965-1975 г.г.), а капитальные затраты оценивались в 4,7 млрд. руб. Из них – 4 млрд. руб. на ЭВМ, 0,3 млрд. руб. на средства связи и 0,4 млрд. руб. на строительство зданий для вычислительных центров.

Важнейшим элементом этих процессов являлась программа «информатизации страны», руководителем и идеологом которой был академик, директор института кибернетики (г. Киев) Виктор Михайлович Глушков. Очевидно, что без полной информации на предприятиях и в министерствах, нельзя было и думать не только о совершенствовании экономических механизмов, но и об извлечении выгоды из централизованных плановых механизмов. Программа информатизации предполагала создание на предприятиях, в первую очередь крупных, автоматизированных систем управления (АСУ) на базе вычислительной техники. Данные системы включали в себя накопление и обработку информации по сырью, материалам, готовой продукции, заработной плате. Во многих системах были элементы компьютерного проектирования новых образцов продукции. Для реализации программы были расширены институты по проектированию компьютеров и создана сеть заводов по производству отечественных компьютеров. Для проектирования АСУ предприятиями в рамках Министерства приборостроения были созданы порядка 35 проектных организаций.

Нельзя не упомянуть еще одного известного советского ученого в области вычислительной техники и информационных систем. Речь идет о инженере-полковнике, докторе технических наук, профессоре Анатолии Ивановиче Китове (09.08.1920 – 14.10.2005) [30-31]. Осенью 1959 года представил разработанный им проект создания общегосударственной автоматизированной системы управления для вооруженных сил и для народного хозяйства страны на базе Единой государственной сети вычислительных центров (ЕГСВЦ) – так называемый проект «Красная книга». Данный проект имел гриф «СС» («Совершенно секретно»). Это первый в СССР проект, предлагавший объединить в одну национальную сеть вычислительных центров все имеющиеся в стране ЭВМ для решения народнохозяйственных задач (в мирное время) и оборонных задач (при возникновении военных действий). Предлагалось вместо распыления по десяткам тысяч предприятий, учреждений и организаций Советского Союза средств вычислительной техники сосредоточить их в единой общегосударственной сети мощных вычислительных центров военного подчинения. Мощности этих центров должны были быть рассчитаны с большими запасами и резервами на пиковые нагрузки решения военных задач (ПВО, ГРУ ГЩ, РВ, управления войсками и др.). В мирное время эти центры должны были решать народно-хозяйственные и научно-технические задачи как для центральных органов, так и для региональных предприятий и учреждений. В соответствии с проектом А.И. Китова обслуживаться эти мощные вычислительные центры должны были военным персоналом, что обеспечивало бы повышенную чёткость и надёжность их работы. Эти центры должны были располагаться в надёжных укрытиях; доступ к ним должен был быть только дистанционный (телеобработка). Как формулировалось в письме А.И. Китова «Реализация данного проекта позволит обогнать США в области разработки и использования ЭВМ, не догоняя их». Идея А.И. Китова была

совершенно блестящая и своевременная. Тем более, что отставание от США в области разработки и использования ЭВМ ещё не обрело фатальной необратимости. Поэтому А.И. Китов буквально «бил в набат», пытаясь «достучаться» до самого высшего руководства страны. Он осознавал, что положение ещё может быть исправлено, если будут предприняты руководителями СССР кардинальные меры по перестройке управления национальной экономики, базирующиеся на повсеместном использовании объединённых в общенациональную компьютерную сеть вычислительных машин и экономико-математических методов. А.И. Китов подчёркивал, что в этом случае будут использованы в полной мере присущие социалистической системе Советского Союза централизованное планирование и управление производством [32].

Для организации внедрения типового программного обеспечения и был создан в 1974 году НПО «Центрпрограммсистем»(ЦПС). В Твери постепенно стал формироваться центр управления разработками более 30 министерств и ведомств [33]. На этом этапе численность сотрудников ЦПС достигла двух тысяч человек, функционировали филиалы в Красноярске, Киеве, Таллинне.

Для выработки совместной научно-технической политики в Болгарии был создан Советско-болгарский институт «Интерпрограмма». Основной целью института являлось обобщение мирового опыта в области программного обеспечения. Специалисты из Твери, вместе с сотрудниками других институтов получили доступ к новейшим разработкам практически всех крупных фирм. Это позволило в НПО «Центрпрограммсистем» накопить к концу 80-х годов уникальный потенциал, который распространялся по всей стране. Этому помогала и реализация программы научно-технического сотрудничества социалистических стран, в которой одна из важнейших подпрограмм - «Базы данных и системы знаний» - возглавлялась НПО «Центрпрограммсистем».

Совместный проект с ГДР привёл к созданию в Твери совместного предприятия «ЦЕНТРОН», учреждённого правительствами двух стран.

5 января 1949 года был создан Совет экономической взаимопомощи (СЭВ). Участники содружества — страны социалистической Европы: Советский Союз, Румыния, Болгария, Польша, Чехословакия и Венгрия, чуть позже к ним присоединилась Албания, Германская Демократическая Республика. В функции СЭВ входило содействовать объединению и координации сотрудничества в планомерном развитии хозяйства, экономического и научно-технического прогресса, выравниванию уровней экономического развития стран-членов организации.

Главная причина создания СЭВ была та разруха, которая возникла вследствие Второй Мировой Войны. Были понесены огромнейшие потери не только человеческие, но и экономические, промышленность, жилой спектр, инфраструктура требовали немедленного восстановления.

Яркое пропагандирование науки, нацеленность на получение образования и участие в научной работе приветствовалось обществом и

воспринималось как «творческая самореализация личности и форма социального вклада». Экономическое и научное взаимодействие стран дало свои плоды, хотя это был и уникальный проект, который строился на отношениях народов разных стран. Практиковался обмен студентами между всеми социалистическими странами, благодаря «железному занавесу» понятия «конкуренция» между восточным и западным рынком не существовало.

Страны-участники могли быть объединены на три группы по их отношению к развитию вычислительной техники в начале 60 годов: с весомым научным опытом и развитым производством (СССР), с развитым научным базисом, но без собственного производства (ГДР, Чехословакия, Венгрия, Польша), и те страны, которые не имели ни развитого научного базиса, ни электронной промышленности (Болгария, Вьетнам, Куба, Монголия, Румыния).

Правительство СССР предполагало, что в девятой пятилетке (1971-1975 годы) будет заложена материальная основа для создания ОГАС с запуском 1600 вычислительных центров в регионах и увеличение выпуска вычислительной техники в 2,6 раза. Но международный обмен научно-технической информацией и покупка вычислительной техники со стороны США были ограничены запретом специальной экспортной комиссии CoCom.

В 1969 г. было подписано Межправительственное соглашение о сотрудничестве социалистических стран в области вычислительной техники (ВТ) [34]. Этим актом было положено начало реализации проекта разработки и внедрения современных средств ВТ в народное хозяйство. Сотрудничество охватило процессы создания вычислительных машин (ЕС ЭВМ и СМ ЭВМ), прикладное программное обеспечение и типовые системы автоматизированного управления для разных областей промышленной и непромышленной сфер народного хозяйства, комплексное обслуживание средств вычислительной техники, системы автоматизированного проектирования, т.е. практически все вопросы разработки и внедрения ЭВМ.

Каждая страна СЭВ имела специализацию в области производства ВТ, например, ГДР разрабатывала и поставляла в другие страны широкий спектр бухгалтерских машин Аскота класса 170 с перфорационной приставкой, настольных клавишных машин типа Зоемтрон, вычислительные комплексы «Роботрон», М-5000 и др.

В феврале 1969 г. в соответствии с условиями межправительственного Соглашения был создан Международный центр научной и технической информации (МЦНТИ) – специализированная международная организация, объединяющая специалистов в области НИИ и информационных технологий [35]. За годы существования МЦНТИ в интересах ее государств - членов были реализованы крупномасштабные многосторонние программы и проекты по координации международного сотрудничества в области НИИ, организации и проведения научно-исследовательских работ и информационного обслуживания пользователей.



За годы существования МЦНТИ реализованы крупномасштабные многосторонние программы и проекты по координации международного сотрудничества в области НТИ, организации и проведения научно-исследовательских работ и информационного обслуживания пользователей. В рамках первого этапа развития (1969-1989 г.г.) были разработаны организационные основы создания Международной системы научно-технической информации (МСНТИ); создана информационная база МЦНТИ и система телеобработки баз данных; разработаны оригинальные программные продукты и современные технологии издательского дела, электронной почты, информационного поиска; реализованы крупномасштабные проекты технического содействия в развитии национальных систем НТИ и подготовке национальных кадров, в том числе в сотрудничестве с организациями системы ООН. Второй этап (1989-1999), характеризовался ориентацией на кооперацию в использовании национальных информационных ресурсов и коллективных действий по интеграции в мировое информационное пространство.

## Литература

1. Golnoosh Hakimdavar (2014). A Strategic Understanding of UN Economic Sanctions. International Relations, Law, and Development. Taylor & Francis. ISBN: 978-0-203-10946-5
2. Jeremy Matam Farrall (2007). United Nations Sanctions and the Rule of Law. Cambridge University Press. ISBN-13 978-0-511-37729-7
3. Lee Jones (2015). Societies Under Siege. Exploring How International Economic Sanctions (Do Not) Work. Oxford University Press. ISBN 978-0-19-874932-5
4. David Cortright, George A. Lopez (2018). Economic Sanctions. Panacea or Peacebuilding in a Post-Cold War World?, Taylor & Francis Group. ISBN 13: 978-0-8133-8909-7
5. Начало блокады Мегар Афинским морским союзом в 432 году - первые в мировой политике экономические санкции. [https://dzen.ru/a/Y3pFBY\\_WPFAOuccE](https://dzen.ru/a/Y3pFBY_WPFAOuccE) (дата обращения 04.05.2024)
6. Golnoosh Hakimdavar (2014). A Strategic Understanding of UN Economic Sanctions International Relations, Law, and Development. Taylor & Francis. ISBN: 978-0-203-10946-5
7. Jeremy Matam Farrall (2007). United Nations Sanctions and the Rule of Law. CAMBRIDGE UNIVERSITY PRESS. ISBN-13 978-0-511-37729-7
8. NIKOLAY ANGUELOV (2015). Economic Sanctions Vs. Soft Power: Lessons from North Korea, Myanmar, and the Middle East. Palgrave Macmillan. ISBN 978-1-137-52376-1 DOI 10.1057/9781137523761
9. MIKAEL ERIKSSON (2016). Targeting Peace Understanding UN and EU Targeted Sanctions. Taylor & Francis Group. ISBN 9781409419327
10. Andrea Charron (2011). UN Sanctions and Conflict: Responding to peace and security threats. ISBN: 978-0-203-80756-9

11. Sachiko Yoshimura (2021). *United Nations Financial Sanctions*. Routledge. ISBN: 978-0-429-26031-5
12. Thomas Dörfler (2019). *Security Council Sanctions Governance: The Power and Limits of Rules*. ISBN: 978-0-429-44232-2
13. Andrea Charron, Clara Portela (2022). *Multilateral Sanctions Revisited: Lessons Learned from Margaret Doxey*. *Multilateral Sanctions Revisited: Lessons Learned from Margaret Doxey*. McGill-Queen's University Press. ISBN 9780228012610
14. Iryna Bogdanova (2022). *Unilateral Sanctions in International Law and the Enforcement of Human Rights. The Impact of the Principle of Common Concern of Humankind*. World Trade Institute Advanced Studies ISBN: 978-90-04-50789-0
15. Hossein Askari, John Forrer, Hildy Teegen, Jiawen Yang (2003). *Economic Sanctions: Examining Their Philosophy and Efficacy*. Praeger Publishers.p. 6. ISBN 1-56720-542-9
16. *Economic sanctions reconsidered / Gary Clyde Hufbauer . . . [et al.]*.—3rd ed 2007. P.17 ISBN 978-0-88132-407-5
17. Peter A. G. van Bergeijk (Editor). (2021). *Research Handbook on Economic Sanctions*. Edward Elgar Publishing Limited. ISBN 978 1 83910 272 1 <http://dx.doi.org/10.4337/9781839102721>
18. Richard Connolly (2018). *Russia's Response to Sanctions. How Western Economic Statecraft is Reshaping Political Economy in Russia*. Cambridge University Press. ISBN 978-1-108-41502-6
19. Стальные трубы. Из истории санкций Запада против СССР. Дата создания: 09.09.2019. <https://oosgr.ru/articles/articles/stalnye-truby-iz-istorii-sankcij-zapada-protiv-sssr> (дата обращения: 04.05.2024).
20. Сделка века «газ — трубы». [https://ru.wikipedia.org/wiki/Сделка\\_века\\_«газ\\_—\\_трубы»](https://ru.wikipedia.org/wiki/Сделка_века_«газ_—_трубы»). (дата обращения: 04.05.2024).
21. Виктор Степанов. Страна семибитного байта. <https://tjournal.ru/news/55415-ussr-usa-tech-sanctions>. (дата обращения: 04.05.2024)
22. Кибернетика в СССР: от лженауки до панацеи. [https://habr.com/ru/company/cloud\\_mts/blog/486932/](https://habr.com/ru/company/cloud_mts/blog/486932/). (дата обращения: 04.05.2024)
23. Санкции и ограничения в области высоких технологий против России. [https://www.tadviser.ru/index.php/Статья:Санкции\\_и\\_ограничения\\_в\\_области\\_высоких\\_технологий\\_против\\_России](https://www.tadviser.ru/index.php/Статья:Санкции_и_ограничения_в_области_высоких_технологий_против_России). (дата обращения: 04.05.2024)
24. История информационных технологий в СССР. Знаменитые проекты: компьютеры, связь, микроэлектроника / Под общ. ред. Ю.В. Ревича. - М.: Книма (ИП Бреге Е.В.), 2016. — 416 с. — ил. ISBN 978-5-9905887-8-3 <https://publications.hse.ru/pubs/share/folder/eg8rzpp6ig/202696142.pdf>
25. 5 историй о ловком обходе санкций: как в СССР появились западные компьютеры. <https://www.techinsider.ru/gadgets/721323-5-istoriy-ob-obhode-sankcij-zapadnye-kompyutery-v-sssr/> (дата обращения: 04.05.2024)

26. Глушков В.М. Введение в АСУ. – Изд. 2-е, испр. и доп. «Техніка», 1974, 320 с.
27. ОГАС В.М. Глушкова: история проекта построения информационного общества. <https://vk.com/@vekrako-ogas-v-m-glushkova-istoriya-proekta-postroeniya-informacionn> (дата обращения: 04.05.2024)
28. Развитие вычислительной техники в России, странах бывшего СССР и СЭВ: история и перспективы: Труды Пятой международной конференции SoRuCom-20 (6–7 октября 2020 г., Москва) / Ред. А.Н. Томилин. М.: МИЭТ НИУ «ВШЭ», 2020. – 368 с. ISBN 978-5-6044274-3-9
29. Глушков В.М. Основы безбумажной информатики. Изд. 2-еб испр. –М.: Наука. Гл. ред. Физ.-мат.лит. 1987.-552 с.
30. Китов В.А., Приходько А.Я., Ревич Ю.В. К истории первого отечественного ВЦ. [http://it-history.ru/images/2/2c/05\\_Вц-1.pdf](http://it-history.ru/images/2/2c/05_Вц-1.pdf) (дата обращения: 26.11.2022)
31. Китов В.А., Сафронов А.В. Страницы истории главного вычислительного центра Госплана СССР. <https://www.computer-museum.ru/books/gosplanccsr.pdf> (дата обращения: 04.05.2024)
32. Проект "Красная книга". <http://www.kitov-anatoly.ru/naucnye-trudy/proekt-krasnaa-kniga> (дата обращения: 04.05.2024)
33. Валерий Куприянов, Лариса Полонникова (2004). "Центрпрограммсистем": 30 лет на рынке программного обеспечения. <https://cps.tver.ru/kompaniya/publikatsii/?id=3> (дата обращения 04.05.2024)
34. Вычислительная техника социалистических стран: Сб. статей/Под общ. Ред. М.Е.Раковского. – Вып. 6. – М., 1978. – 149 с.
35. 1969 – 2009. 40 ЛЕТ МЦНТИ. Основные направления и результаты работ. Международный центр научной и технической информации. –М.: МЦНТИ. <http://www.icsti.su/portal/news/icsti40/rus/text.pdf> (дата обращения: 04.05.2022)

### ГЛАВА 3. МЕЖДУНАРОДНЫЕ САНКЦИИ КАК ОБЪЕКТ ИССЛЕДОВАНИЙ

Санкции не так давно стали объектом комплексных исследований. Как указывается в [1, с.30-35], отправной точкой была научная дискуссия о санкциях, состоявшаяся в конце 90-х годов между коллективом во главе с Хафбауэром Г.Л. [2] и учеными Болдуин, Д.А. и Папе, Р.А. [3]. Обсуждалось определение объекта исследования. Дискуссия ограничивалась категорией «экономические санкции» и представления их в качестве инструмента влияния. Классическое определение санкций включает «преднамеренно спровоцированный правительством разрыв...торговых или финансовых отношений (для получения) внешнеполитических целей». В этом определении, сформулированном Хафбауэром Г.Л., можно выделить два центральных элемента. Первое, в концепции экономических санкций предусматривается, что мера принуждения должна быть по своей природе экономической, во-вторых, цель санкций должна быть политической. Паппе Р.А. уточняет данное определение для характеристики отличий между экономическими санкциями и торговыми войнами. В его редакции экономические санкции «стремятся снизить экономическое благосостояние государства-мишени за счет сокращения международной торговли с целью заставить правительство изменить свое политическое поведение». Страны, вовлеченные в торговые споры, находятся перед дилеммой – идти на уступки или нет в зависимости от того какой выбор максимизирует их благосостояние. Объекты экономических санкций, с другой стороны, понимают, что они имели бы лучшее экономическое положение в случае принятия требований и принимают решение на основе сравнения (эффективности) политических целей и экономических издержек – выбор следования экономическим, а не чисто политическим расчетам.

Из этого следует, что переменные, которые доминируют в процессе принятия решений государствами-мишенями, разные и отвечают на различные запросы. Среди исследователей сложился консенсус в отношении того, что экономические санкции и торговые войны аналитически различны и их не следует смешивать.

Основоположником общей теории санкций является Йохан Галтунг (Johan Galtung) [4]. Он назвал ее «наивной» теорией санкций. В ней постулируется – экономический спад, вызванный санкциями, приведет к политическому давлению и это, в конечном итоге, заставит руководство страны-мишени изменить свою политику, либо приведет к его свержению. Согласно классической формулировке санкции являются инструментом, который действует аналогично военным действиям. И санкции, и военные действия преследуют одну и ту же цель – политическое разложение противника для отказа от достижения своих целей (метод лишения ценностей). Теория предполагает примерно пропорциональное соотношение между этими

явлениями, но чем интенсивнее уменьшение ценности, тем больше политический распад.

Как можно объяснить неэффективность санкций? Существует несколько точек зрения. На практике проходит пересмотр отношения к санкциям, в том числе санкциям США и ЕС. Как отмечают некоторые эксперты наблюдается переход от «экономических потрясений» к «экономической» и «неэкономической бесполезности». Первоначальный посыл санкций заключался в следующем: чем больше ущерб экономике страны-мишени, тем выше шансы на успех санкций. Следуя этой логике несколько экспертов предложили несколько индикаторов для определения вреда, который наносится стране-мишени [ 2 ]:

- стоимость санкций, налагаемых на страну-мишень в процентах от ее валового национального продукта (ВВП) и стоимость для страны-отправителя;

- уровень торговли между отправителем и страной-мишенью в процентах от общего объема торговли;

- экономическая мощь стран, измеряемая соотношением их ВВП;

- тип санкций, а именно запрет на экспорт, запрет на импорт или отказ в финансировании.

Следует обратить внимание на важный факт – приведенные показатели относятся к экономическим. В частности, экономические потери, понесенные страной-мишенью, выражаются количественно в долях ВВП и являются показателями, характеризующими ущерб. Показателем также объем торговли до и после введения санкций, так как он указывает на важность прерывания коммерческих отношений. Соответственно, сравнение экономической мощи стран, измеряемые отношениями их ВВП, четко выражает дисбаланс экономического потенциала.

Получила отражение оценка, в соответствии с которой, вред, причиняемый санкциями, традиционно связан с двумя факторами:

- уязвимость страны-мишени к той или иной мере санкций;

- степень эффективности реализации.

### **Модели оценки эффективности санкций**

Несмотря на длительный период споров относительно эффективности, универсальный аппарат оценки санкций, либо модель определения их результативности так и не были разработаны. Несмотря на отсутствие общепринятой адекватной модели успешной реализации санкций, рядом исследователей используются свои модели оценки эффективности санкций. В частности, это графовая модель разрешения конфликтов (Graph Model for Conflict Resolution - GMCR), представленную в [5, с. 309-328]. Стратегические конфликты обычно включают двух и более лиц, принимающих решение, и множество возможных действий. Допущенные ошибки обычно обходятся дорого и зачастую необратимы. Данная модель представляет собой систему моделирования и анализа стратегических конфликтов. Она позволяет понять,

чего можно достичь, учитывая набор ограничений, с которыми сталкиваются лица принимающие решения (ЛПР) используя ходы и контрходы для достижения цели или максимизации выгоды. Данная модель была применена ко многим стратегическим конфликтам для определения характера и эффективности экономических санкций. Одновременно с достигнутыми успехами, авторы выделяют сложность предсказания желаемого воздействия на объект и результатов влияния экономических санкций в силу неизвестности возможных исходов. Приводится следующий пример – если США введут экономические санкции против Китая, стремясь достичь определенного результата, Китай может подчиниться, а может и нет. Решение Китая приведет к двум или более различным сценариям, соответственно реакция США может быть разной для каждого сценария. В большинстве современных конфликтов неопределенность в действиях игроков делает ход конфликта трудно отслеживаемым, а количество возможных исходов может кардинально увеличиваться. Использование данной модели включает два этапа – собственно моделирование и анализ результатов.

Этап моделирования включает шесть шагов:

- собственно выбор конфликта и временного интервала. В некоторых случаях рекомендуется отдельный анализ для разных фаз конфликта, понимая динамику процесса;
- определение круга лиц, принимающих решение и оказывающих влияние на исход конфликта;
- определение вариантов действий ЛПР, включая санкции, интервенции и военные действия. Каждая возможная комбинация опций представляет собой состояние графовой модели;
- удаление невыполнимых состояний и комбинаций вариантов;
- определение допустимых переходов между состояниями;
- ранжирование состояний для каждого ЛПР в порядке предпочтений, которые регулируют их поведение.

На этапе анализа реализуются 4 действия:

- оценка индивидуальной стабильности. Состояние считается стабильным, если ЛПР не желает от него отходить из-за собственных предпочтений и ожиданий относительно того, как другие ЛПР отреагируют на этот переход;
- оценка равновесия. Состояние, которое является стабильным для всех ЛПР, является равновесием (возможным решением);
- анализ чувствительности;
- анализ информации для пользователей.

Рассматриваемая модель была проиллюстрирована на материалах противостояния США и Ирана. В указанной книге приведены также результаты построения моделей и исследования влияния экономических санкций на следующие сектора экономики: банковская система, туризм, прямые иностранные инвестиции, международная торговля, продовольственная безопасность.

Еще одной важной для нашего исследования является модель санкций NOEM (New Open Economy Macro), которая представляет макромоделю новой открытой экономики и дает представление о том, как макроэкономисты могут информировать политиков об эффективности государственного управления [6, с.105-123]. Суть данной модели заключается в том, что макроэкономическая политика зарождается в экономике отправителя и передается через ее международные связи в другие экономики. В каждой стране производится и потребляется уникальная корзина товаров и целевой рынок и рынок «остального мира» образуют совокупность, но с разными политическими результатами. Именно на товарных рынках появляются торговые санкции.

Базовая схема модели санкций NOEM описывается следующим образом – участвуют три страны, два товара и один финансовый актив для равновесия платежного баланса. Третья страна выступает либо в качестве члена коалиции с отправителем санкций, либо придерживается условий страны-мишени. Третья сторона относится к ROW, что означает «Остальной мир». Если санкций нет, то эта модель распадается до базовой модели двух стран, т.е. страны-отправителя и всех других иностранных объединенных экономик. Данная модель обеспечивает возможность отслеживать влияние экономического принуждения на благосостояние как на целевую экономику, так и на экономику-отправителя. Опишем суть данной модели вкратце.

В мировой экономике производится товара: отечественный и иностранный с точки зрения отправителя, обозначенного буквами  $z$  и  $z^*$ . Мы можем думать о  $z$  и  $z^*$  как о корзинах товаров, потребляемых в странах-отправителях и странах-мишенях; таким образом, каждая страна производит уникальную корзину товаров. Эта дихотомия позволяет экспортировать и импортировать разные товары в каждой стране. В соответствии с рыночным ценообразованием (pricing-to-market - PTM) каждая страна устанавливает свою собственную цену, поскольку для каждой страны существует монополистическая конкуренция за соответствующий товар. Остальные страны мира (Rest of World –ROW) принимают цены, заданные отправителем и мишенью.

Введенные санкции перераспределяют доходы в виде «платы за политику». Отправитель санкций может либо потерять доход, либо заставить это объект санкций, с помощью экспортных и импортных санкций. Экспортные санкции снижают доходы, характерные для внутреннего товара отправителя ( $z$ ), в свою очередь, импортные санкции сокращают предложение иностранного товара ( $z^*$ ), происходящего только из страны-цели, в зависимости от доли импорта из целевой страны. Следует отметить, что импортные санкции сокращают целевые доходы страны-мишени и выступают в качестве зеркала экспортных операций. В модели для каждого товара существует три цены – внутренняя цена товара, производимого отправителем, внутренняя цена целевого товара, внешняя цена, устанавливаемая отправителем.

При реализации данной модели широко используется информация, характеризующая товарные рынки, рынки активов, бюджеты фирм и домохозяйств, экономическое государственное управление и перераспределение благосостояния, оптимизацию домашних хозяйств, деятельность государства под санкциями. В конце концов, реализация данной модели позволяет определить влияние экономических санкций на благосостояние страны-мишени. Наведение моста между экономическими эффектами и политическими целями санкций является основной конечной целью. Основной задачей исследований заключается в том, чтобы описать уровень достаточного шока в целях обратить вспять действия страны-мишени.

Использование санкций в международной политической жизни резко возросло. Санкции признаны наиболее важными инструментами внешней политики США в отношении таких государств, как Российская Федерация, Иран, Китай, Венесуэла и Куба. Данный перечень не является полным. Достигли цели введенные санкции против России или нет? Предпримем попытку найти ответ на поставленный вопрос в экономической литературе аналитиков из США, в том числе [7-12].

Экономические санкции могут иметь любое сочетание следующих целей [11, с. 10-11]:

- модификация поведения цели,
- возмездие или
- наказание, или как сигнал цели или другим государствам третьих стран.

Более того, обоснование экономических санкций может включать продвижение военных целей с одной стороны, и сохранение мира с другой. Или это может быть связано с использованием санкции как средство сдерживания и/или диалога. Некоторыми политическими целями санкций могут быть сдерживание или принуждение цели, или сдерживание или принуждать другие государства или лица, которые непосредственно не являются объектом санкций, но кто торгует или ведет торговые дела.

Приведем 7 ключевых параметров для классификации эффективности санкций, предложенных Йоханом Галтунгом [4]:

1. Санкции либо вознаграждают (положительны), либо наказывают (отрицательны);
2. Санкции направлены на отдельных лиц или коллектив;
3. Санкции налагаются в связи с внутренними или внешними действиями со стороны цели;
4. Санкции бывают односторонними, многосторонними или универсальными;
5. Санкции общие или выборочные;
6. Санкции бывают полными или частичными; а также
7. Санкции ограничивают сочетание торговли, финансирования, коммуникаций, и дипломатические отношения.



В частности, Ксения Киркхэм [3], предложила проанализировать результаты влияния санкций на Россию и Иран на основе нового подхода к оценке режима государства всеобщего благосостояния (WSR - Welfare State Regime). Данный подход сочетает в себе институциональные, экономические и культурные структурные измерения процессов, которые развиваются в России и Иране в условиях санкций. Автор отмечает, что не смотря на существенные культурные различия, Россия и Иран обнаруживают важные структурные, политические и экономические общие черты [3, с.3].

В книге выполнен анализ санкций как инструмента соперничества, поскольку они превратились из их первоначальной цели – инструментов предотвращения войны – в оружие геэкономической войны. За последние 50 лет санкции стали доминирующими и все более мощным невоенным инструментом в неоимперской борьбе. Например, количество санкций достигло более 160, из них более 70 % были введены США в одностороннем порядке. Экстерриториальность санкций поддерживается подчинением мира американской политике финансовой либерализации и американским режимам накопления, составляющим цель гегемонистского проекта США.

Социально-экономические и политические несчастья, проистекающие из несвоевременной и недостаточной защиты общества от воздействий противоречий капитала на общественное самочувствие, - это механизмы, с помощью которых действуют санкции: обостряя данные противоречия, санкции нацелены на и без того неустойчивый режим государства всеобщего благосостояния и требуют разработки и реализации защитных мероприятий.

Другими словами, механизмы санкций можно проследить через оценку следующих противоречий капитала, обострившихся внутри государства [3, с.61-62]

Во-первых, санкции закрепляют и увеличивают противоречие между транснациональным капиталом и национальным трудом: снижение реальных доходов наиболее уязвимых социальных групп ставит под угрозу стабильное потребление и увеличивает спрос на государственные расходы, а каналы финансирования воспроизводства труда за счет заимствований на мировых финансовых рынках сужаются из-за «отказа в любом кредите, кредитных гарантиях или другой финансовой помощи со стороны правительства США.

Во-вторых, экономические санкции, призванные сделать разделение капитала на национальный и международный более осуществимым, могут отключить государство-мишень от глобальных цепочек создания стоимости, подорвав экономические и фискальные возможности государства и, в конечном счете, его способность к детоваризации.

В-третьих, санкции могут усилить «противоречие между свободой и господством» и подтолкнуть широкие слои населения к оппозиции правительству подсанкционного государства, которое неизбежно принимает меры для противодействия центробежным демократическим тенденциям в обществе и ужесточает контроль над стратегическими секторами экономики.

В-четвертых, санкции могут спровоцировать воздействие противоречий, связанных с «неравенством в доходах и богатстве в глобальной экономике», на перераспределительные способности целевой экономики, что приведет к организации внутреннего производства в пользу «небольшой группы олигархов», неизбежно перенаправляя инвестиционные потоки в сторону от «целевого» государства, усугубляя его неокOLONиальный статус, нанося ущерб способности государства к первичному распределению богатства, искажая вторичные механизмы распределения богатства и разрывая внешнее и внутреннее предложение-спрос связи.

В-пятых, санкции могут еще больше усилить борьбу за распределение богатства, которая взаимосвязана с другими формами неравенства, такими как неравенство перед законом, неравенство политических представлений, неравенство возможностей получения образования и трудоустройства.

В-шестых, санкции могут спровоцировать противоречие «бунт человеческой природы: всеобщее отчуждение» (там же: 74), разрушая социальную солидарность и подрывая доверие к институтам государства-мишени во всем мире. Опасность заключается в том, что социальное «множественное отчуждение» усиливает геополитическое соперничество, порождает крайний национализм и распространяется на западные общества, трансформируя и разрушая социальную солидарность. Наконец, санкции могут нарушить связующие способности целевого государства всеобщего благосостояния посредством механизма, присущего противоречию между частной собственностью и государством, путем усиления классового и неклассового соперничества и напряженности между демократизацией и накоплением капитала.

Было предложено теоретическое развитие категории государства всеобщего благосостояния (WSR - Welfare State Regime) на базе сравнения нескольких концепций (табл. 5).

Таблица 5. Режим государства всеобщего благосостояния - теоретическое развитие

Теории/ Компоне нты	Функционали сты и энергетичес кий ресурс	«Средний путь» по Вуду и Гофу	Грамши	Государство всеобщего благосостояния
Актеры	Государство Рынок Домохозяйст во	Государство Рынок Домохозяйств о Официальное сообщество Неформальны е и нелегальные игроки	Государство Рынок Домохозяйств о Официальное сообщество Неформальны е и нелегальные игроки	Государство Рынок Домохозяйство Официальное сообщество Неформальные и нелегальные игроки Международны е эквиваленты

Теории/ Компоне нты	Функционали сты и энергетичес кий ресурс	«Средний путь» по Вуду и Гофу	Граамши	Государство всеобщего благополучия
		Международн ые эквиваленты	Международн ые эквиваленты Интеллектуал ы Исторический блок	Интеллектуалы Исторический блок 'Heartland' vs 'Contenders
Структур ы	Институцион альный Политически й Социальный	Институциона льный Политический Социальный Социально построенный «Институцион альные условия»	Институциона льный Политический Социальный Социально построенный «Институцион альные условия» Материальны й Культурный	Институционал ьный Политический Социальный Социально построенный «Институциона льные условия» Материальный Культурный
Функции благополучия	Декоммодиф икация Перераспреде ление Стратификац ия	Декоммодифи кация Перераспреде ление Стратификаци я Деклиентилиз ация Мобилизация «Репродуктив ные последствия»	Декоммодифи кация Перераспреде ление Стратификаци я Деклиентилиз ация Мобилизация «Репродуктив ные последствия» Стабилизация (Согласие против принуждения)	Декоммодифик ация Перераспредел ение Стратификация Деклиентелиза ция Мобилизация «Репродуктивн ые последствия» Стабилизация (Согласие против принуждения) Связь с социализацией
Благополучия режимов	Консервативн ый Либеральный	Консервативн ый Либеральный	Консервативн ый Либеральный	

Теории/ Компоне нты	Функционали сты и энергетичес кий ресурс	«Средний путь» по Вуду и Гофу	Грашши	Государство всеобщего благополучия
	Социал- демократичес кий	Социал- демократичес кий Неформальная безопасность  Неуверенност ь	Социал- демократичес кий Неформальная безопасность  Неуверенност ь «Претендент на режим государства всеобщего благополучия?»	

*Источник:* Ksenia Kirkham (2022). The Political Economy of Sanctions: Resilience and Transformation in Russia and Iran. Palgrave Macmillan. Pp. 44-45. ISBN 978-3-031-04055-9 doi.org/10.1007/978-3-031-04055-9

Таблица 6. Топ-100 транснациональных корпораций по странам (прибыль)

№ п/п	2020 г. В % от 1259 млрд дол	2017 г. В % от 942 млрд дол
1	США – 46%	США – 45%
2	Китай – 22%	Китай – 22%
3	Европа – 16 %	Европа – 14 %
4	Япония – 5%	Япония – 7%
5.	Саудовская Аравия – 4%	Саудовская Аравия – 4%
6	Гонконг – 2 %	Гонконг – 2 %
7	Россия – 1%	Россия – 2%
8	Другие – 4%	Другие – 8%

*Источник:* Ksenia Kirkham (2022). The Political Economy of Sanctions: Resilience and Transformation in Russia and Iran. Palgrave Macmillan. p.166

Данные таблицы свидетельствуют о том, что изменения в объеме получаемой прибыли коснулись практически всех ведущих стран: доля США возросла на 1 %, у Европы рост на 2 %. Снижение отмечается у Японии – 2 %, России – 1 % и у других стран на 4 %. Приведем несколько примеров санкций, описанных в [6, с. 170, 204-205].

В первую очередь, нас интересует перечень стран, против которых применялись санкции и время их действия. В отношении СССР фигурировала информация, представленная в таблице 7.

Таблица 7. Санкции против СССР по годам

Санкционирующая страна	Годы	Санкционные инструменты	Оценка вклада	Продолжительность (месяцев)	Лаги
СССР	1975-90	IM, FS	2	180	2
СССР	1978-80	EX	1	24	2
СССР	1980-82	EX	1	24	3
СССР	1981-81	EX	1	12	2
СССР	1983-83	IM	1	12	2

*Примечание:* IM – импортные санкции; EX – экспортные санкции; FS – финансовые санкции.

*Источник:* Robert Eyster (2007). Economic Sanctions. International Policy and Political Economy at Work. Palgrave Macmillan. P.135. ISBN 1–4039–7463–2

Приведенные в таблице данные характеризуют санкции времен холодной войны и реакцией на угрозу распространения идеологии коммунизма за счет советского финансирования и торговой поддержки новых независимых правительств. Против СССР были применены все типы экономических санкций – импортные, экспортные и финансовые. Можно назвать множество эпизодов введения санкций и наиболее важным из которых является эмбарго на зерно в 1981 году, многие из этих мер были небольшими по своим масштабам.

Наглядным примером могут служить начальные и кумулятивные эффекты санкционного шока — первый месяц (1 или 1 или 0) по сравнению с прошлым месяцем (1 или 1 или 0), приведенные в таблице 8.

Таблица 8. Начальные и кумулятивные эффекты санкционного шока — первый месяц (1 или -1 или 0) по сравнению с прошлым месяцем (1 или -1 или 0)

Цель	Дата	Экспортные санкции	Импортные санкции	Финансовые санкции	
		Первый месяц	Последний месяц	Первый месяц	Последний месяц
СССР	1975-90	0	0	1	0
СССР	1978-80	1	1	0	0
СССР	1980-82	-1	1	0	0
СССР	1981-81	1	1	0	0
СССР	1983-83	0	0	-1	0

*Источник:* Robert Eyster (2007). Economic Sanctions: International Policy and Political Economy at Work. Palgrave Macmillan. P.137. ISBN-13: 978–1–4039–7463–1

Для данного случая, независимыми переменными являются экспорт, импорт и чистые финансовые потоки между странами, вовлеченными в санкции. В каждом случае определяют какие шоки включаются в расчеты VaR. В исследовании были выдвинуты две гипотезы, которые носят глобальный характер и не зависят от коэффициентов.

Гипотеза 1: Шоковое воздействие должно иметь предсказуемые последствия на обменные курсы в течение срока действий санкций. Например, экспортные санкции должны повысить целевой обменный курс \$ США; импортные санкции должны понизить обменный курс; а финансовые санкции должны повышать обменный курс.

Гипотеза 2: В течение срока действия санкционной политики эффект от шока не должен ослабевать. Эффект обменного курса имеет большое значение для убедительности экономического принуждения. Ожидания отправителя заключается в том, что шок будет постоянным по своему воздействию.

Весьма важным условием является оценка гуманитарного эффекта вводимых санкций, т.е. мониторинг побочного ущерба, причиняемого санкциями. Эксперты инициировали разработку нового набора факторов, которые следует отслеживать и проверять эмпирически. Если считать, что санкции выступают в качестве «грубого» набора инструментов воздействия на макроэкономическую политику страны-мишени, то побочный ущерб в гуманитарной плоскости будет являться печальным последствием экономического управления. Непрерывная эффективность введенных санкций предполагает, что экономический успех санкций должен быть отделен от гуманитарного ущерба, присущего всем странам и всем санкциям.

Работа начинается с выбора зависимой переменной, которая представляет собой составной показатель, построенный на сумме субпоказателей. Основная сложность заключается в правильном выборе компонентов. Экспертами предлагается восемь категорий для измерения условий жизни людей в стране: доступ к здравоохранению, воде, образованию и продовольствию; управление и экономические условия; экологические и демографические показатели. Они включают следующее:

- доступ к здравоохранению: распространенность и смертность от малярии и туберкулеза; детская смертность в возрасте до 5 лет; показатели младенческой и материнской смертности.

- доступ к продовольствию: преобладание детей с недостаточным весом до 5 лет.

- доступ к воде: доля населения, имеющего доступ к улучшенным источникам воды и санитарии.

- окружающая среда: доля земель, покрытых лесом; выбросы углекислого газа (CO<sub>2</sub>); потребление озоноразрушающих хлорфторуглеродов (ХФУ).

- образование: доля учеников, которые поступают в первый класс и достигают пятого класса; уровень грамотности; соотношение девочек и мальчиков в среднем и высшем образовании.

- управление: доля мест, занимаемых женщинами в национальном парламенте.

Итоговые данные по оценке гуманитарной составляющей для СССР приведены в таблице 9.

Таблица 9. Оценки гуманитарных данных для санкционных случаев

## Гуманитарные индикаторы

Страна-мишень	Даты	Здоровье	Продовольствие	Вода	Окружающая среда	Образование	Управление	Всего
		1	1	0	-1	0	0	1
СССР	1975-90							
СССР	1978-80	0	1	0	-1	0	0	0
СССР	1980-82	0	1	0	1	0	0	2
СССР	1981-81	1	0	0	-1	0	0	0
СССР	1983-83	1	0	0	-1	0	0	0

*Источник:* Robert Eyler (2007). Economic Sanctions. International Policy and Political Economy at Work. Palgrave Macmillan. P. 144. ISBN 1–4039–7463–2

В 1972 году СССР ввел «налог» на эмиграцию образованных граждан в Израиль. Это послужило основанием для снятия с СССР режима наибольшего благоприятствования в торговле. Начиная с 1975 года импорт из США и финансовые потоки в СССР были ограничены из-за снятия этого режима. И данный процесс имел продолжение на протяжении нескольких лет. Следующим этапом стал 1978 год, когда была пресечена разведывательная деятельность агентов США и они предстали перед судом. И как результат – ограничения на экспорт технологий в СССР.

## Литература

1. Clara Portela (2010). European Union Sanctions and Foreign Policy. When and why do they work? Taylor & Francis Books. ISBN 978-0-203-84751-0
2. Hufbauer, G.C., Schott J.J., Elliot, K.A. and Oegg, B. (2007) (3rd edn) Economic Sanctions Reconsidered. History and Current Policy, Washington, DC: Institute for International Economics. ISBN 978-0-88132-407-5
3. Baldwin, D.A. and Pape, R.A. (1998) 'Evaluating Economic Sanctions', International Security 23(2): 189-98. <https://direct.mit.edu/isec/article-abstract/23/2/189/11606/Evaluating-Economic-Sanctions?redirectedFrom=fulltext>
4. Galtung, J. (1967) 'On the Effects of International Economic Sanctions, with Examples from the Case of Rhodesia', World Politics 19: 378-416. <https://doi.org/10.2307/2009785>; [web.stanford.edu/class/ips216/Readings/galtung\\_67.pdf](http://web.stanford.edu/class/ips216/Readings/galtung_67.pdf) (дата обращения: 04.05.24)
5. Peter A. G. van Bergeijk (Editor). (2021). Research Handbook on Economic Sanctions. Edward Elgar Publishing Limited. ISBN 978 1 83910 272 1 <http://dx.doi.org/10.4337/9781839102721>
6. Eyler Robert (2007). Economic Sanctions: International Policy and Political Economy at Work. Palgrave Macmillan. ISBN-13: 978–1–4039–7463–1

7. Ali Z. Marossi, Marisa R. Bassett (Ed.) (2015). *Economic Sanctions under International Law: Unilateralism, Multilateralism, Legitimacy, and Consequences*. T.M.C. Asser Press. ISBN 978-94-6265-051-0, DOI 10.1007/978-94-6265-051-0
8. Ksenia Kirkham (2022). *The Political Economy of Sanctions: Resilience and Transformation in Russia and Iran*. Palgrave Macmillan. ISBN 978-3-031-04055-9 doi.org/10.1007/978-3-031-04055-9
9. Nicholas Mulder (2022). *Weapon the Rise of Sanctions as a Tool of Modern War*. Yale University Press. ISBN 978-0-300-25936-0
10. Kern Alexander (2009). *Economic Sanctions: Law and Public Policy*. Palgrave Macmillan. ISBN-10: 0-230-52555-5
11. A. Cooper Drury (2005). *Economic Sanctions and Presidential Decisions. Models of Political Rationality*. Palgrave Macmillan. ISBN 978-1-4039-7695-6 DOI 10.1057/9781403976956



## ГЛАВА 4. САНКЦИИ: ПОЛИТИЧЕСКИЙ И ЭКОНОМИЧЕСКИЙ АСПЕКТЫ

За последние несколько десятилетий международные санкции (политические и экономические) превратились в основной инструмент глобального управления. С одной стороны, как правило, в санкциях участвуют государства или международные организации, которые пытаются принудить правительства страны, на которую направлены санкции, внести политические изменения посредством ограничения экономического взаимодействия с другими странами, включая торговлю, инвестиции, финансы и туризм. С другой стороны, страна, к которой международные организации предъявляют претензии относительно ее политики и поведения. Практически в большинстве случаев, проигравшей стороной является страна, к которой предъявлены претензии [1-2].

За прошедшие годы экономические санкции получили множество названий: блокада, эмбарго, бойкот или, альтернативно, карантин или экономическое принуждение. Рассмотрим эти основные категории [3-6]. Санкции часто используются отдельным государством или группой государств, сотрудничающих между собой, чтобы вызвать определенные виды давления (т. е. дипломатического, морального и военного). Существует как минимум пять определенных классов экономических санкций, которые могут быть наложены на страну-мишень, т.е. запрет на:

- экспорт оружия, боеприпасов и вооружения;
- импорт;
- поставки сырья и технологий;
- международный бойкот.

Несмотря на то, что различные термины используются в качестве синонимов экономических санкций, следует отметить их существенные различия.

Бойкот — это действие, целью которого является экономическая или социальная изоляция отдельного лица, группы или нации для выражения неодобрения, принуждения к изменениям или в качестве дополнения к военной кампании. Часто бойкоты проводятся как публичная кампания с целью выражения критики и применения принуждения к намеченной цели. Эмбарго определяется международным правом «как запрет на перемещение товаров в иностранное государство по суше, морю или воздуху». Эмбарго служит различным целям, таким как помощь в военных действиях, принуждение другого государства, и содействие коммерческому производству путем предотвращения вывода скудных ресурсов из страны. Таким образом, эмбарго обычно вводятся во время войны или военных действий и представляют собой очень строгие меры, часто имеющие силу закона. Бойкот отличается тем, что он часто не имеет силы закона и проводится на частной арене с целью направить остракизм на намеченную цель.

Санкция – это наказание, налагаемое на страну с целью заставить ее соблюдать международное право или изменить ее политику или поведение. Санкции вводят не только международные организации, такие как Организация Объединенных Наций и ее предшественница Лига Наций, но они часто используются в одностороннем порядке могущественными государствами, особенно Соединенными Штатами. Это мощный инструмент внешней политики, когда он используется против относительно слабого государства, поскольку оно не в состоянии противостоять коллективным санкциям под мандатом или даже односторонним санкциям более могущественной страны. Таким образом, санкция используется как карательная мера против государства-мишени.

Эксперты выделяют 4 отдельные категории экономических санкций по способу достижения результата. Первая категория санкций является целенаправленной, и ее можно охарактеризовать как санкции, разработанные для принуждения другой страны к принятию конкретных политических целей или курса действий. Эта категория соответствует большинству санкций, которые используются в настоящее время.

Вторая категория санкций – это так называемая «паллиативная». Данные санкции часто являются символическими санкциями, используемыми для передачи символического сообщения или в качестве сигнального сообщения. Эти санкции используются в качестве протеста против какого-либо события и не обязательно применяются для изменения поведения объекта, а скорее для выражения некоторого недовольства.

Третья категория санкций является карательной и применяется в качестве наказания страны-мишени. В данном случае инициатор санкций стремится нанести значительный экономический ущерб стране-мишени, но это косвенно может оказать влияние и на другие страны. Карательные санкции часто применяются для наказания страны за ее поведение или правонарушения, либо используются в качестве предупреждения последующих действий и решений.

Последняя категория санкций – это выборочные, которые более или менее предназначены для получения экономической выгоды или убытков для определенной группы населения в стране-отправителе. Такого рода санкции часто приносят пользу конкретному лицу, группе или сектору страны-отправителя за счет целевой страны. Например, ограничения импорта определенного товара может принести отечественным производителям несправедливое преимущество. Эксперты указывают, что эти санкции никогда не могут быть оправданы, поскольку экономические санкции все чаще становятся удобным средством для США, чтобы выразить свое недовольство поведением других стран.

Исследователями выделяются цели санкций. В частности, Маргарет П. Докси указывает восемь политических целей санкций. Они классифицируются следующим образом:

- сдерживание;

- подчинение;
- наказание;
- дестабилизация;
- ограничение конфликта;
- солидарность;
- символизм;
- сигнализация.

Первые пять связаны исключительно с политическими намерениями, «солидарность» относится к союзникам и партнерам, а «символизм» и «сигнализация» могут демонстрировать позицию страны для внутренней и внешней аудитории.

Сдерживание является основной функцией санкций. Если бы существовала устойчивая система соблюдения норм, то санкции могли бы стать мощным сдерживающим фактором. Санкции носят угрожающий и, следовательно, предупредительный характер. Существуют также дополнительные возможности сдерживания. Санкции, однажды наложенные, могут оказать сдерживающее воздействие на третьи государства, планирующие аналогичные действия. Дополнительное давление оказывается с помощью дипломатических, культурных, коммуникативных и экономических санкций, либо их комбинации, для достижения соответствия требованиям. Дестабилизация является главной целью не только односторонних санкций, но и во многих случаях групповых санкций. Устранение руководства, несомненно, являлось негласной целью санкций против Ливии и Ирака. Очевидными примерами являются также Куба и Югославия.

Ограничение конфликта должно быть указано в качестве основной цели международных санкций, независимо от того, применяются подобные меры отдельно или в сочетании с другими стратегиями.

Статистика экономических санкций свидетельствует о беспрецедентном росте их применения. Например, в середине 20 столетия только пять стран подверглись санкциям, а к 2000 году их количество увеличилось почти до 50. За это время содержание санкций значительно изменилось – от применения всеобъемлющего эмбарго с блокированием морских и сухопутных границ, до «умных» или адресных санкций.

Как указывают Клиффорд Тэдди и Барри Икес в своей статье «Остановят ли санкции Путина?»: «Нужно понимать разницу между эффективностью и последствиями. Такие экономические показатели, как спад торговли, иностранных инвестиций, кредитных потоков, передачи технологий, снижение ВВП, доходов и т.д. – это последствия санкций. Но эти цифры не говорят, изменит ли Россия свое поведение – т.е. насколько эффективными они будут [7].

Попробуем проанализировать доступную статистику об эффективности санкций. Следует отметить, что практически не существует официальной статистики с объяснением причин и факторов наложения санкций. Среди

основных источников следует упомянуть коллектив авторов во главе с Гари Хафбуэра [8-12], который много лет проводит исследования эффективности политических и экономических санкций, которые применялись ООН, США и др. Рассмотрим статистику, характеризующую динамику и их количественное измерение применимых санкций, приведенных в исследовании .

Таблица 10. Основные отправители санкций (средние значения за десятилетие)

Страна	1970-1989	1990-1999
США	25	38
ЕК/ЕС	5	19
СССР/Россия	0	6
ООН	1	11

*Источник:* Gary Clyde Hufbauer, Jeffrey J. Schott, Kimberly Ann Elliott, Barbara Oegg (2008). Economic Sanctions: New Directions for the 21st Century. Presentation at the book release meeting. July 15, 2008. <https://www.piie.com/commentary/speeches-papers/economic-sanctions-new-directions-21st-century> (дата обращения: 04.05.24)

Как видно из данных, приведенных в таблице, основным инициатором санкций являются США, которые лидируют по количеству введенных санкций в двух временных интервалах (25 и 38), затем Европейский Союз и т.д. В книге выделяются пять основных направлений внешней политики, для достижения которых были использованы санкции:

- изменение политики целевой страны относительно малыми затратами;
- дестабилизация целевого правительства;
- предотвращение военной операции;
- нанести ущерб военному потенциалу страны-мишени;
- значительно изменить политику целевой страны.

В таблице 11 приведены данные о «мишенях» санкций по регионам.

Таблица 11. Санкции «мишени» по регионам (средние значения за десятилетие)

Регион	1970-1989	1990-1999
Африка	5	18
Азия	7	8
Латинская Америка	10	8
Средний Восток	4	3
СССР/бывшие страны СССР	3	8

*Источник:* Gary Clyde Hufbauer, Jeffrey J. Schott, Kimberly Ann Elliott, Barbara Oegg (2008). Economic Sanctions: New Directions for the 21st Century. Presentation at the book release meeting. July 15, 2008. <https://www.piie.com/commentary/speeches-papers/economic-sanctions-new-directions-21st-century> (дата обращения: 04.05.24)

Анализ данных таблицы свидетельствует о незначительных колебаниях в рамках двух временных интервалов. В частности, отмечается рост с 3 до 8 для СССР/бывших стран СССР, для Африки с 5 до 18. И незначительное уменьшение для регионов Среднего Востока (4 и 3) и Латинской Америки (10 и 8).

В таблице 12 приведены данные об результативности достижения политических целей.

Таблица 12. Результативность достижения политических целей

Политическая цель	Успешные случаи	Отрицательные случаи	Всего	Коэффициент успеха (в процентах от общего числа)
Незначительные изменения политики	22	21	43	51
Смена режима и демократизация	25	55	80	31
Предотвращение военных операций	4	15	19	21
Повреждения военной техники и инфраструктуры	9	20	29	31
Другие важные изменения в политике	10	23	33	30
Все случаи	70	134	204	34

Источник: Gary Clyde Hufbauer, Jeffrey J. Schott, Kimberly Ann Elliott, Barbara Oegg (2008). *Economic Sanctions: New Directions for the 21st Century*. Presentation at the book release meeting.

Анализ данных таблицы свидетельствуют о достаточно низком коэффициенте успеха – только 34% для всех случаев введенных санкций. Самый высокий коэффициент успеха отмечается у такой цели, как «незначительные изменения политики» - 51%, самый низкий – у цели «Предотвращение военных операций» - 21%. Наибольшее количество санкций отмечалось для цели «смена режима и демократизация» - 80, успешных только 25, отрицательных – 55.

В таблице 13 приведены данные об уровне результативности санкций в зависимости от типа режима, в % от успешных случаев.

Таблица 13. Результативность в зависимости от типа режима (в % от успешных случаев)

Политическая цель	Автократия	Анократия	Демократия
Незначительные изменения политики	30	50	69
Смена режима и демократизация	23	28	78

Политическая цель	Автократия	Анократия	Демократия
Предотвращение военных операций	33	11	25
Повреждения военной технике и инфраструктуре	37	50	0
Другие важные изменения в политике	9	34	47
Все случаи	28	34	47

Источник: Gary Clyde Hufbauer, Jeffrey J. Schott, Kimberly Ann Elliott, Barbara Oegg (2008). *Economic Sanctions: New Directions for the 21st Century*. Presentation at the book release meeting.

Результаты анализа данных таблицы свидетельствует о преобладании уровня успеха для «демократии» - 47%, больший процент приходится на «смену режима и демократизацию» - 78% от успешных случаев.

В таблице 14 приведено соотношение успеха по типу санкций.

Таблица 14. Успех по типу санкций

Тип санкций	Успешные случаи	Неуспешные случаи	Всего	Частота успеха (в %)
Финансы, экспорт и импорт	25	37	62	40,3
Только финансовые	19	34	53	35,8
Экспорт или импорт или оба	10	30	40	25,0
Финансы и импорт	2	8	10	20,0
Финансы и экспорт	5	23	28	17,9

Источник: Gary Clyde Hufbauer, Jeffrey J. Schott, Kimberly Ann Elliott, Barbara Oegg (2008). *Economic Sanctions: New Directions for the 21st Century*. Presentation at the book release meeting.

Наибольший успех характерен для санкций «финансы, экспорт и импорт» - 40,3 %. (при общем количестве случаев 62, успешных только 25 и неуспешных 37. Самые низкие показатели для санкций «финансы и экспорт» - 17,9 % (при общем количестве 28, успешных случаев только 5 и отрицательных результатов 23).

Таблица 15. Опыт США в отношении санкций со времен Второй мировой войны

1	2	3	4	5	6	7	8	9
США 1945-69								
успехи	14	50,0	1,6	1,8	2,5	3,2	26,3	1,4
неудачи	14	50,0	2,4	2,4	1,4	1,5	28,5	2,1

1	2	3	4	5	6	7	8	9
1970-89								
успехи	13	30,8	1,6	1,6	2,3	1,4	27,2	1,9
неудачи	41	24,3	1,7	2,1	1,9	0,9	16,9	1,8
1990-2000								
успехи	17	29,4	3,0	1,4	2,2	3,9	59,5	1,8
неудачи	33	27,3	2,5	1,6	2,1	2,5	46,5	1,8
Другие страны								
успехи	23	17,4	1,8	2,2	2,4	3,7	21,3	2,0
неудачи	41	43,9	2,0	2,2	2,2	1,8	27,9	2,1

*Источник:* Gary Clyde Hufbauer, Jeffrey J. Schott, Kimberly Ann Elliott, Barbara Oegg (2008). *Economic Sanctions: New Directions for the 21st Century*. Presentation at the book release meeting

Условные обозначения:

- 1 – Страна
- 2 – Количество наблюдений
- 3 - Частота сопутствующих политик (процент случаев)
- 4 – Международная кооперация с индексом отправителей (средние значения)
- 5 – Индекс здоровья и стабильности (средние значения)
- 6 - Индекс предыдущих отношений
- 7 - Стоимость достижения цели (в процентах к ВВП, средние значения)
- 8 – Торговые связи (в %, средние значения)
- 9 - индекс стоимости отправителя (средние значения)

Анализ данных, приведенных в таблице, позволяет сделать следующие выводы. Во-первых, количество введенных санкций США возрастает с 28 (в период 1945-69) до 50 (в период 1990-2000). Во-вторых, индекс стоимости санкций для отправителя, т.е. США, варьируется в пределах от 1,4 до 1,9 для успешных санкций и 2,1 до 1,8 для неудачных санкций.

### **Санкции и экономическая теория**

Экономические эффекты от внедрения санкций многими авторами рассматриваются сквозь призму экономической теории. И этому есть объяснение. Экономическая теория – одна из общественных наук, объектом исследования которой являются отношения между рынком и государством, индивидом и обществом, а также процессы перераспределения богатства в результате политических решений и их экономические эффекты. Независимо от вида санкций (односторонние или многосторонние, универсальные), остается открытым вопрос о получении потенциального дохода в обход санкций за счет более высоких цен в других странах и потерянных рынков.

К сожалению, среди экспертов отсутствует единая точка зрения относительно эффективности модели или моделей для прогнозирования и

анализа последствий санкций. Подобный подход должен помочь в выработке рекомендаций вариантов санкционной политики, которые уравнивают экономическую, гуманитарную и политическую эффективность одновременно. Санкции, в конечном счете, являются макроэкономическим явлением и их последствия должны быть проанализированы и спрогнозированы. Необходимо рассчитывать экономический ущерб, причиняемый санкциями по отношению к целевым социально-экономическим группам, которые возмещают ущерб от санкций. Некоторые аналитики и средства массовой информации заявляют о неэффективности санкций, но ответ находится в других вариантах действий – больше дипломатических переговоров, миротворчества или, в конечном счете, военных действий. Именно подобная постановка проблемы должна расширять понимание сути политических и экономических санкций.

Рассмотрим состав санкций. Во-первых, используем экономическую интерпретацию санкций – это дискриминация страны с помощью ограничения торговых или кредитных потоков в попытке повлиять на текущую политику. Санкции предполагают использование экономического давления, как оружия для ведения невоенной компании, с расширением дипломатического процесса. Одновременно с этим, важным аспектом является поведение третьих стран и их уровень вовлеченности в данные процессы. Поскольку некоторые будут помогать стране, которая ввела санкции, другие будут помогать стране, которая попала под санкции. Все будет зависеть от потенциальной прибыли указанных вариантов.

Таким образом, экономические санкции – дипломатические акты, используемые для изменения политической деятельности иностранного правительства, при условии, что санкции действуют так, как будто они являются макроэкономической политикой, передающей принудительные экономические эффекты от отправителей к целям [13, с.4-5]. Называя эту политику эмбарго, санкциями, принуждением, управлением либо другим термином, обоснование и предполагаемые последствия имеют один и тот же генезис. Поэтому данные термины используются в качестве синонимов. Другими словами, санкция представляет собой квоту или количественное ограничение на количество товаров, услуг или финансовые потоки между двумя странами. Типичная санкция накладывает ограничения при обмене от 0 до 100%.

Жизненный цикл (ЖЦ) санкций, который можно представить в виде следующей последовательности действий: инициирование, оценка, корректировка, достижение целей и снятие, характеризует возможность сравнения и противопоставления отдельных санкций с точки зрения развития.

На начальном этапе основным является решение о введении экономических санкций по отношению к предполагаемому нарушителю международного права. Данный этап формирует правовую основу первоначального решения о санкциях и ограничении полномочий действовать и проистекает из гуманитарного права соответствующих конвенций.



Второй этап ЖЦ санкций характеризуется оценкой их последствий. Оценка осуществляется путем сравнения порогов отдельных показателей, которые установлены в международных гуманитарных конвенциях, которые анализируются на первом этапе, приведенном выше.

На третьем этапе ЖЦ происходит фактическое оспаривание санкций, поиск и идентификация правового форума, национального или международного, и определение содержания и форм претензий.

Заключительный этап ЖЦ включает процесс оспаривания с юридическими, политическими и фактическими последствиями – возмещение ущерба, аннулирование или изменение соответствующих санкций. Именно на данном этапе принятое судебное решение противостоит политическому решению.

Рассмотрим классификацию экономических санкций, приведенную на следующем рисунке [14].

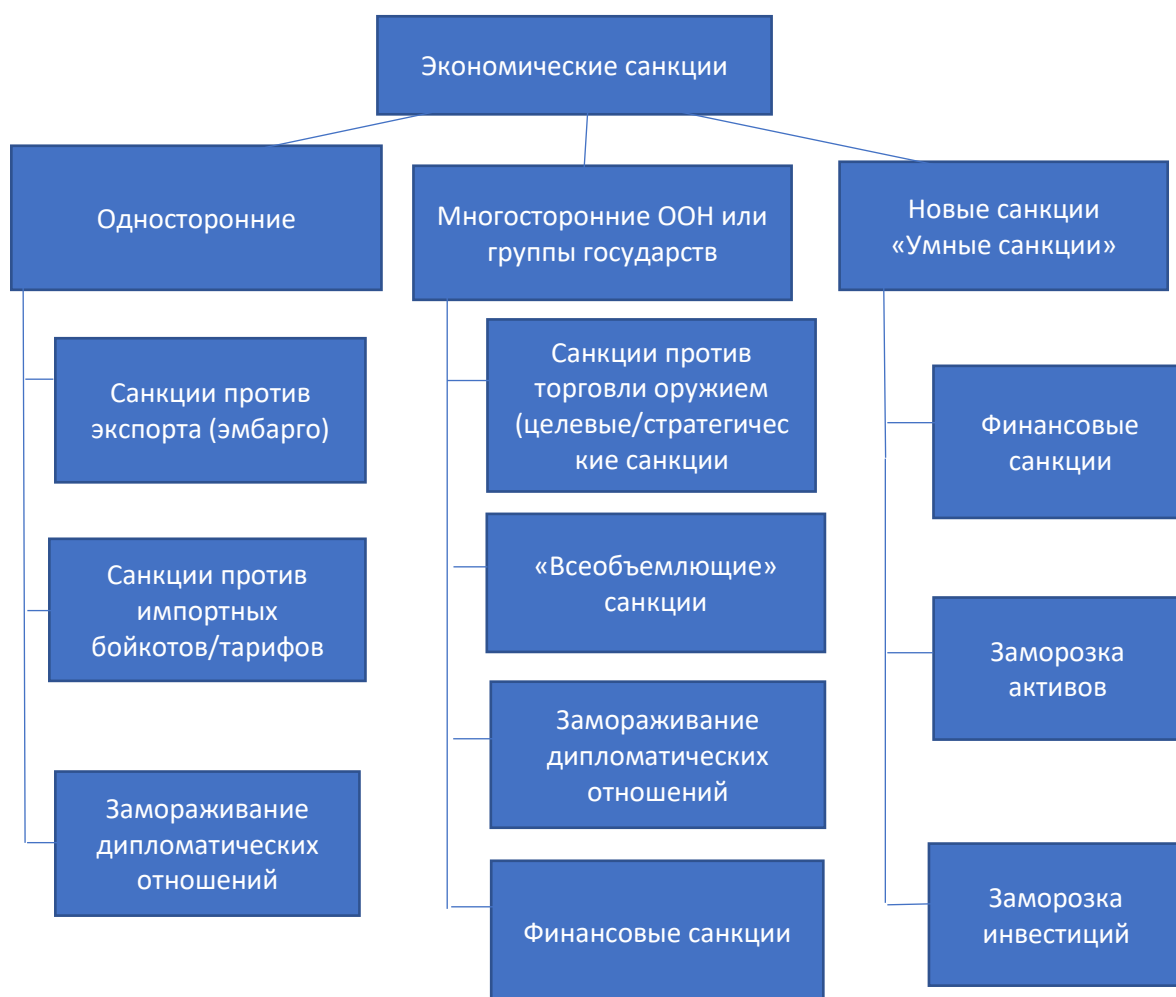


Рис. 1. Классификация санкций

Источник: Golnoosh Hakimdavar (2014). A Strategic Understanding of UN Economic Sanctions International Relations, Law, and Development. Taylor & Francis Group. ISBN: 978-0-203-10946-5

В работе Ли Джонса [15] рассматриваются вопросы содержания санкций. Виды санкций и затронутые им группы экономических агентов приведены в следующей таблице.

Таблица 16. Виды санкций и затронутые группы

Тип	Группы, которые могут быть затронуты
Торговля	<ul style="list-style-type: none"> <li>• Экспортные санкции: страдают группы производителей и экспортеры. Мультипликативные эффекты вероятны в промежуточных секторах.</li> <li>• Импортные санкции: группы потребителей (например, городской средний класс) и секторы, зависящие от импорта, пострадают; могут выиграть отрасли, конкурирующие с импортом. Эмбарго на основные сырьевые товары, такие как нефть, может привести к росту затрат в масштабах всей экономики.</li> <li>• Контрабандисты могут получать неожиданную прибыль.</li> <li>• Государственные органы, зависящие от торгового налогообложения, могут пострадать; доходы также могут пострадать, если потери в торговле снизят общую экономическую активность.</li> <li>• Если санкции приведут к тому, что экспорт упадет ниже импорта, создав дефицит платежного баланса, государственное вмешательство, направленное на снижение спроса на импорт, может замедлить экономическую активность с дальнейшими последствиями.</li> </ul>
Инвестиции	<ul style="list-style-type: none"> <li>• В краткосрочной перспективе местные предприниматели получают выгоду, поскольку они могут приобретать дешевую распродажу активов иностранных фирм, а поскольку капитал становится все более дефицитным, его доходность возрастает.</li> <li>• В долгосрочной перспективе отсутствие инвестиций, передачи технологий и иностранных высококвалифицированных кадров может снизить производительность, прибыль, рост и возможности трудоустройства, особенно для квалифицированных рабочих. Эффект мультипликатора в масштабах всей экономики вероятен.</li> <li>• Государственному аппарату может быть нанесен непосредственный ущерб, если инвестиции являются важным источником иностранной валюты, и косвенно, если задержка роста наносит ущерб налоговым поступлениям.</li> <li>• Отказ от инвестиций может привести к снижению спроса и, следовательно, стоимости местной валюты, снижая покупательную способность импортеров и увеличивая</li> </ul>

Тип	Группы, которые могут быть затронуты
	расходы по погашению внешнего долга как для частных, так и для государственных заемщиков.
Помощь и финансы	<ul style="list-style-type: none"> <li>• Непосредственно вредит группам, зависящим от внешней помощи/финансирования, т.е. за средства к существованию или инвестиционный капитал. Возможный мультипликативный эффект.</li> <li>• Наносит прямой ущерб государственному аппарату, зависящему от зарубежной помощи и займов; и косвенно сектора, на которые эти ресурсы будут потрачены.</li> </ul>
Ресурсы	<ul style="list-style-type: none"> <li>• Наносит вред тем, чьи активы заморожены, и их иждивенцам.</li> </ul>
Денежный (валютные манипуляции)	<ul style="list-style-type: none"> <li>• Импортёры, экспортёры и потребители (частные и государственные) страдают от волатильности цен и изменений покупательной способности.</li> <li>• Частные и государственные заемщики с кредитами в иностранной валюте сталкиваются с более высокими затратами на погашение.</li> <li>• Правительству может быть нанесен идеологический удар, если национальная валюта будет иметь идеологический резонанс.</li> <li>• Секторы, не связанные с торговлей, или жизнеобеспечение будут затронуты в меньшей степени.</li> </ul>
Оружие	<ul style="list-style-type: none"> <li>• Может ограничить способность государства к войне или внутреннему принуждению.</li> <li>• Как и в случае с эмбарго на импорт в целом, потенциальные непредвиденные выгоды для отечественных производителей и контрабандистов</li> </ul>

*Источник:* Lee Jones (2015). *Societies Under Siege. Exploring How International Economic Sanctions (Do Not) Work.* Oxford University Press. ISBN 978-0-19-874932-5

Отличным подспорьем исследований эффективности санкций выступает «Глобальная база данных о санкциях (GSDB -The Global Sanctions Data Base) [16]. GSDB охватывает 729 публично отслеживаемых, многосторонних, плюрилатеральных и чисто двусторонних санкций за период с 1950 по 2016 годы (<https://www.globalsanctionsdatabase.com>). Кроме того, GSDB классифицирует эти санкции на основе трех важных аспектов. Во-первых, по типу рассматриваемых санкций (например, торговые санкции, финансовые санкции, санкций за поездки и т.д.). Во-вторых, по политическим целям, стоящим за наблюдаемыми санкциями. В частности, система GSDB группирует цели санкций в отдельные категории (например, изменение политики, дестабилизация режима, предотвращение войны, права человека и т.д.) зарегистрированных целей политики. В-третьих, по воспринимаемой степени успеха для каждой идентифицированной санкции, охватываемой

пятью отдельными категориями, начиная от неудачных санкций и заканчивая полным согласием цели с требованиями отправителя.

GSDB определяет санкции как обязательные ограничительные меры, применяемые отдельными странами, группами стран, Организацией Объединенных Наций (ООН) и другими международными организациями для устранения различных видов нарушений международных норм путем побуждения целевых стран изменить свое поведение или ограничить свои действия. Санкции классифицируются в GSDB по трем основным параметрам, включая: тип санкции, цели санкции и успех санкции.

GSDB классифицирует санкции по типу в пяти категориях, охватывающих: торговлю, финансовую деятельность, вооружение, военную помощь, поездки, а также остаточную категорию, включающую другие санкции.

Рассмотрим торговые санкции. GSDB определяет торговые санкции как меры, направленные на сдерживание экономического взаимодействия со страной-мишенью путем ограничения международной торговли. Авторы отмечают, что ключевым мотивирующим фактором для создания GSDB была необходимость количественной оценки экономического воздействия торговых санкций. Для достижения этой цели GSDB стремится охватить три важных аспекта торговых санкций.

Во-первых, в зависимости от направления торговых потоков GSDB различает санкции в отношении экспорта от отправителя к получателю (т. е. экспортные санкции), санкции в отношении импорта от получателя к отправителю (т. е. импортные санкции) и санкции, которые одновременно применяются как к экспорту, так и к импорту между двумя сторонами (т. е. двусторонние торговые санкции).

Во-вторых, GSDB проводит различие между санкциями, которые применяются только к определенным товарам и/или определенному сектору торговли (т. е. частичные торговые санкции) или ко всем секторам (т. е. полные торговые санкции).

В-третьих, GSDB проводит различие между санкциями, налагаемыми одной страной (т.е. односторонние санкции) по сравнению с санкциями, которые вводятся одновременно многими странами (т. е. многосторонние санкции).

И, наконец, финансовые санкции. Еще одной важной категорией санкций, охватываемых GSDB, являются финансовые ограничения. Значение финансовых ограничений со временем значительно возросло, прежде всего по двум причинам. Первая связана с расширением глобальной экономической деятельности, в том числе с интеграцией финансовых рынков. Вторая связана с тем фактом, что финансовые санкции могут применяться, отслеживаться и обеспечиваться относительно легче благодаря достижениям в области информационных технологий. В многих случаях эти санкции включают замораживание обмена финансовыми активами и инвестициями. Иностранные активы могут быть заморожены полностью или частично для определенных

лиц, как правило, влиятельных политиков или лидеров отрасли (адресные санкции). Аналогичным образом, финансовые санкции могут ограничивать прямые инвестиции и/или ограничивать доступность кредита для платежей при обмене товаров, включая выплаты помощи. В последние годы эффективность финансовых санкций была дополнительно повышена за счет технического запрета любых финансовых транзакций, связанных с подпадающей под санкции экономикой, и за счет применения новых методов правоприменения (таких как запрет на участие в SWIFT).

Ограничения на путешествия. Данные ограничения классифицируются как ограничения на поездки, когда они ограничивают свободу географического передвижения физических лиц. GSDB определяет два типа санкций за поездки: ограничения на поездки людей в страну-отправителя; и поездки из страны, на которую распространяются санкции, в страну, на которую распространяются санкции. Некоторые случаи включают запрет на поездки только для дипломатического персонала стран, на которые распространяются санкции. Этот тип индивидуального ограничения на поездки определяется отдельно в GSDB.

Санкции в экономической сфере имеют множество целей. Одной из них выступает снижение предпринимательского потенциала, путем снижения эффективности предпринимательской деятельности и ограничения инвестиционных потоков.

Еще на заре санкционной кампании против России в 2014-2015 гг. велись активные дискуссии относительно экономической составляющей санкционных мер.

По заявлению руководства страны в апреле 2015 г., из-за санкций Россия недополучила 160 млрд дол. в виде инвестиций. Эксперты прогнозировали банкротство и сокращение российского предпринимательского сектора. Однако по мнению экспертов Национального института системных исследований проблем предпринимательства, «появление новых успешных стартапов тоже неизбежно, даже среди предпринимателей кто-то видит больше возможностей и рискует больше других» [17]. В теории запрет на ввоз целого ряда продукции и девальвация – это серьезный стимулирующий фактор для появления новых производств и развития старых. Девальвация, по мнению В. Буева, – это шанс для развития (включая импортозамещение) даже целых отраслей: продукция становится более конкурентоспособной по цене. Но серьезные сдвиги, по мнению эксперта, возможны не в краткосрочном, а в лучшем случае в среднесрочном периоде (3–5 лет).

Но и инициаторы «санкционного противостояния» тоже несут убытки. По заявлению министра иностранных дел Испании Хосе Мануэль Гарсиа-Маргальо, из-за санкций против России Евросоюз потерял 21 млрд евро [18].

История экономической мысли знает сторонников научно обоснованного положительного влияния экономической изоляции на развитие страны. В частности, в их числе представители немецкой исторической школы экономической теории (Ф. Лист, В. Зомбарт, М. Вебер и др.), которые считали,

что экономика каждой страны развивается по своим собственным законам, которые связаны с ее географическими условиями, национально-культурными традициями и даже чертами национального характера. Политика свободной международной торговли считалась приемлемой только для стран, находящихся на высших стадиях экономического развития. Страны, находящиеся на стадии институционального становления, должны придерживаться «воспитательного протекционизма», то есть вводить ограничения на импорт и поддерживать национального производителя [19]. Ограничивая приток продукции извне, развитые страны фактически дают возможности для развития внутреннего производства в России и создания условий для становления собственного внутреннего рынка. В качестве угроз, возникающих в процессе развития отечественных малых и средних предприятий, необходимо отметить следующие:

- политико-экономические (возможность ограниченной и неэффективно распределенной поддержки либо ее полное отсутствие в связи с изменением политических приоритетов страны в пользу поддержки обороноспособности в современных условиях сложной геополитической обстановки в отношении Украины, США и ряда европейских стран);

- экономические, обусловленные нестабильной экономической ситуацией в стране (низкий спрос и платежеспособность конечного потребителя, отсутствие приемлемых финансовых инструментов для пополнения оборотных и внеоборотных средств из-за высоких процентных ставок по привлекаемым заемным средствам (особенно это сказывается на предпринимательстве в промышленном секторе));

- социальные, напрямую связанные с экономическими и политическими угрозами (рост социальной напряженности трудоспособного населения из-за невысокого уровня оплаты труда и стремления работать на крупных предприятиях, характеризующихся относительной стабильностью по сравнению с малыми и средними);

- технологические (проблема технологического отставания в производственной сфере, связанная с отсутствием собственных средств на развитие технологий у отечественных малых и средних предприятий); правовые (изменения, ежегодно вносимые в законодательство, особенно в сфере налогообложения (например, ставки и перераспределение отчислений по фондам по оплате труда в России меняются ежегодно, благодаря чему появляется возможность построить долгосрочную стратегию управления финансами)).

Иллюстрируя макроэкономический эффект воздействия санкций на состояние экономики приведем отрывок из статьи известного российского экономиста Нуреева Рустема Махмутовича «Экономические санкции запада и российские антисанкции: успех или провал?» в Журнале институциональных исследований (в соавторстве с Бусыгиным) [20].

Нуреев Р.М. рассматривает последствия от действий российского правительства в лице Центрального Банка на примере модели Манделла-

Флеминга (или по-другому ISLM-BP). На рис. 2 наглядно видно, каким образом правительство попыталось покрыть дефицит бюджета, который был вызван в том числе снижением уровня ВВП при фиксированной ставке рефинансирования (ключевой ставке) (ВВП уменьшился на 2.5 трлн. рублей – с 63 трлн. рублей в 2014 до 60.6 трлн. рублей в 2015). В результате значительного снижения экспорта кривая IS сдвинулась влево (из положения  $IS_0$  в положение  $IS_1$ ); то же самое произошло с кривой BP за счет снижения чистого экспорта (в 2015 году - 146 млрд долларов, в 2014 - 189.7 млрд долларов) и вывода капитала из России, что произошло в результате введения санкций и снижения цен на нефть; увеличение ключевой ставки (при этом ставка рефинансирования осталась без изменения) приводит к сдвигу кривой LM влево. В результате того, что с 2014 года рубль был отпущен, – это привело к резкому падению курса рубля, что в значительной степени помогло справиться с дефицитом бюджета (по данным Минфина на 2015 год дефицит бюджета РФ составил 1.96 трлн. рублей). Таким образом,  $E_2$  становится равновесной точкой модели, но проводимая правительством политика негативно отражается как на компаниях, так и на потребителях.

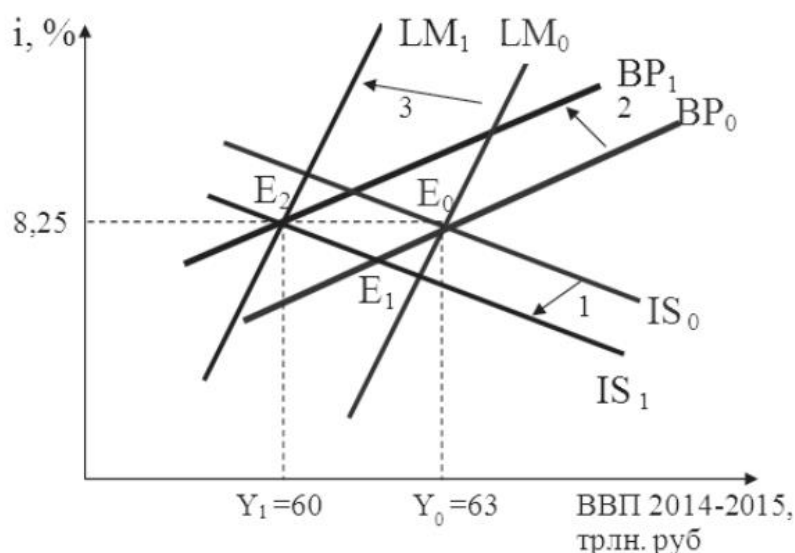


Рис. 2. Влияние санкций на кривые IS-LM-BP в 2014-2015 годах  
 Источник: Нуреев Р.М., Бусыгин Е.Г. (2016) Экономические санкции запада и российские антисанкции: успех или провал? Журнал институциональных исследований. № 1

Также авторами указывается, что путь импортозамещения, который был выбран в результате введения санкций западными странами, в большей степени был вынужденной мерой, продиктованной сверху. Исходя из исследования, опубликованного в отчете «The Global Competitiveness Report 2016-2017», проводимого Всемирным Экономическим форумом, Россия заняла 91 место по такому показателю, как конкуренция на внутреннем рынке (что включает в себя оценку интенсивности конкуренции, степень

доминирования участников рынка, эффективность антимонопольного законодательства и другое) (World Economic Forum). Что касается показателя международной конкурентоспособности (который включает анализ тарифной

политики, распространенность иностранной собственности в РФ, импорт и другое), Россия заняла 120 место (World Economic Forum). Исходя из этих данных, можно сделать вывод, что текущая ситуация, сложившаяся в результате введения санкций, может привести к ухудшению конкурентоспособности российских предприятий как на внешнем, так и на внутреннем рынках. Особенно это касается пищевой промышленности, где конкуренция снизилась в результате введения продуктового эмбарго, что, в свою очередь, может привести не только к ухудшению качества выпускаемой продукции, но и к уменьшению вложений в новые технологии.

Обращаясь к экономическим санкциям, введенным против России США и странами ЕС, следует отметить, что их список велик (табл.17)

Таблица 17. Направленность экономических санкций, введенных против России странами ЕС и США в 2014–2015 гг.

	ЕС	США
Оборонно-промышленный комплекс	<ul style="list-style-type: none"> <li>– запрет организации долгового финансирования для трех оборонных концернов России («Уралвагонзавод», «Оборонпром», «Объединенная авиастроительная корпорация»);</li> <li>– включение в санкционный список девяти российских оборонных концернов;</li> <li>– эмбарго на импорт и экспорт оружия и подобного материала в Россию; – запрет на экспорт товаров двойного назначения и технологий для военного использования в Россию или российским конечным военным пользователям.</li> </ul>	<ul style="list-style-type: none"> <li>– прекращение лицензирования экспорта в Россию товаров и услуг оборонного назначения;</li> <li>– приостановление сотрудничества с Россией в сфере борьбы с наркотиками;</li> <li>– запрет на продажу России высокотехнологичных товаров, которые могли бы усилить боеспособность российской армии, и аннулирование ранее выданных лицензий на их поставки.</li> </ul>
Экономическая сфера	<i>Финансовые ресурсы</i>	
	<ul style="list-style-type: none"> <li>– прекращение финансирования новых проектов в России Европейским инвестиционным банком;</li> <li>– запрет на инвестиции в инфраструктурные, транспортные,</li> </ul>	<ul style="list-style-type: none"> <li>– американским гражданам и компаниям запрещено покупать облигации банков и корпораций, затронутые секторальными санкциями, а также</li> </ul>



	ЕС	США
	<p>телекоммуникационные и энергетические секторы и оказание для них финансовых и страховых услуг;</p> <p>– запрет европейским финансовым структурам выдавать кредиты или приобретать доли в проектах, которые затронуты секторальными санкциями;</p> <p>– ужесточение ограничений на предоставление займов и инвестиционных услуг для банков России.</p>	<p>предоставлять им кредиты;</p> <p>– замораживание банковских счетов лиц, против которых были применены санкции.</p>
<i>Отраслевой комплекс</i>		
<i>Торговля</i>		
	<p>Запрет на покупку 250 наименований товаров, среди которых полезные ископаемые, минералы и углеводороды.</p>	<p>– исключение России из торговой программы, позволяющей странам с переходной экономикой беспошлинно импортировать в США товары;</p> <p>– ужесточение экспортного режима в отношении российских компаний.</p>
<i>Нефтегазовая промышленность</i>		
	<p>– принятие резолюции рекомендательного характера, призывающей отказаться от строительства газопровода «Южный поток»;</p> <p>– запрет организации долгового финансирования трех топливно-энергетических компаний России;</p> <p>– запрет на добычу нефти, газа и минералов, поставку оборудования для этих секторов, оказание для них финансовых и страховых услуг;</p> <p>– запрет на покупку полезных ископаемых минералов и углеводородов;</p>	<p>Запрет на поставку в Россию оборудования для глубоководной добычи (свыше 152 метров), разработки арктического шельфа и сланцевых запасов нефти и газа, поставку технологий нетрадиционной добычи энергоносителей.</p>

	ЕС	США
	– запрет на поставки в Россию высокотехнологичного оборудования для добычи нефти в Арктике, на глубоководном шельфе и сланцевой нефти.	
Сфера образования	– отмена саммита ЕС–Россия; – отказ от участия в конференции «Энергетический диалог Россия–ЕС: газовый аспект».	Отмена большинства планируемых конференций, совместно проводимых Россией и США.
Политическая сфера	- ввод санкций против государственных и военных деятелей (физических лиц) РФ и Крыма – запрет въезда на территорию Евросоюза или транзита; – запрет посольствам ЕС в России выдавать жителям Крыма все виды виз.	– ввод санкций против государственных и военных деятелей (физических лиц) РФ и Крыма; – прекращение работы российско-американской президентской комиссии.

*Источник:* Пескова (Орлова) Д.Р., Евсеева О.А. (2015) Санкционированное развитие российского предпринимательства. Экономика и управление: научно-практический журнал, № 3

Отметим основные, с нашей точки зрения, возможности дальнейшего эффективного развития отечественных малых и средних предприятий как основных субъектов предпринимательской деятельности в современных условиях: государственная поддержка; венчурное финансирование; развитие инновационной деятельности; кооперация с крупными предприятиями (особенно актуально для промышленных предприятий); кооперация с научно-исследовательскими и образовательными учреждениями; работа в кластерах, особых экономических зонах; реализация акселерационных программ для промышленности и дистанционное обучение предпринимательству.

Кроме государственной финансовой поддержки, совершенствования информационного пространства, необходимо обратить внимание и на внутренние резервы для развития у самих предприятий: в этой связи возможности для развития предоставляет формирование стратегии, ориентированной на повышение эффективности использования совокупного потенциала развития, на уровне предприятия.

Политика импортозамещения при выборе эффективных новых «точек роста», не зависимо от характера изначального стимула, может давать высокие результаты в области повышения уровня благосостояния страны.

В этих условиях малый и средний бизнес как активный субъект предпринимательской деятельности может послужить одной из таких «точек роста» и способствовать выходу из кризисного состояния. В современных

условиях важно стимулировать его развитие, ориентированное на устойчивый рост в долгосрочной стратегической перспективе.

## Литература

1. Mark Daniel Jaeger (2018). *Coercive Sanctions and International Conflicts: A Sociological Theory*. Routledge. ISBN: 978-1-315-52243-2
2. Masahiko Asada (2020). *Economic Sanctions in International Law and Practice*. Routledge. ISBN: 978-0-429-05298-9
3. Margaret P. Doxey (2000). Sanctions through the Looking Glass the Spectrum of Goals and Achievements. *International Journal* Vol. 55, No. 2 (Spring, 2000), pp. 207-223. <https://www.jstor.org/stable/40203477>; doi.org/10.2307/40203477 (дата обращения: 04.05.24)
4. Margaret P. Doxey (1980). *Economic Sanctions and International Enforcement*. The Macmillan Press LTD. ISBN 978-1-349-04335-4. DOI 10.1007/978-1-349-04335-4
5. Margaret P. Doxey (1996). *International Sanctions in Contemporary Perspective*. The Macmillan Press LTD. ISBN 978-1-349-25016-5. DOI 10.1007/978-1-349-25016-5
6. Kim Richard Nossal (1998). *International Organization*. Vol. 43, No. 2 (Spring, 1989), pp. 301-322. <https://www.jstor.org/stable/2706704> (дата обращения: 04.05.24)
7. Клиффорд Гэдди, Барри Икес. Остановят ли санкции Путина? Россия в глобальной политике. 02.07.2014. <https://globalaffairs.ru/articles/ostanovyat-li-sankczii-putina/> (дата обращения: 04.05.24)
8. Gary Clyde Hufbauer, Jeffrey J. Schott, Kimberly Ann Elliott, Barbara Oegg (2008). *Economic Sanctions: New Directions for the 21st Century*. Presentation at the book release meeting. July 15, 2008. <https://www.piie.com/commentary/speeches-papers/economic-sanctions-new-directions-21st-century> (дата обращения: 04.05.24)
9. Hufbauer, G.C., Schott J.J., Elliot, K.A. and Oegg, B. (2007) (3rd edn). *Economic Sanctions Reconsidered. History and Current Policy*, Washington, DC: Institute for International Economics.
10. Gary Clyde Hufbauer, Jeffrey J. Schott, Barbara Oegg (2001). *Using Sanctions to Fight Terrorism*. <https://www.piie.com/publications/policy-briefs/using-sanctions-fight-terrorism> (дата обращения: 04.05.24)
11. Gary Clyde Hufbauer, Jeffrey J. Schott. *Economic Sanctions and U.S. Foreign Policy*. PS: Political Science & Politics, Volume 18, Issue 4, Fall 1985, pp. 727 - 735 DOI: <https://doi.org/10.1017/S1049096500022654>
12. Gary Clyde Hufbauer, Euijin Jung. What's new in economic sanctions? *Eur Econ Rev*. 2020 Nov; 130: 103572. doi: 10.1016/j.eurocorev.2020.103572. <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7518878/> (дата обращения: 04.05.24)

13. Robert Eyster (2007). *Economic Sanctions International Policy and Political Economy at Work*. Palgrave Macmillan. ISBN 1–4039–7463–2
14. Golnoosh Hakimdavar (2014). *A Strategic Understanding of UN Economic Sanctions International Relations, Law, and Development*. Taylor & Francis Group. ISBN: 978-0-203-10946-5
15. Lee Jones (2015). *Societies Under Siege. Exploring How International Economic Sanctions (Do Not) Work*. Oxford University Press. ISBN 978-0-19-874932-5
16. Gabriel Felbermayr, Aleksandra Kirilakha, Constantinos Syropoulos, Erdal Yalcin Yoto V. Yotov (2020). *The Global Sanctions Data Base*. <https://drive.google.com/file/d/11djwEIr96SFt6YpMzo9gaB6ZJrOer8AX/view> (дата обращения: 04.05.24)
17. Буев В. В. (2015) России не любят бизнес // *Ведомости*. 16 января.
18. Пескова (Орлова) Д.Р., Евсеева О.А. (2015) Санкционированное» развитие российского предпринимательства. *Экономика и управление: научно-практический журнал*. № 3
19. Березин И. (2000) *Краткая история экономической мысли*. ISBN: 5-93840-007-4
20. Нуреев Р.М., Бусыгин Е.Г. (2016) Экономические санкции запада и российские антисанкции: успех или провал? // *Журнал институциональных исследований*. № 1. 2016.

## ГЛАВА 5. ОСОБЕННОСТИ САНКЦИЙ В СФЕРЕ ИТ

Попытки исследовать эффективность санкций мировым научным сообществом производятся уже более сорока лет, но обоснование факторов, определяющих успех санкций, пока не дало результатов [1-4]. Положение усугубляется тем, что сами санкции претерпевают глубокую трансформацию. Классические санкции носили экономический характер, но в 90-х годах на первый план вышли так называемые целевые или «умные» санкции (smart sanction).

Данный вид санкций направлен не на общество в целом, а на конкретных лиц, управляющих в санкционированной стране. Для этого используют разнообразные меры, а том числе такие, как запрет на выдачу виз, финансовые санкции, эмбарго на поставки вооружений и запреты на полеты. Особое значение приобретают санкции в сфере информационных технологий, их число и разнообразие форм активно возрастают. Рассмотрению их разновидностей и их особенностей посвящена эта глава.

### КИБЕРБЛОКАДА

Технологии, особенно информационно-коммуникационные, обеспечили новую возможность людям вести войны и вмешиваться в дела других государств во всех сферах деятельности. В дополнение к стимулированию человеческой экспансии в новые области, такие как суша, море и воздух, технологии обеспечили разработку новых средств и методов, с помощью которых можно вести войну и интервенцию. С созданием киберпространства кибервойны и вмешательство с помощью кибератак стали возможными и превратились в обычное явление на уровне государств и коммерческих структур. Каждая новая область расширения поднимала сложные правовые проблемы, с которыми государства сталкивались, полагаясь на существующее международное право с соответствующими корректировками, с целью обозначить и учесть уникальные атрибуты новой области. Многие юристы, специализирующиеся в области международного права совместно со специалистами в области ИТ, пытались исследовать и решить проблему разработки законодательства о кибервойне и кибервмешательстве на основе существующего международного права [5-9 и др.].

Помимо правовых проблем, связанных с функционированием новой сферы приложения ИТ, следует отметить определенные трудности с определением основных категорий, что привело к отсутствию ясности в научных и практических исследованиях. В частности, различные способы определения такой категории, как кибератака, что приводит к разночтениям в оценках применения силы.

Новым разделом, который описывает организацию и действие санкций, является область киберпространства, описать которую еще предстоит. В частности, появился новый политический инструмент и новое оружие воздействия – киберсанкции. С развитием компонент ИТ, под воздействием

которых сформировалась цифровая среда, последняя превратилась в арену конкуренции между ведущими в информационном плане государствами. Сформировалась целая система вызовов цифровой среды по отношению к личности, обществу и государству [7-9].

Киберсанкции определяются как экономические и финансовые меры, направленные на изменение поведения целей с использованием злонамеренных действий в киберпространстве и/или вторжений [10]. Анализ теории и практики взаимодействия различных субъектов в кибернетической сфере свидетельствует о том, что концепция киберсанкций является относительно новым направлением исследований в мировой политике.

Общее определение киберсанкций следующее: «Киберсанкции определяются как экономические и финансовые меры, направленные на изменение поведения целей с использованием злонамеренных действий в киберпространстве и/или вторжений. Поскольку режимы киберсанкций используются странами, эти инструменты используются преимущественно странами. Таким образом, единицами анализа являются страны международной системы. Другими словами, страны, а не негосударственные субъекты, включая компании, являются основными субъектами и лицами, принимающими решения, когда речь идет об угрозе и/или применении киберсанкций на международном уровне. Концепция киберсанкций является относительно новым направлением в мировой политике. Сегодня у нас есть несколько стран, которые приняли меры и приняли законодательство, включающее регулирование, связанное с кибербезопасностью, для защиты своих информационных технологий. С другой стороны, многие страны, в том числе развитые страны, не обновили свое законодательство в соответствии с этой новой областью безопасности, то есть киберпреступлениями [10].

Множество экспертов отмечают отсутствие единого международного института-регулятора оценки действий государств в киберпространстве, а также существующего недоверия к механизмам киберсанкций [11]. Односторонняя санкционная политика США и ЕС направлена на «сдерживание» ряда стран, в числе которых РФ, Китай и др., в целях утверждения собственного доминирования в ряде областей (экономика, торговля, научные исследования и т.д.). Еще один важный момент отмечают эксперты – применяемые санкции основываются только на предположениях и отсутствии доказательной базы, что приводит к нерешенной проблеме атрибуции, т.е. определению источника кибератаки. Тем более, что современные ИТ позволяют маскировать нарушителю собственные действия и скрывать истинное местоположение (например, нелегальные торговые площадки, специальное программное обеспечение, предлагаемые наборы криминальных услуг, среда DarkNet и т.д.).

Киберсанкции входят в состав односторонних ограничительных мер. Киберсанкции появились в 2015 году и их появление было обусловлено ускоренным развитием ИКТ, ростом числа киберинцидентов и отсутствием глобального партнерства для решения проблем, связанных с

функционированием цифровой среды. Они включали в себя заморозку активов, финансовые ограничения, блокировку аккаунтов в социальных сетях, цифровую изоляцию, запрет на въезд. Эксперты отмечают весьма важную деталь – киберсанкции вводятся за деятельность в нерегулируемом кибернетическом пространстве, причастность к которой в настоящее время нельзя достоверно доказать [12]. Вопросы атрибуции в настоящее время имеют преимущественно политический и декларативный характер.

Проблема атрибуции, т.е. сложность выяснения того, кто организовал киберконфликт была одной из самых обсуждаемых [13]. Некоторые итоги эмпирической практики были доложены публично, однако подобные заявления часто остаются весьма спорными. Публичная атрибуция в самой элементарной форме – это возложение вины на конкретного субъекта как ответственного за киберинцидент. Данный процесс могут проводить самые разные субъекты, включая правительства, коммерческие компании, неправительственные организации и научные круги. Приписывание правительством ответственности имеет особое значение, поскольку действия правительства по возложению вины по своей сути являются политическим актом. Таким образом, правительство обладает сильным стимулом использовать публичную атрибуцию в качестве политического инструмента, что требует дополнительного исследования в современных условиях. Сам процесс публичной атрибуции можно условно разделить на две фазы: комплекс механизмов, которые приводят к публичной атрибуции и то, что происходит после того, как инцидент публично приписывается. Следует отметить, что эти фазы мало исследованы по отношению к атрибуции киберинцидентов. Особого внимания заслуживает вторая фаза – что происходит после того, как правительство обнародует информацию о киберинциденте. Понимание сущности данного этапа является очень важным, поскольку публичная атрибуция киберинцидентов является одним из основных источников, из которых общественность узнает о том, кто кого атакует в киберпространстве, тем самым формируя восприятие угрозы широкими слоями общества. Таким образом формируется пространство знаний, в которое вводятся утверждения об атрибуции.

Эти знания структурно формируют наше понимание и восприятие конфликта с помощью комплекса факторов – операционным (политическим, коммерческим и юридическим) и структурным. Имеется в виду следующее – коммерческие стимулы со стороны частного сектора и политическая предвзятость со стороны правительства, приводят к тому, что общедоступные структурные данные о киберконфликте вызывают недоверие к публичным заявлениям об атрибуции. В решении данной проблемы должны внести свой вклад научные исследования [14-17 и др.]

Рассмотрим кратко суть процесса атрибуции, используя [18-21]. Кибератрибуция — это процесс, с помощью которого собираются, анализируются и связываются доказательства злонамеренной киберактивности с исходной стороной (т. е. злоумышленником) [19].

Указывается, что растет объем литературы, посвященной техническим проблемам приписывания киберинцидента физическому лицу или государственному учреждению. Кроме того, в некоторых исследованиях рассматривались конкретные стратегические, юридические и этические проблемы, возникающие, когда стране, организации или физическому лицу пытаются приписать киберсобытия.

Считаем необходимым привести доводы, которые были использованы для ввода санкций из-за якобы вмешательства российских хакеров в местные выборы в Болгарии в 2015 году. Кибератаки были организованы на сайты Центризбиркома, МВД и другие государственные ведомства. Начальник управления по борьбе с киберпреступностью МВД Болгарии Явор Колев сообщил об этом во время конференции «Киберпреступность в Евросоюзе: как предупредить растущую угрозу»: Группа связана с военной разведкой России и **подозревается** (выделено авторами) в организации ряда атак на болгарские сайты в 2015 году, во время проведения местных выборов, а также в манипуляциях во время избирательной кампании в США, – заявил Колев [22].

Ранее председатель Комиссии по общественному порядку парламента Болгарии, заместитель председателя правящей партии ГЕРБ (Граждане за европейское развитие Болгарии) Цветан Цветанов также отметил, что Россия **чаще всего упоминалась** (выделено авторами) на Софийской конференции как государство, которое может вмешиваться в выборы, которые проходят в странах Евросоюза, в том числе и выборы в Европарламент [23].

Еще серьезнее приведены доводы с статье Дэвида Перера «Российские хакеры атаковали нефтеперерабатывающую компанию в стране НАТО» [24]. «Отсюда и попытка компрометации **неустановленной нефтеперерабатывающей компании в неустановленной стране, которая является членом военного альянса** (выделено авторами). По словам исследователей, это расширение целей отражено в том, что группа использует фишинговые приманки на английском языке, а также стандартные сообщения на украинском языке.»

Еще один характерный пример. Хакеров из Китая подозревают в многолетнем шпионаже за VW. Злоумышленники похитили тысячи файлов и за кибератаками на автомобильный концерн могут стоять китайские хакеры [25]. Журналист Жан Рофу (DW) опубликовал заметку о том, что Германский автомобильный концерн Volkswagen (VW) на протяжении нескольких лет подвергался атакам хакеров, предположительно из Китая. О кибератаках ранее сообщили немецкий еженедельник Der Spiegel и телеканал ZDF, ссылаясь на внутренние документы VW. По их информации, атаки происходили в несколько волн с 2010 по 2015 год. В 2010 году хакеры начали анализировать ИТ-инфраструктуру Volkswagen, чтобы выявить возможные лазейки. Это им удалось уже через год. В период с 2011 по 2014 год было зафиксировано несколько утечек данных, свидетельствуют документы компании. Следы указывают на Китай.



Прямых доказательств причастности Китая нет, но есть множество косвенных свидетельств. В частности, IP-адреса хакеров вели к Пекину и китайским военным, рассказал один из инсайдеров. Почти все эксперты, с которыми беседовали Der Spiegel и ZDF, в том числе сотрудники немецких органов безопасности, также считают атаку государственных хакеров КНР **весьма вероятной** (выделено нами).

Вот и вся атрибуция!

В.Котенко и С.Хмыров в [15] представили комплексный анализ моделей и методик атрибуции киберинцидентов. Они указывают, что: «Постоянно меняющийся ландшафт киберугроз и стремительный рост экосистемы рынков даркнета позволил применять на практике схожий инструментарий, усложняя идентификацию конкретной кибергруппировки. Методы запутывания аналитиков и аналитических систем во время расследования инцидента также затрудняют атрибуцию. АРТ стараются подделывать время компиляции, работают в нерабочее время, внедряют различные языки или уникальные культурные свидетельства в строки кода, повторно регистрируют ранее используемые командно-управляющие домены других злоумышленников и т.п.». Дополнительным действием является применение универсального программного обеспечения (ПО), которое эффективно при достижении краткосрочной цели или выполнении узконаправленной задачи. Такое же ПО используют как кибергруппировки, так и отдельные нарушители. Поскольку в большинстве случаев применяется одно и то же ПО, выяснить, стоит ли за целевой кибератакой АРТ или обычный злоумышленник очень проблематично. Соответственно, свидетельства и доказательства, применяемые для атрибуции атак, можно подделать и замаскировать, тем самым усложнив атрибуцию. Последний вывод для нас является весьма важным. Другими словами, процесс публичной атрибуции может быть проведен на основе ложных или измененных данных, характеризующих киберинцидент.

В качестве основных проблем атрибуции выделяются следующие:

- постоянное прогрессирование АРТ;
- определение источников (мест запуска и инициализации) кибератаки;
- определение ответственного за кибератаку (основного актора);
- обработка большого количества несортированных (сырых) данных;
- децентрализация и запутанность существующих систем публично-частной атрибуции;
- использование методов имитации кибератак с целью формирования ложных обвинений конкретного нарушителя, кибергруппировки и/или государства;
- АРТ часто применяют определенные методы и сценарии реализации атаки, выстраивая необходимую среду (экосистему) для достижения поставленных целей, выполняется распределенная согласованная последовательность сложно отслеживаемых этапов (возможно несколько зависимых или независимых цепочек действий).

Рассмотрим доступную статистику, характеризующую количественную структуру АРТ. Для этого используем сохранившиеся архивные данные с сайта <https://apt.thaicert.or.th/cgi-bin/aptstats.cgi> (Thailand Computer Emergency Response Team) [26]. Данные охватывают временной интервал с 19 июля 2020 г. по 21 января 2022 года. Статистика базы данных по состоянию на 17 июля 2020 года представлена в следующей таблице.

Таблица 17. Энциклопедия угроз

№ п/п	Показатель	Значение
1	Всего групп угроз	312 (в том числе 239 АРТ, 40 других, 33 неизвестных)
2	Всего псевдонимов групп	794
3	Всего операций	1239
4	Всего контр операций	70
5	Уникальные страны-источники	27
6	Уникальные страны-жертвы	160
7	Уникальные секторы жертв	42
8	Уникальные инструменты	1327
9	Всего псевдонимов инструментов	1966
10	Уникальные внешние ссылки	4868

*Источник:* архивные данные с сайта Thailand Computer Emergency Response Team (ThaiCERT), <https://www.thaicert.or.th>

Общие статистические данные представим в двух разрезах – все страны-источники и страны-жертвы, которые представлены в следующих таблицах.

Таблица 18. Все страны-источники угроз

№ п/п	Страна	Количество АРТ-групп
1	Китай	106
2	РФ	42
3	Иран	31
4	КНДР	8
5	США	7
6	Индия	4
7	Турция	4
8	Украина	3
9	Ливан	3
10	Пакистан	3
11	Сирия	3
12	Южная Корея	2
13	Тунис	1
14	Вьетнам	1
15	Румыния	1
16	Великобритания	1

№ п/п	Страна	Количество АРТ-групп
17	Мексика	1
18	Ливия	1
19	Израиль	1
20	Бразилия	1
21	Узбекистан	1
22	Франция	1
23	ОАЭ	1
24	Беларусь	1
25	Казахстан	1
26	Италия	1
27	Саудовская Аравия	1

*Источник:* архивные данные с сайта Thailand Computer Emergency Response Team (ThaiCERT), <https://www.thaicert.or.th>

Явным лидером выступает Китай (106 групп), с большим отрывом на втором и третьем местах отстают Россия (42 группы) и Иран (31 группа). Впервые в практике названы и присутствуют группы из США (7 групп) и Израиля (1 группа).

Таблица 19. 27 ведущих стран-жертв

№ п/п	Страна-жертва	Количество случаев
1	США	126
2	Великобритания	85
3	Россия	72
4	Германия	65
5	Индия	63
6	Китай	55
7	Южная Корея	52
8	Канада	50
9	Япония	49
10	Франция	44
11	Турция	44
12	Таиланд	41
13	Саудовская Аравия	40
14	Австралия	38
15	Тайвань	38
16	Украина	38
17	Пакистан	36
18	Израиль	35
19	ОАЭ	35
20	Иран	33
21	Гонконг	32
22	Малайзия	32
23	Италия	31

№ п/п	Страна-жертва	Количество случаев
24	Бразилия	30
25	Филиппины	30
26	Вьетнам	29
27	Швейцария	28

*Источник:* архивные данные с сайта Thailand Computer Emergency Response Team (ThaiCERT), <https://www.thaicert.or.th>

Распределение стран-жертв по континентам явно неравномерное – на Америку приходится только 3 страны-жертвы (11,1 %), на Европу – 8 (29,6 %), на Азиатский континент – 15 (55,6 %), Австралия и Новая Зеландия – 1(3,7 %).

Данные о наиболее пострадавших секторах экономики приведены в следующей таблице.

Таблица 20. Наиболее пострадавшие сектора

№ п/п	Наименование пострадавшего сектора	Количество
1	Правительство	136
2	Оборона	85
3	Финансы	73
4	Энергетика	59
5	Телекоммуникации	55
6	Средства массовой информации	52
7	Образование	41
8	Здравоохранение	37
9	Промышленность	34
10	Высокие технологии	31

*Источник:* архивные данные с сайта Thailand Computer Emergency Response Team (ThaiCERT), <https://www.thaicert.or.th>

Эксперты высказывают серьезные опасения по поводу роста угроз в секторе здравоохранения и эта тенденция отмечается практически во всех развитых в информационном отношении странах.

Эксперты считают нынешнее положение дел настолько сложным и серьезным, что выдвигались даже многочисленные предложения о стандартизации отчетов об атрибуции или даже создать новые международные или частные организации, задачей которых является выявление злонамеренной киберактивности. Эксперты также разработали аналитические модели, помогающие структурировать процедуры атрибуции:

- модель Diamond использует теорию графов для формальной характеристики отдельных компонентов киберинцидента и отслеживания любых изменений этих характеристик с течением времени [27];

- модель Q использует концептуальный и стратегический подход, чтобы помочь аналитикам лучше понять интрузионную активность [28].

В настоящее время разработаны и применяются два механизма киберсанкций. Это санкции Европейского союза и США. С 2017 года ЕС

внедрил комплексный набор инструментов кибердипломатии, включая автономный режим горизонтальных киберсанкций для предотвращения, сдерживания и реагирования на злонамеренное поведение в киберпространстве [29].

Приведем описание введенных киберсанкций ЕС против РФ, отраженных в [30].

Таблица 21. Введенные Европейским союзом киберсанкции против РФ

№	Дата	Подсанкционные лица	Киберсанкции	Причина введения киберсанкций
1	30.07.2020	1 российское, 1 китайское, 1 северокорейские юридические лица, 4 российских и 2 китайских физических лица	Запрещен въезд в ЕС, банковские активы в Союзе подлежат заморозке, европейскому бизнесу запрещено поддерживать финансовые связи с подсанкционными лицами	Подсанкционные лица якобы причастных к кибератакам WannaCry, NotPetya, Cloud Hopper
2	22.10.2020	2 российских физических лица, 1 российское юридическое лицо	Запрещен въезд в ЕС, банковские активы в Союзе подлежат заморозке, европейскому бизнесу запрещено поддерживать финансовые связи с подсанкционными лицами	За предполагаемое осуществление кибератаки на бундестаг в 2015 году

*Источник:* Яникеева И.О. Роль киберсанкций в международных отношениях. Вестник Дипломатической Академии МИД России. Россия и мир. 2022, 1(31), с.16. ISSN: 2410-2415

Киберсанкции, введенные США значительно отличаются от подобных киберсанкций ЕС, как по структуре, так и по количеству. Их состав приведен в следующей таблице.

Таблица 22. Введенные США киберсанкции против РФ

№	Дата	Подсанкционные лица	Киберсанкции	Причина введения киберсанкций
1	15.03.2018	19 физических лиц и 5 юридических, включая ФСБ, лиц	ОFAC* включило в блокирующий список (SDN List)**	Санкции являются частью более широких усилий США по противодействию кибератакам, якобы

№	Дата	Подсанкционные лица	Киберсанкции	Причина введения киберсанкций
				исходящим из России
2	11.06.2018	3 российских физических и 5 юридических лиц	OFAC включило в SDN List	За связь с ФСБ. Подсанкционные лица якобы напрямую способствовали улучшению киберпотенциала России, работая с ФСБ и тем самым ставя под угрозу безопасность США и их союзников
3	21.08.2018	2 российских физических и 2 юридических лица	OFAC включило в SDN List	Вторичные санкции
4	20.03.2018	6 российских физических и 2 юридических лица	OFAC включило в SDN List	За сознательное участие в деятельности, подрывающей кибербезопасность США от имени Правительства Российской Федерации
5	05.12.2019	7 российских юридических и 11 российских физических лиц	OFAC включило в SDN List	Связано с их деятельностью с хакерской группировкой «Evil Corp.»
6	10.09.2020	3 российских физических лица	OFAC включило в SDN List	Вмешательство в американские выборы. Россия якобы пыталась влиять на кандидатов в президенты США. Министерство финансов США заявило, что Москва стремится «посеять рознь между политически

№	Дата	Подсанкционные лица	Киберсанкции	Причина введения киберсанкций
				ми партиями США и вызвать внутренние разногласия с целью оказания влияния на избирателей»
7	16.09.2020	2 физических лица	OFAC включило в SDN Lis	За предполагаемые преступления в сфере кибербезопасности. Лица являются также объектами обвинительного заключения, обнародованного Министерством юстиции США
8	23.09.2020	8 российских и связанных с Россией физических и 7 юридических лиц	OFAC включило в SDN List	За предполагаемые преступления в сфере кибербезопасности, за предполагаемое вмешательство в американские выборы, а также в связи с украинским сюжетом

*Примечание:*

\*Office of Foreign Assets Control (OFAC) - Управление по контролю над иностранными активами (Управление по контролю за иностранными активами — подразделение Министерства финансов США, занимающееся вопросами финансовой разведки, планированием и применением экономических и торговых санкций в целях поддержки целей американской национальной безопасности и внешней политики). <https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information>

\*\* (SDN, Specially Designated Nationals List) OFAC публикует специальный черный список лиц, в котором перечислены люди, организации и корабли, с которыми гражданам США и постоянным жителям страны запрещено заниматься бизнесом. Источник: Яникеева И.О. Роль киберсанкций в международных отношениях. Вестник Дипломатической Академии МИД России. Россия и мир. 2022, 1(31), с.20. ISSN: 2410-2415

Следует обратить внимание на еще один факт, который характеризует деятельность системы Управления по контролю над иностранными активами Министерства финансов США (OFAC). По состоянию на 1 января 2020 г. Управление иностранных активов Министерства финансов США в одностороннем порядке ввело санкции в отношении следующих стран: Беларусь, Бурунди, Центральноафриканская Республика, Куба, Демократическая Республика Конго, Иран, Ирак, Ливан, Ливия, Мали, Никарагуа, Северная Корея, Россия, Сомали, Сербия, Судан, Южный Судан, Сирия, Венесуэла, Йемен и Зимбабве.

Хотя этот список и не является исчерпывающим, он включает самые бедные страны мира, которые не в состоянии выдержать потерю торговли и основных продуктов питания и лекарства. Во многих случаях санкции также препятствуют возможности экономической реанимации, поскольку США вводят санкции также против третьих государств, которые участвуют в торговле со странами из списка министерства финансов. При этом большинство стран, на которые США и их союзники накладывают санкции обеспечены нефтью и стратегическими полезными ископаемыми, и природными ресурсами для новых технологий и военного применения.

Нас будут интересовать перспективы будущих войн, которые представлены в [31] коллективом автором из RAND Corporation. Тенденции будущих войн представлены в следующих разрезах: геополитические тенденции, военные тенденции, космические и ядерные тенденции, кибер тенденции и тенденции сдерживания. Считаем необходимым отметить тренды и ключевые тенденции в области киберпространства, которые представлены в следующей таблице.

Таблица 23. Кибер тренды

Тренд	Кто будет сражаться	Как Соединенные Штаты будут сражаться	Где США будут сражаться	Почему Соединенные Штаты будут сражаться
1. Информационный контроль	Россия, Китай, Иран, Северная Корея и негосударственные субъекты	Информационные операции по противодействию нарративному киберпространству противника	Киберпространство	Не допустить, чтобы пропаганда влияла на общественность США и вызывала внутренние разногласия
2. Кибершпионаж	Китай, Россия и	Усилить киберзащиту; продолжать	Киберпространство	Защищать национальную безопасность



Тренд	Кто будет сражаться	Как Соединенные Штаты будут сражаться	Где США будут сражаться	Почему Соединенные Штаты будут сражаться
	негосударственные субъекты	разрабатывать более совершенные методы обнаружения кибер-вторжений	странство	США, интеллектуальную собственность, исследования и разработки
3. Киберсаботаж	Россия, Иран, Северная Корея и негосударственные акторы	Создание отказоустойчивых сетей с резервированием	Киберпространство	Защита критически важной инфраструктуры и сетей связи, предотвращение уничтожения данных

*Источник:* Raphael S. Cohen, Nathan Chandler, Shira Efron, Bryan Frederick, Eugeniu Han, Kurt Klein, Forrest E. Morgan, Ashley L. Rhoades, Howard J. Shatz, Yuliya Shokh (2020). The Future of Warfare in 2030. RAND Corporation. P.25. ISBN: 978-1-9774-0295-0

Анализ содержания таблицы свидетельствует о полном совпадении объектов по всем трем трендам, с которыми предполагают противостоять США. Это РФ, Китай, Северная Корея и Иран, а также негосударственные субъекты. Возникает комплекс вопросов – какие ответы рассматривали США в ответ на киберкомпроментацию государственных информационных систем; удалось ли США существенно повлиять на поведение противника с помощью прошлых ответов; как следует реагировать на подобные инциденты в будущем? Ответ попытаемся найти в [32].

У аналитиков есть множество вариантов ответов, которые можно сгруппировать по следующим направлениям:

- экономические: санкции против государственных служащих, отдельных субъектов, частных организаций;
- ограничения на поездки физических лиц (применяются в одностороннем порядке или в коалиции с другими странами);
- политические/дипломатические меры: демарши, изгнание иностранных правительственных чиновников;

- разведка: отслеживание сложных постоянных угроз, контрразведывательные операции, скрытые действия, раскрытие вредоносного программного обеспечения и тактики противника;
- действия правоохранительных органов: конфискация активов, демонтаж инфраструктуры по решению суда, арест и судебное преследование;
- военные: кибердемонстрация силы, оборонительные кибероперации против правительственных систем и в «сером пространстве» (например, наступательные или оборонительные ответные действия), наступательные кибероперации.

Традиционно специалисты рассматривали несколько разновидностей блокад, в том числе морские, сухопутные, а с развитием самолетостроения – воздушные, с появлением космической техники и специальных спутников – космической. С бурным развитием вычислительной техники и коммуникационных средств, появилась возможность вводить информационные блокады. Каждый вид блокады имел свои исторические особенности, они различались по затратам и, естественно, эффективности. Во второй половине и в конце 20 века ученые определили возможность введения киберблокады и ограничения в области киберпространства.

Еще не так давно человечество обладало только двумя физическими средами (доменами) – суша и море. Каждая из них имела совершенно разные физические характеристики. Море могло осваиваться людьми только с помощью специальных технологий в виде парусного судна, парохода, атомной подводной лодки. Землю можно было использовать только с помощью технических средств – колеса, плуга и т.д. Существенные перемены произошли столетие назад, когда к двум доменам была добавлена третья физическая область – авиакосмическая. С полетом первого спутника в 1957 году произошло добавление нового домена - космического пространства. Развитие отрасли по производству вычислительной и коммуникационной техники, а также создание государственных и частных информационных систем, и сетей послужило основой формирования еще одного домена – информационного.

В настоящее время к указанным доменам добавили шестой – киберпространство. Аналитики предлагают множество определений киберпространства, в том числе такое, как – условная среда, в которой оцифрованная информация передается по компьютерным сетям. Или другое определение - киберпространство (cyberspace) — глобальный домен в пределах информационной среды, состоящий из взаимозависимых инфраструктур информационных сетей с хранящимися и циркулирующими в них данными, включая Интернет, сети передачи данных, компьютерные системы и используемые в них процессоры и контроллеры [33]. Анализ ряда определений киберпространства проведен в [34]. Но автор отмечает, что со временем эта категория будет меняться и уточняться в зависимости от бурно развивающихся технических, технологических, экономических и социальных аспектов нашей жизни. В специализированной литературе категория

«киберпространство» трактуется неоднозначно и остается дискуссионной, но чаще всего содержание термина связано с деятельностью субъекта (пользователя, групп пользователей) в виртуальной пространственной модели. В числе компонентов, передающих дополнительную информацию относительно деятельности в киберпространстве, входят характеристики субъекта, места, свойства, которые выражаются такими подкатегориями, как цель, способ, инструмент, продолжительность, результат и атрибуты действия. Категория «киберпространство» тесным образом связана с терминами «кибервойна» и «киберпреступность». В категории «Кибервойна» заложено представление о неизбежности появления угрозы национальной безопасности из-за роста влияния коммуникационных технологий на жизнь общества (т.е. после «освоения киберпространства»). Именно такая логика построения модели знаний позволяет к защите рубежей на суше, на море, в воздушном и космическом пространстве присоединить концепцию национальной обороны в киберпространстве.

В отличие от физических пространств (природы, космоса, макро- и микромира) киберпространство является продуктом и средой человеческой деятельности и не может существовать в отрыве от деятельного или воспринимающего субъекта. Другими определениями выступают:

1. Электронная (включая фотоэлектронные и пр.) среда, в (посредством) которой информация создается, передается, принимается, хранится, обрабатывается и уничтожается [35].
2. Глобальная область информационного пространства, представляющая собой взаимосвязанную сеть инфраструктур информационных систем, включающих Интернет, телекоммуникационные сети, компьютерные системы, встроенные процессоры и контроллеры [36].
3. Комплексная (сложная) среда, позволяющая осуществлять взаимодействие между людьми, программным обеспечением и службами, используя глобально распределённые устройства и сети информационных и коммуникационных технологий [37].
4. Программное обеспечение, которое работает в компьютерных устройствах, информация, которая сохраняется (и передается) в этих устройствах, или информация, которая создается этими устройствами. Оборудование и здания, в которых расположены эти устройства, также являются частью киберпространства [38].

Более точное определение киберпространства приведено в [39]. Киберпространство — искусственная неоднородная технологическая система с множеством разноуровневых органов оперативного и технологического управления, процесс создания и эксплуатации которой не предопределяется требованиями одной системы управления, а функционирует

в интересах множества разнородных, в том числе антагонистических систем управления. При этом свойства зависят как от характеристик собственных элементов, так и от объема и свойств реализуемых процессов в интересах внутренних и внешних потребителей.

Естественно, что нас будет интересовать действия, связанные с реализацией блокады в последнем домене – киберблокада. Киберблокада представляет собой специально созданную ситуацию, вызванную атакой на кибеинфраструктуру или информационные системы, что препятствует доступу государства к киберпространству, предотвращая передачу данных за пределы географических границ.

Следует обратить внимание на существенное отличие киберблокады от цензуры или других форм внутреннего контроля, которые имеют место в практике управления государством. В данном случае правительство не позволяет получать или передавать определенную информацию, как правило, из соображений внутренней стабильности. Киберблокада должна быть эффективной для предотвращения передачи информации, продолжительность блокады является второстепенным фактором, который имеет значение только с точки зрения создания и достижения желаемого эффекта. Например, блокада, которая длится всего несколько долей секунды, будет иметь относительно малое значение, но блокада в критическое время (день выборов, к примеру) или продолжающаяся в течение нескольких недель или месяцев может считаться весьма эффективной в зависимости от целей. Как и в случае с морской блокадой, поддержание киберблокады в течение определенного, заранее установленного периода времени не является обязательным. Важным является конечная эффективность блокады в достижении поставленных целей.

В следующей таблице приведены данные, характеризующие операции по блокаде в следующих доменах: морской, воздушный, сухопутный, космический, информационный и киберпространство.

Таблица 24. Сходства между операциями по блокаде в шести разных доменах

	Морской	Воздушный	Сухопутный	Космический	Информационный	Киберпространство
Действия	предотвратить вход/выход кораблей или плавсредств из портов или гаваней	предотвратить вход самолета в воздушное пространство или беспилотную зону	запретить въезд или выезд из определенного города или региона	предотвратить выход в открытый космос	предотвратить передачу информации за пределы национальных границ	предотвратить передачу данных за пределы национальных границ
Актеры	государства, независимые территории	государства, независимые территории	государства	государства	государства	государства, негосударственные субъекты,

	Морской	Воздушн ый	Сухопутн ый	Космичес кий	Информа ционный	Киберпрос транство
						индивиду алы
Возмо жности	превосхо дные морские возможн ости; знание домена и уязвимо сти оппонен тов	превосхо дные воздушн ые возможн ости; знание домена и уязвимо сти оппонен тов	превосход ные наземные возможн ости; знание домена и уязвимость и оппонент ов	превосход ные технологи ческие или экономич еские возможн ости; знание домена и уязвимость и оппонент ов	историчес ки, возможно сти морского базирован ия для создания помех кабелям, знание домена и уязвимость и оппонент ов	технологи ческие возможнос ти; знание домена и уязвимость и оппоненто в
Наличи е конфли кта	война или существ ующий конф ликт	война или существ ующий конф ликт	война	война или существ ующий конфликт	война	война или существ ующий конфликт
Роль нейтра лов	защищен ные права	защищен ные права	защищенн ые права	защищенн ые права	защищенн ые права	нейтральн ые не преследую тся конкрет но, но последств ия трудно предска зать

*Источник:* Russell Alison Lawlor (2014). Cyber blockades. Georgetown University Press. ISBN 978-1-62616-113-9, p.81, 184.

Считаем необходимым привести комплекс выводов, сделанных по результатам анализа категории киберблокада в [40,с172-179].

Вывод 1. Киберблокада – это ситуация, вызванная атакой на киберинфраструктуру или системы, препятствующие доступу госструктур к киберпространству, тем самым предотвращая передачу (вход-выход) данных за пределами географических границ. Киберблокада является законным инструментом международного государственного управления и, в

соответствии с другими типами блокады, может считаться актом войны (хотя в конечном счете государство-мишень решает, хочет ли оно рассматривать ее как акт войны и потенциально обострить ситуацию). Киберблокада нацелена на государства целиком и пытается вызвать массовые сбои в работе элементов критической инфраструктуры. Целью киберблокад является предотвращение передачи данных за пределы географических границ посредством манипулирования, контроля или доминирования в киберпространстве и связанных с ним технологиях с целью нанесения политического, экономического, социального или психологического вреда противнику.

Киберпространство — это физическая сеть, которой можно манипулировать, чтобы наказать злоумышленников, препятствуя их доступу к потоку данных, необходимому для безопасности и процветания, а киберблокировки — эффективное средство отказа или затруднения доступа к киберпространству.

Вывод 2. Субъекты используют киберблокаду как инструмент международных отношений и санкций, потому что они являются эффективным и недорогим методом контроля доступа противника к современным сетям и могут осуществляться таким образом, чтобы повысить анонимность преступника или правдоподобное отрицание, тем самым снижая риск возмездия. Кроме того, существует несколько альтернативных вариантов действий для достижения того же результата, особенно для негосударственных акторов.

Вывод 3. Государства, прокси-группы, негосударственные субъекты или отдельные лица могут проводить киберблокады, если у них есть возможности. Однако группы, не спонсируемые государством, также могут ввести киберблокаду, если они обладают надлежащими техническими навыками для планирования и координации масштабной кибератаки, направленной на все государство. Физические атаки на киберинфраструктуру требуют мало ресурсов и небольшой опыт; как минимум, злоумышленники должны иметь возможность обнаруживать и уничтожать ключевую киберинфраструктуру. Электромагнитные атаки относятся к области государственной войны и требуют значительно больше ресурсов для достижения. Таким образом, в зависимости от того, как создается киберблокада (посредством цифровых, физических или электромагнитных атак), порог возможности проведения кибератаки может варьироваться от достаточно низкого (физическое уничтожение кабелей или терминалов) до высокого (электромагнитные атаки).

Вывод 4. Киберблокады могут затронуть все аспекты технологий киберпространства, включая электрические сети, электростанции, услуги обычной телефонной связи и услуги мобильной связи, среди прочего. Киберблокады, как и другие блокады, по своей сути ненасильственны, но они могут привести к повреждению, разрушению или смерти, в зависимости от того, как они реализуются и их воздействия на цели. Цели, классифицируемые

как «ограниченные» в соответствии с международным правом, такие как больницы, по-прежнему будут ограничены в киберпространстве.

Вывод 5. Киберблокады можно создавать с помощью механических, электромагнитных или цифровых атак. Физические атаки являются жизнеспособной альтернативой цифровым атакам и представляют собой акт насилия в соответствии с международным правом, поскольку наносят ущерб физической инфраструктуре киберпространства. Электромагнитные атаки возможны, но менее вероятны, поскольку требуют больших ресурсов; тем не менее, они остаются эффективным способом осуществления киберблокировки.

Вывод 6. Как грубые инструменты ведения войны, киберблокады очень эффективны для достижения конкретных результатов, но они не всегда могут быть предпочтительным инструментом для субъектов. В определенных ситуациях лица, принимающие решения, могут отдавать предпочтение более специализированным типам кибератак, которые являются очень изощренными и точными и могут достигать таких результатов, как шпионаж или уничтожение целевой системы при сохранении целостности других систем.

Вывод 7. Киберблокады могут быть установлены относительно быстро и за низкую стоимость, в зависимости от используемого метода атаки. Скорость и стоимость варьируются в зависимости от различных типов киберблокады (например, электромагнитная блокада требует больше ресурсов, чем физическая блокада), но в целом дает злоумышленнику преимущества высокоскоростного и относительно недорогого варианта.

Вывод 8. Киберблокады технически осуществимы против любой страны, но их легче достичь против географически меньших стран. Более крупные страны обычно имеют больше соединений с киберпространством, создавая более устойчивую сеть соединений между этой страной и другими странами. Таким образом, было бы сложнее ввести киберблокаду в отношении более крупной страны с хорошими связями, чем в отношении небольшой страны с меньшим количеством внешних киберподключений и потенциально менее устойчивой системой.

Вывод 9. Киберблокады можно рассматривать как подмножество информационной блокады, потому что они нацелены на передачу информации. Однако информационные блокады не получили широкого признания, поэтому эта классификация может быть не самой полезной для политиков. Помимо того, что киберблокады являются подгруппой информационных блокад, их также следует рассматривать отдельно, поскольку они происходят в определенной области и, таким образом, могут быть полезны при сравнении между областями. Таким образом, киберблокады являются одновременно доменными блокадами киберпространства и подмножеством информационных блокад.

Вывод 10. Киберблокады могут быть, но не всегда должны считаться актами войны. Контекст имеет ключевое значение: в зависимости от

обстоятельств киберблокада может считаться полной блокадой. Эволюция блокад в других областях показывает, что, хотя большинство блокад считались актами войны между воюющими сторонами, полные блокады не являются актами войны. Это следствие остается актуальным для киберпространства. Объявление войны по своей сути является политическим решением, мотивированным различными факторами. Поскольку киберблокировки нарушают государственный суверенитет, торговлю, связи, военные операции и другие действия, они могут по праву считаться актом войны, независимо от причиняемых ими физических разрушений. Однако мирная блокада является формой принудительной дипломатии, когда блокирующее государство заявляет, что оно не стремится спровоцировать войну, а скорее заставить блокадное государство уступить предъявляемым к нему требованиям. Весьма вероятно, что в какой-то момент в ближайшем будущем международное сообщество попытается ввести киберблокаду в качестве формы санкций против государств, нарушающих международное право.

Вывод 11. Киберблокады и киберзапретные зоны — это два различных вида операций. Киберблокады — это операции, препятствующие доступу, тогда как киберзапретные зоны — это операции по запрету доступа. Оба применимы к международной политике и праву, но это не одно и то же.

Вывод 12. Увеличение количества и типов акторов в киберпространстве представляет сложную ситуацию для атрибуции и делает возможным анонимность или правдоподобное отрицание на беспрецедентном уровне в кибервойне. Хотя это верно для всех аспектов киберпространства и усилий по кибербезопасности, это особенно актуально для блокад, поскольку их потенциальное воздействие очень серьезно. Государства не могут полагаться на традиционную модель сдерживания киберблокад, потому что они могут быть не в состоянии идентифицировать преступников, поэтому они должны больше сосредоточиться на разработке надежных, избыточных и устойчивых систем, способных противостоять или быстро восстанавливаться после киберблокады.

Вывод 13. Государственно-частные партнерства имеют особое значение для киберблокировки, потому что область киберпространства не является чисто общественным благом — она принадлежит и управляется в основном частными корпорациями или отдельными лицами, однако правительствам поручено защищать ее как часть критической национальной инфраструктуры. Предыдущие типы блокад в разной степени затрагивали частный сектор (например, торговые суда, коммерческие самолеты или даже телеграфные кабели), но киберблокировки представляют собой первый случай, когда общественные и частные интересы переплелись до такой степени.

Вывод 14. По мере изменения топологии киберпространства и акторов изменить свои возможности, уязвимости, связанные с киберблокадой тоже меняются. Технический прогресс уменьшит уязвимости в некоторых областях,



в то время как изменения в самом киберпространстве, скорее всего, обнаружат новые уязвимости, которыми воспользуются злоумышленники.

Алисон Рассел в заключении своей книги предлагает комплекс важных рекомендации. Условно их можно разделить на две категории: политические и научные. Во многих отношениях усилия политического сообщества и ученых могут частично совпадать, что может быть полезно для продвижения исследований в области киберблокад, но в целях лучшей организации эти рекомендации представлены отдельно.

**Первый комплекс рекомендаций** разработан для академического сообщества.

Поскольку академическое сообщество продолжает свои исследования в области киберпространства и кибербезопасности, важно, чтобы оно разработало общую терминологию для обсуждения событий и явлений в киберпространстве. В настоящее время научная литература разнится в определениях самых основных терминов, таких как киберпространство, кибератаки, кибервойна и применение силы. В некоторых областях начинает появляться консенсус, но важно, чтобы научное сообщество разработало согласованный комплекс терминов для обозначения всех аспектов и событий в киберпространстве.

Исследователи должны проявлять бдительность и осторожность при уточнении и определении того, как исторический опыт может подходить или не подходить для понимания киберпространства и обеспечения его безопасности. Это исследование в значительной степени опиралось на историческую эволюцию блокад и запретных зон в других областях, для определения блокады в киберпространстве и выявления общих черт в разных областях. Однако исторический опыт и междоменные сравнения не всегда идеально подходят для киберблокировок, и в оценке любых новых разработок, нужно знать, что существуют дополнительные факторы или инновации, которые не могут быть рассмотрены через историческую парадигму. Для анализа и оценки категории «киберблокада», необходима информация о большом количестве субъектов на разных уровнях анализа, роли анонимности, скорости кибератаки и стоимости киберблокировки — все это представляет собой значительное отклонение от прошлого опыта; их уникальность и важность необходимо учитывать, но не преувеличивать.

Таким образом, очень важно достигнуть точной балансировки уникальных атрибутов киберпространства с междисциплинарными теоретическими приложениями или историческим опытом, для понимания комплекса проблем в этой конкретной области. История и исторический экскурс могут многое предложить для постановки новых задач, но в погоне за пониманием нельзя ни забывать, ни преувеличивать уникальность области и ее атрибутов.

По мере достижения консенсуса в отношении терминологии киберпространства для научного сообщества также важно разрабатывать новые теории или модифицировать существующие теории для объяснения и

прогнозирования событий в киберпространстве. Теории международных отношений полезны для прояснения ключевых элементов киберпространства, но всесторонний подход к разработке теории был бы нецелесообразен для решения всех аспектов домена. Комплексный подход позволил бы «отобразить» аспекты предметной области для будущих исследований и выделить связи с существующими научными исследованиями.

**Второй комплекс рекомендаций** ориентирован на политическое сообщество в виде трех рекомендаций. Первая рекомендация заключается в том, чтобы политики и государственные чиновники осуществляли планирование сценариев, при которых доступ к киберпространству будет запрещен в течение значительного периода времени. Отказ в доступе может быть результатом несчастного случая или результатом преднамеренной атаки на критическую инфраструктуру страны. Хотя ситуация, приведшая к массовому отказу в доступе, может быть маловероятной, но это будет серьезное, трудно предсказуемое и редкое событие — к которому подходит определение события «черный лебедь» («Чёрный лебедь» — теория, рассматривающая труднопрогнозируемые и редкие события, которые имеют значительные последствия). Учитывая зависимость общества и правительства от действий в киберпространстве для повседневной деятельности, и эти действия настолько обыденны и рутинны, что их часто игнорируют или упускают из виду. Поэтому очень трудно оправдать отсутствие процессов противостояния кризису, в условиях, когда доступ к киберпространству подвергается атакам.

Данная двусмысленность порождает некоторые трудности во время конфликтов, поскольку акторы не имеют четких границ и общих определений применения силы в киберпространстве. В результате этого, лица, принимающие решения в данной области, могут по-разному относиться к «красным линиям» при нападении, что может привести к непреднамеренной эскалации конфликта.

Во-вторых, для общего понимания конфликта решающее значение имеет использование международных норм относительно приемлемого поведения и применения силы. Эксперты высказывают мнение об отсутствии консенсуса относительно рамок допустимого использования киберпространства или кибертехнологий. Данный вопрос постоянно дискутируется на уровне международных и межправительственных организаций, но достигнуть консенсуса в отношении того, как должно и как не должно использоваться киберпространство государствами и негосударственными субъектами не достигнуто [41]. Эта двусмысленность порождает трудности во время конфликтов,

Все большую поддержку получает тезис о том, что киберблокада является инструментом управления государством. Она соответствует историческому опыту блокадных операций на море, в воздухе и на суше, а также международному праву о блокадных операциях. Учитывая исторические и юридические прецеденты, есть все основания считать

киберблокаду частью логической эволюции военных действий в новом домене. Высказывается мнение, что в качестве законного инструмента международных отношений только государства будут иметь право применять блокады. Необходима разработка правил атрибуции, но с учетом того, что они не являются строго обязательными по аналогии с действиями подводных лодок. Кроме того, негосударственные субъекты не могут заниматься киберблокадами, так же как они не могут на законных основаниях проводить морскую, воздушную или наземную блокады. Кроме того, в соответствии с традиционным пониманием блокадных операций как комплекс военных действий, киберблокады могут быть признаны военными действиями. Соответствующие усилия по достижению внутреннего и международного консенсуса в отношении надлежащего использования киберпространства позволят создать правовые основы для сотрудничества. Необходимо исследовать вопрос о том, какие действия в киберпространстве представляют собой «применение силы» или «вооруженное нападение» для установления «красных линий» до начала конфликта и предотвратить непреднамеренную эскалацию. Подобные усилия должны касаться также активной и пассивной защиты и ответных мер для государства, ставшего жертвой кибератаки.

В-третьих, важной областью является частно-государственное партнёрство. В некоторых, в экономически развитых странах, частный сектор владеет и управляет более чем 80% критической инфраструктуры и технологиями киберпространства, но правительство играет ведущую роль в защите инфраструктуры. Это объясняется тем, что случае киберблокады против конкретной страны будут затронуты как национальная безопасность, так и коммерческие интересы. Никому не выгодно иметь критическую инфраструктуру и кибертехнологии, для которых не хватает безопасности и надежности и безопасность домена может быть поставлена под угрозу из-за обременительных требований безопасности.

В любом случае, государственный и частный секторы проиграют в случае, если киберпространство не будет защищено должным образом. Поэтому бремя затрат и ответственности должно быть разделено между субъектами из двух секторов. Правительство обязано защищать собственную критическую инфраструктуру в виде сетей и систем, а также санкционировать, регулировать и применять меры для стимуляции частного сектора вкладывать средства в безопасность коммерческих систем.

Следует иметь в виду, что блокады не являются историческими событиями прошлого (например, морские блокады), они являются явлениями современными и будут происходить до тех пор, пока будут оставаться эффективным средством воздействия и кибероружием. В связи с этим, государствам необходимы разработки по планированию защиты от киберблокировок и планов восстановления после их реализации, необходимо разработать стратегии ответов на кибернападение.

Впереди огромные объемы теоретических исследований и практических разработок по интеграции знаний в теорию киберпространства с другими

теориями о власти, коммуникациях, информационном обществе и роли информации в наступившем тысячелетии. Развитие и распространение негосударственных акторов требует рассмотрения множества вопросов о роли частных лиц и правах государства в будущих конфликтах. Негосударственные субъекты играют все большую роль в международной политике, поэтому возникает законный вопрос о необходимости модификации соответствующих законов о вооруженных конфликтах и возможности, и ответственности, за перенос действий в киберпространство.

Следует обратить внимание на разновидность блокады – киберблокаду [40, 42]. В условиях развития информационного общества, сети и системы играют решающую роль в развитии цифровизации общества и самым серьезным образом могут быть труднопреодолимым фактором и вызовом.

Кибератакам и кибервойне уделяют значительное внимание при анализе развития общества и бизнеса из-за угрозы, которую они представляют. Кибератаки осуществляются регулярно – против государственных учреждений, военного ведомства и частного бизнеса. Постоянно растущая зависимость стран от развития киберпространства может сыграть отрицательную роль в процессе противостояния, противник может атаковать те области, в которых киберпространство является решающим элементом.

Киберблокада – это следствие или результат кибератак, которые могут быть реализованы различными средствами и разными субъектами. Для их оценки следует использовать подход к категоризации и классификации кибернетических атак. Классификация кибератак по полученному эффекту обеспечивает три основные категории: кража, отказ и уничтожение. Данный подход упрощает анализ исходной точки атаки, характеристик преступника, его местонахождения, используемого метода и т.д.

Кибер-кража представляет собой незаконный и несанкционированный захват информации (в том числе включая интеллектуальную собственность), которая принадлежит физическим лицам, коммерческим или государственным структурам. Данная категория охватывает информацию начиная от кражи персональных данных, взлома корпоративных сетей для получения коммерческой тайны, до государственного шпионажа. Все эти деяния считаются кражей, поскольку связаны с несанкционированным доступом к информации. Атаки типа «отказ в обслуживании» блокируют доступ к информации, находящейся в киберпространстве. Эти атаки направлены на отказ в доступе к финансовой информации, банковским системам, СМИ, а также правительственным сообщениям. Реализация подобных атак относительно проста в исполнении, но может иметь масштабные последствия. Уничтожение – это несанкционированное искажение или уничтожение информации. Данная категория охватывает уничтожение персональной, корпоративной или государственной информации и варьируется от порчи корпоративных вебсайтов, кибератак с политическими лозунгами, а также атак, с помощью которых можно разрушить физическую инфраструктуру.

Следует отметить, что атаки в киберпространстве могут носить тактический или стратегический характер. Исследования в области информационной безопасности сосредоточены, в основном, на тактических угрозах – атаки на отдельных лиц или небольшие группы, деятельность хакеров и корпоративный или государственный шпионаж. В тоже время киберпространство является основой для реализации стратегических атак. Страны, способные контролировать (мониторить) чужое киберпространство, способны нанести серьезный ущерб экономике, военной мобилизации, общественным организациям и политическим движениям. Примерами могут служить деятельность таких стран, как Иран, Бирма, Египет, Сирия и др. в период внутренних потрясений с серьезными последствиями. В частности, по данным ОЭСР и другим источникам, экономика Египта теряла около 18 млн дол. в день, а общие потери составили 90 млн. дол. за пять дней, так называемой «Египетской весны» [43,44]. Данный пример свидетельствует о том, что киберпространство отдельной страны или региона можно «выключить» и сделать его недоступным. Это является серьезной проблемой для тех, кто в своей работе полагается на киберпространство для основных видов научной и хозяйственной деятельности.

Представляется необходимым рассмотреть типы кибератак, которые являются основой киберблокады. Необходимо также рассматривать и анализировать существующие киберблокады. Анализ должен начинаться с рассмотрения характеристик блокадных операций, в их числе такие, как выполненные действия, действующие лица (акторы) и их возможности, обстановка, предшествующая началу конфликта, поведение нейтральных соседей и т.д. Во внимание должны быть приняты факторы, способствующие проведению блокады – уязвимости, предполагаемые результаты блокады и альтернативные варианты действий.

Блокады возникают в разных средах и по разным причинам. Кроме того, эти действия не всегда называют «блокадами». Необходим полный анализ спектра выполненных блокировок по всем областям, прежде чем анализировать операции по киберблокаде или киберблокировке. Необходимо иметь в виду, что существующие блокады не являются статичными, они постоянно эволюционируют во времени с постоянным расширением спектра воздействий, которые отличаются физическими особенностями и операционными процедурами. И самое главное, применительно ко всем областям, а это – земля, море, воздух, космос и киберпространство, организация и проведение блокад является сильнейшим оружием, которое подвластно только лидерам информационного пространства.

### **Показатели оценки киберконфликта**

История взаимоотношений между народами и странами, их объединениями насчитывает несколько тысяч лет. Взаимоотношения могут последовательно находиться в нескольких стадиях. В их числе такие, как сотрудничество, интеграция, соревнование и противостояние (рис.2).

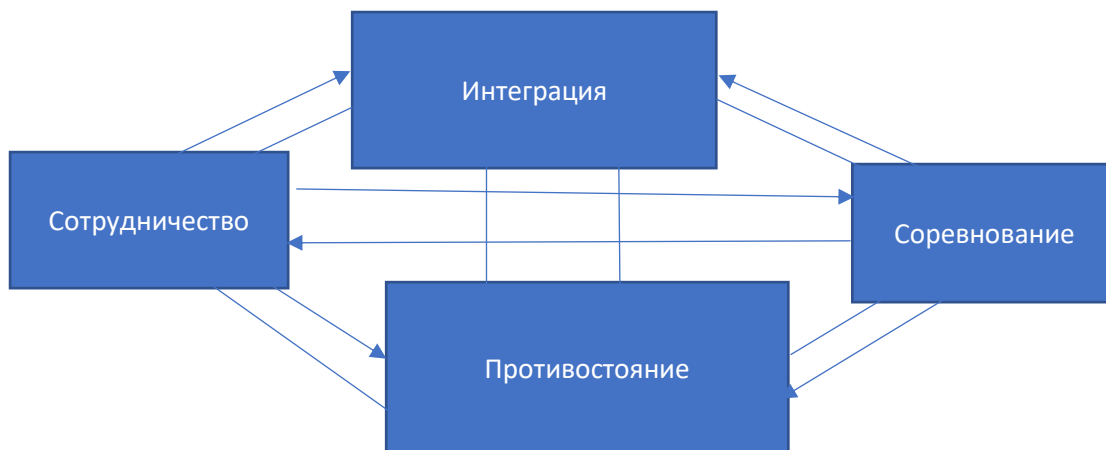


Рис.2. Модель ЖЦ взаимоотношений систем

Следует отметить, что перечисленные стадии объединяют множество областей – политическую, военную, экономическую, технологическую, социальную и идеологическую. Взаимодействие и противостояние осуществляются на разных уровнях – глобальном, стратегическом, тактическом и индивидуальном. В настоящем разделе основное внимание уделено стадии противостояния в относительно новой, недостаточно исследованной сфере деятельности – киберпространстве.

Важность данной темы определяется стремлением каждого государства обеспечить защиту национальных интересов с точки зрения кибербезопасности [45]. Важным замечанием является утверждение, приведенное в [46], отличие домена киберпространства от других доменов. Во-первых, киберпространство создано руками человека. Во-вторых, военные и гражданские (дипломатические, торговые и т.д.) возможности в других доменах управляют с помощью и через кибердомен. В-третьих, военные и гражданские аспекты киберопераций трудно, а иногда и невозможно отличить, поскольку они переплетаются. В-четвертых, очень трудно установить атрибуцию операций в киберпространстве.

Еще одной характерной чертой является отсутствие таких показателей (или единиц измерения) как масса, гравитация, трение или расстояние. Кроме того, получили распространение следующие утверждения: киберпространство – это абстрактное пространство; киберпространство не имеет естественных границ; киберпространство может иметь любое количество подпространств (например, Интернет, телефонная система, система радиосвязи); киберпространство не ограничено в ряде своих измерений (например, Интернет имеет IP-адрес, MAC-адрес, номер порта и т.д.); каждое измерение киберпространства не имеет ограничений; каждый киберобъект имеет свои координаты; один киберобъект может принадлежать более чем одному подпространству; объекты киберпространства могут взаимодействовать с объектами в физическом пространстве [47].

В рамках существующего киберпространства многие авторы сходятся во мнении, что возможность активного присутствия в этом домене зависит от множества политических, экономических и социальных факторов. Деление на определенные представительные группы обуславливает возможность отдельного государства разрабатывать механизмы реагирования на киберугрозы, поощрять инвестиции в исследования и разработку процессов цифровой трансформации, принятие законов по защите данных, созданию компьютерных групп реагирования на чрезвычайные ситуации (CSIRTs), наращивание киберпотенциала (ССВ), противостоять кибератакам и т.д.

Приведенные факторы позволяют выделить несколько групп: группа стран «Глобального Севера» и «Глобального Юга», небольшая группа «крупных игроков» в составе США, Китая и России, небольшая группа стран (Китай, Россия, Иран, Северная Корея), чья экономическая деятельность находится под постоянной критикой. Данные различия между крупными игроками и развивающимися странами определяются за счет экономической нестабильности, высоким уровнем безработицы и низкой заработной платой. Последнее обстоятельство побуждает их жителей заниматься киберпреступной деятельностью.

### **Модели, показатели и индикаторы**

Аналитики в качестве основных механизмов используют две модели, которые широко используются для измерения кибернетического потенциала стран, а именно: the Oxford Cybersecurity Capacity Maturity Model (CMM) and the International Telecommunications Union Global Cybersecurity Index (ITU GCI). Оба механизма выполняют важную роль для оценки ранжирования и оценки по группам показателей. Это позволяет выявить существующие пробелы, сильные и слабые стороны.

Oxford Cybersecurity Capacity Maturity Model представляет собой методологическую основу, предназначенную для анализа потенциала кибербезопасности страны. Данная модель постоянно развивалась с помощью фокус-групп, тематического кодирования, консультаций экспертов. Данная модель получила развитие в более 87 стран.

Таблица 25. Параметры для измерения наращивания киберпотенциала: Оксфордская модель зрелости потенциала кибербезопасности

Параметры	Описание
Политика и стратегия	Изучает потенциал страны для разработки и реализации стратегии кибербезопасности, а также для повышения ее устойчивости к кибербезопасности за счет улучшения реагирования на инциденты, киберзащиты и защиты критической инфраструктуры (КИ).
Культурный	Рассматривает важные элементы культуры ответственной кибербезопасности, такие как понимание связанных с кибербезопасностью рисков в обществе, уровень доверия к интернет-сервисам, услугам электронного правительства

Параметры	Описание
	и электронной коммерции, а также понимание пользователями защиты личной информации в Интернете.
Наращивание потенциала	Проверяет наличие, качество и использование программ для различных групп заинтересованных сторон, включая правительство, частный сектор и население в целом, и относится к программам повышения осведомленности о кибербезопасности, формальным образовательные программы и программы профессионального обучения.
Правовые рамки	Изучает способность правительства разрабатывать и принимать национальное законодательство, которое непосредственно и косвенно относится к кибербезопасности, с особым акцентом на темы нормативных требований к кибербезопасности, законодательства о киберпреступности и связанных с ним законодательство.
Стандартизация и технологии	Изучает внедрение стандартов и передовой практики кибербезопасности, развертывание процессов и средств контроля, а также разработку технологий и продуктов для снижения рисков кибербезопасности.

*Source:* Louise Marie Hurel (2022) Interrogating the Cybersecurity Development Agenda: A Critical Reflection, *The International Spectator*, 57:3, 66-84, DOI: 10.1080/03932729.2022.2095824

За прошедшие годы было разработано несколько индексов кибербезопасности. Индексы для отдельных стран включают следующие:

1. Киберзрелость в Азиатско-Тихоокеанском регионе, разработанная Австралийским институтом стратегической политики (<https://www.aspi.org.au/report/cyber-maturity-asia-pacific-region-2017>);
2. Национальный индекс кибербезопасности, разработанный Эстонской академией электронного управления (<https://ega.ee/project/national-cyber-security-index/>);
3. Глобальный индекс кибербезопасности, разработанный Международным союзом электросвязи (МСЭ) (<https://www.itu.int>);
4. Индекс кибербезопасности «Лаборатории Касперского» ([https://www.kaspersky.com/about/press-releases/2016\\_21-29-60-kaspersky-lab-presents-the-first-cybersecurity-index](https://www.kaspersky.com/about/press-releases/2016_21-29-60-kaspersky-lab-presents-the-first-cybersecurity-index));
5. Азиатско-тихоокеанская информационная панель кибербезопасности, разработанная Business Software Alliance (BSA) (<https://www.bsa.org/news-events/news/new-bsa-study-shows-how-apac-markets-can-bolster-national-cybersecurity-strategies>);
6. Индекс киберготовности, разработанный Потомакским институтом политических исследований (который включает существующие возможности) (<https://www.potomac institute.org/academic-centers/cyber-readiness-index>);



7. Cyber Green Index, в котором основное внимание уделяется техническим угрозам (<https://cybergreen.net>).

Дополнительно следует отметить, что используются и другие руководства, в их числе The Cyber Resilience Index: Advancing Organizational Cyber Resilience. White Paper, July 2022 [48], Cybersecurity Capacity Maturity Model for Nations (CMM) [49], Global Cybersecurity Index [50].

Рассмотрим существующие подходы к выбору показателей и их расчетам.

Одним из самых значимых показателей оценки является **кибермощь (cyber power)**. Данный показатель, его методология расчета, представлен в National Cyber Power Index 2022, как пример целостного национального подхода [51]. В расчетах используется комплекс показателей, характеризующих такие, как накопление и защита богатства; контроль и манипулирование информационной средой; определение международных кибернорм и технических стандартов; уничтожение или отключение инфраструктуры возможного противника; данные внешней разведки для национальной безопасности; растущая национальная компетенция в области кибербезопасности и коммерческих технологий; укрепление и усиление киберзащиты; наблюдение и мониторинг домашних групп. Дополнительно используются следующие индексы: индекс грамотности и образования в области киберрисков; кадровое обеспечение кибервоинских сил; законы о конфиденциальности данных; свобода в сети; глобальный индекс мягкой силы; уровень заражения мобильных/компьютерных устройств; деятельность национального органа по стандартизации; население в Интернете; использование социальных сетей. В методологии 2022 года использовались наборы из 29 показателей. Итоговые агрегированные данные расчета NCPI за 2022 год приведены в таблице 26.

Таблица 26. 10 самых кибермощных стран

Место	Страна
1	США
2	Китай
3	Россия
4	Великобритания
5	Австралия
6	Нидерланды
7	Тайвань
8	Вьетнам
9	Франция
10	Иран

*Источник:* Julia Voo, Irfan Hemani, Daniel Cassidy (2022). National Cyber Power Index 2022. Report September 2022. p.8. [www.belfercenter.org/project/cyber-project](http://www.belfercenter.org/project/cyber-project)

Рейтинги отдельных государств учитывались по следующим направлениям: финансы, наблюдение, разведка, торговля, оборона, информационный контроль, разрушения, нормы.

Авторы отмечают, что их объективно-ориентированный анализ страдает некоторыми ограничениями, в их числе такие как, ограниченность доступных данных о кибервозможностях для отдельных государств, государства могут намеренно скрывать свои возможности в стратегических целях, отсутствие прозрачности о численности персонала, участвующего в деструктивных кибероперациях и др.

Еще одной индексированной переменной, относящейся к серии Cyber Power, выступает **уравнение индексации кибервласти** (Indexing Equation for Cyber Power) [52]. Компоненты силы включают следующие переменные: военная составляющая, правовая и нормативная база, экономический и социальный контекст, технологическая инфраструктура, промышленное применение, распределение военного бюджета, возможный спектр угроз, национальная цифровая уязвимость.

Следует отметить, что в литературе для описания киберконфликтов используют элементы теории ожидаемой полезности, с помощью которых можно описать любую политическую ситуацию и предполагаемое решение. Полезность, по Буэно де Мескита и др. [53-56], может быть оценена между +1 и -1, с 0 в качестве середины.

Процесс построения, изучения и применения модели принятия киберрешений включает использование следующих переменных: потенциальный инициатор киберконфликта и его возможности (нападающая сторона); потенциальный защитник; нации (страны), чья политика рассматривается как дружественная; нации (страны), чья политика рассматривается как недружественная; неприсоединившиеся нации (страны), чья политика рассматривается как недружественная ни по отношению к нападающей стороне, ни по отношению к защищающейся стороне, ни по отношению к другим государствам. При определении ожидаемой полезности конфликта дополнительно используют следующие переменные:

- характеристики относительной силы нападающей и защищающейся сторон;
- ценность, которую нападающая сторона придает изменению политики защищающейся стороны для проверки соответствия;
- относительная сила и предполагаемые политические интересы всех сторон.

Составные аспекты теории полезности разжигания двустороннего конфликта определяются следующим образом:

- ожидаемая полезность для развертывания двусторонних военных действий;
- полезность для собственной политики;
- полезность для политик нападающей стороны. Это выражение может варьироваться от +1 до -1;
- восприятие нападающей стороны того, что может быть получено в случае успеха в двухстороннем конфликте, в результате которого можно навязать защищающейся стороне новую политику;

- восприятие нападающей стороны того, что может быть потеряно, если она потерпит неудачу в двухстороннем конфликте, в котором защищающаяся сторона сможет навязать нападающей стороне новую политику;
- текущее восприятие нападающей стороны своей вероятности добиться успеха против противника в двухстороннем конфликте;
- текущее восприятие нападающей стороны вероятности проигрыша в двухстороннем конфликте;
- восприятие ожидаемого изменения в будущем по сравнению с текущими воспринимаемыми различиями в политике защищающейся стороны.

Лукас Кело в своей работе [57], предлагает формулу для расчета сдерживания для оценки будущего конфликта, в которой чистая выгода или затраты равны отношению суммы преимуществ и вреда, наносимого жертве, по отношению к сумме затрат и вреда, который ожидается от жертвы.

Еще одним из важных показателей оценки может выступать сводный индекс национального потенциала CINC (The Composite Index of National Capability). Это статистический показатель национальной мощи, созданный Дж. Дэвидом Сингером для журнала *Correlates of War*. Данный показатель рассчитывается как отношение статистических данных отдельной страны по отношению к общемировому уровню.

Проводится расчет соотношения по следующим показателям: соотношение общей численности населения страны; соотношение городского населения страны; соотношение производства железа и стали в стране; коэффициент потребления первичной энергии; коэффициент военных расходов; соотношение военнослужащих. Первая тройка стран-лидеров включает: Китай (оценка составляет .198566), США (.142249), Индия (.073444). Соответственно, на 5 месте РФ (.039274), 18 место занимает Украина (.011835), 49 место у Румынии (.003213), на 132 месте Молдова (.000346).

Еще одним дополнительным специфическим показателем, который предложен в [58], является воспринимаемая кибермощь. Данный подход характеризуется комплексом показателей, которые характеризуют:

- критическую массу, которая определяет размер и возраст населения, а также уровень их киберосведомленности. Граждане играют решающую роль в обеспечении национальной кибербезопасности и, следовательно, национальной безопасности. Поскольку они могут быть использованы в процессе разглашения конфиденциальной информации, либо как участники ботнетов или атаках на критическую информационную инфраструктуру. Здесь учитывается и количество киберэкспертов;
- экономическая составляющая, которая объединяет характеристики критической информационной инфраструктуры, критических технологий и доступ к последней. Учитывается техническая и киберподдержка и доступные киберуслуги;

- военная составляющая, которая включает использование информационных технологий в вооруженных силах и развитие киберкомандования, а также возможности киберзащиты;

- информационная составляющая, которая объединяет связь и потоки информации между системами и технологиями;

- стратегическая составляющая, включает реализацию национальной киберстратегии, предотвращения роста киберпреступности и развитие системы образования в области кибербезопасности (включая нормативно-правовую базу);

- влияние людей на ответственное использование правил кибербезопасности через осведомленность и предотвращение киберпреступности.

Элементы, критерии и альтернативы, определенные данной моделью приведены в следующей таблице.

Таблица 27. Элементы, критерии, подкритерии и альтернативы

Элементы	Критерии	Подкритерии
Критическая масса (С)	Уровни образования	<ul style="list-style-type: none"> <li>• Зачисление студентов высших учебных заведений в процентах от общего числа учащихся</li> <li>• Ожидаемые годы обучения</li> <li>• Знание английского языка</li> </ul>
	Технические навыки	<ul style="list-style-type: none"> <li>• Рост производительности труда</li> <li>• Исследователи в области исследований и разработок на миллион человек</li> <li>• Выпускники по кибербезопасности, компьютерным наукам и инженерии</li> </ul>
Экономический (Е)	Торговля	<ul style="list-style-type: none"> <li>• Экспорт информационных и коммуникационных технологий в процентах от общего объема экспорта</li> <li>• Импорт информации и связи как процент технологий от общего объема импорта</li> <li>• Открытость для торговли</li> </ul>
	Инновационная среда	<ul style="list-style-type: none"> <li>• Исследования и разработки в процентах от валового внутреннего продукта</li> <li>• Внутренние патентные заявки</li> <li>• Прямой и венчурный капитал в процентах от валового внутреннего продукта.</li> <li>• Умные сети</li> </ul>
	Электронная коммерция и управление	<ul style="list-style-type: none"> <li>• Интеллектуальный транспорт</li> <li>• Электронное здравоохранение</li> <li>• Размещение заказов через интернет (деловые и индивидуальные)</li> <li>• Финансы (интернет-банкинг и т. д.)</li> </ul>

Элементы	Критерии	Подкритерии
Военный (М)	Развитие кибервозможностей	<ul style="list-style-type: none"> <li>• Военные исследовательские центры</li> <li>• Военные учебные заведения по кибервойне</li> <li>• Кибер-поле для тренировок</li> <li>• Доступ к негосударственным субъектам</li> </ul>
	Возможности кибер- и разведывательных операций	<ul style="list-style-type: none"> <li>• Стратегия киберзащиты</li> <li>• Военные киберподразделения (Киберкомандование / Киберармия)</li> <li>• Кибероружие</li> </ul>
Информационный (I)	Доступ к информации и коммуникационным технологиям	<ul style="list-style-type: none"> <li>• Проникновение в Интернет</li> <li>• Проникновение мобильной сотовой связи</li> <li>• Точка доступа Wi-Fi на миллион человек</li> <li>• Проникновение в социальные сети</li> </ul>
	Качество информационных и коммуникационных технологий	<ul style="list-style-type: none"> <li>• Пропускная способность Интернета</li> </ul>
	Доступность информационных и коммуникационных технологий	<ul style="list-style-type: none"> <li>• Тарифы на мобильную связь</li> <li>• Тарифы на широкополосный интернет</li> <li>• Расходы на информационные технологии в процентах от ВВП.</li> </ul>
	Безопасные серверы	<ul style="list-style-type: none"> <li>• Меры защиты программного и аппаратного обеспечения</li> <li>• Регулярное тестирование уязвимостей</li> <li>• Программы устойчивости</li> </ul>

Источник: Jansen van Vuuren, J.C., Leenen, L. (2018). A Model for Measuring Perceived Cyberpower. Proceedings of the 13th International Conference on Cyber Warfare and Security, National Defence University, 8-9 March 2018, Washington D.C., pp. 320-327 ISBN 978-1-5108-5963-0 <http://hdl.handle.net/10204/10361> (дата обращения 13.05.24)

Таким образом, воспринимаемая киберсила (кибермощь, кибервласть) определяется следующим образом:

$$\text{Киберсила} = (C + E + M + I) * (S + W) + \text{Взаимосвязи}(C, E, M, I),$$

где:

C - критическая масса, которая включает в себя размер и возраст населения, а также уровень кибернетической осведомленности населения. Сюда также входят различия в кибер-осведомленности географически распределенного населения. Граждане играют критически важную роль в обеспечении

кибербезопасности, поскольку они могут быть использованы в качестве носителя конфиденциальной информации или стать частью бот-нета или кибератаки. Существенное влияние оказывает количество киберэкспертов.

E - экономический элемент, который включает критическую киберинфраструктуру, технологии, техническую и киберподдержку;

M – военный элемент, включающий использование кибертехнологий в составе вооруженных сил и создание киберкомандования или аналогичных структур;

I – информационный элемент, характеризующий коммуникацию и технологии доступа;

S – стратегия, которая включает реализацию национальной киберстратегии, предотвращение киберпреступлений с обеспечением правовой и нормативной базы;

W – влияние на людей с целью ответственного использования киберпространства и предотвращения киберпреступлений.

В условиях всеобщей цифровизации невозможно не упомянуть проблемы кибернетических атак и противостояния. На фоне введения комплекса санкций противостояние между странами не закончилось. Наоборот, усилия противоборствующих сторон совершенствуются как в качественном отношении, так и увеличиваются повсеместно.

Логика и темпы развития процессов цифровизации позволяют обоснованно предполагать, что интерес к противоправной деятельности в данной сфере будет стремительно возрастать. Причем рост отмечается как со стороны государственных органов управления, так и представителей криминального бизнеса. Их развитие, по мнению авторов, будет развиваться на базе комплекса бизнес-моделей. Рассмотрим кратко их состав и описание, опираясь на [59-61]:

1. Упрощенная модель - (основана на прибыли) создание комплекса вредоносного ПО и обеспечение им киберпреступников (вирусы, черви, троянцы и т.д.).

2. Сборочная модель – создание для заказчика вредоносного ПО с набором заданных свойств на основе имеющихся программных и логических механизмов.

3. Киберпреступность-как-услуга (Cybercrime-as-a-Service CaaS) - это предоставление услуг другим лицам для облегчения совершения ими киберпреступлений. Эти услуги также называются "атаки как услуга", "вредоносное ПО как услуга" и "мошенничество как услуга". Это комплекс моделей разработки криминальных функций, которые киберпреступники поставляют своим клиентам (заказчикам) в обмен на оплату их услуг и продуктов. Ниже приведены некоторые распространенные примеры модели CaaS:

- программы-вымогатели как услуга (Ransomware as a service (RaaS)). Киберпреступники предлагают пакеты ransomware, которые другие лица или группы могут использовать для заражения и шифрования данных своих целей. Затем злоумышленники требуют от жертвы выкуп за расшифровку данных.

Программы-вымогатели постоянно получают свое развитие за счет разработки дополнительных функций, и они превращаются в изощренный механизм целенаправленных и успешных кибератак. Это обусловлено растущей конкуренцией в среде разработчиков, предлагающих Ramsonware-as-a-service (RaaS), а также желанием привлечь больше заказчиков для максимизации своей прибыли;

- фишинг как услуга (Phishing-as-a-Service PhaaS). Данная услуга предлагает фишинговый набор за определенную цену. Этот набор содержит инструменты и знания для проведения фишинговой атаки. Киберпреступники обладают доступом к уже готовым фишинговым страницам, фишинговым сообщениям, списку потенциальных жертв и т.д. Киберпреступники предлагают удобный пользовательский интерфейс для создания и управления фишинговыми кампаниями, понятный даже для людей, не обладающих техническими знаниями. Следует отметить, что, как правило, подобные сервисы предоставляют готовые шаблоны фишинговых действий, услуги хостинга для фишинговых сайтов и инструменты для сбора персональных данных о потенциальных жертвах;

- распределенный отказ в обслуживании как услуга (Distributed Denial of Service-as-a-Service DDoSaaS). В рамках данной услуги киберзлоумышленники предоставляют набор инструментов и инфраструктуру для проведения распределенных атак типа «отказ в обслуживании» (DDoS) на веб-сайты или онлайн-сервисы, в результате чего они становятся недоступными для легитимных пользователей с вытекающими последствиями;

- ботнеты напрокат как услуга (Botnets-for-Hire). Киберпреступники могут сдавать в аренду созданные и поддерживаемые ботнеты, которые представляют собой сети взломанных компьютеров или устройств (например, промышленный интернет или интернет вещей), которые контролируются центральным лицом (ботмастером). Киберпреступники могут использовать ботнеты для реализации множества действий, в том числе таких, как рассылка спама, проведения DDoS-атак или распространения вредоносного ПО;

- кража учетных данных как услуга (Credential Theft Services (CTS). Группа киберпреступников может предлагать набор услуг по краже учетных данных (например, имен пользователей и соответствующих паролей) у частных лиц или сотрудников компаний. Другая группа киберпреступников может использовать эти учетные данные для реализации дальнейшего несанкционированного доступа или продавать их в Даркнете;

- вредоносное ПО как услуга (Malware-as-a-Service (MaaS). Киберпреступники предлагают к продаже готовые наборы вредоносного ПО или инструменты, позволяя другим пользователям совершать криминальные действия (атаки), не затрачивая сил на создание вредоносного ПО с нуля;

- преступление в качестве услуги (Crime-as-a-Service CaaS). В качестве примера можно рассмотреть следующий пример - жертва получала от кибермошенников предложение об инвестировании больших средств в

недвижимость. При заключении сделки кибермошенники предлагали установить специальное приложение для управления криптовалютами. После установки приложения мошенники, используя технические программные инструменты, брали под контроль криптовалютные кошельки жертвы. И только тогда, когда платежи производились с помощью этого приложения, жертвы понимали, что с их криптовалютных кошельков исчезали все средства. Для отмывания средств часть процесса передавалась внешним поставщикам услуг (своеобразный аутсорсинг) для поиска «денежных мулов».

4. Теневой рынок или криптомаркет (Dark Web Marketplaces (DWM) and DarkNet). Это скрытая сеть, соединения которой устанавливаются только между доверенными узлами (пирами), с использованием нестандартных транспортных протоколов и портов. Даркнет – это часть интернета, которая не индексируется традиционными поисковыми системами и для доступа к которой требуется специальное программное обеспечение. Именно в Даркнете сосредоточено множество торговых площадок, на которых киберпреступники могут покупать и продавать различные SaaS-приложения (например, вредоносное ПО, эксплойты или украденные данные). Сайты, размещенные в Даркнете, не индексируются поисковыми системами из-за контроля доступа, динамического содержимого или других механизмов (например, шифрования или специализированного ПО). Соответствующая закрытая инфраструктура содержит криминальный контент в виде краденой персональной информации, доступ к «высококласным» вредоносным программам и эксплойтам, а также поддерживает другие категории криминальной деятельности. К ним относят, в первую очередь, детскую порнографию, торговлю оружием и наркотиками, проституция, торговля людьми и поддержка террористических организаций и операций. Большинство этих сайтов являются временными, работают непродолжительное время и постоянно меняют адреса, тем самым пытаясь свести к минимуму риск разоблачения со стороны правительственных агентств, правоохранительных органов и исследователей кибербезопасности. Дополнительно существуют онлайн-форумы, на которых покупается и продается соответствующая информация, инструментарий и услуги, для достижения поставленных целей киберпреступниками [62].

В Даркнете на продажу выставляются, прежде всего, персональные данные (например, сканы и фото документов, или данные банковских карт), так и сведения, которые характеризуют деятельность отдельных компаний (БД с информацией о сотрудниках, партнерах или клиентах, документы, содержащие корпоративную информацию, коммерческую тайну и др.). Отдельным сегментом выступают вредоносные программы, предлагаемые по модели MaaS (malware-as-a-service), а также различные виды услуг (например, сбор конфиденциальной информации по запросу, вывод украденных денег, атаки типа DDOS и постоянные отказы в обслуживании (Permanent Denial-of-Service (PDoS) [63], или рассылка спама и т.д.). Киберпреступные группировки, используя ресурсы Даркнет, могут осуществлять также подбор персонала на постоянную или временную работу. Следует иметь в виду, что



дополнительно используется «модель гаранта» (посредника) для совершения сделок. В целях уменьшения рисков при заключении сделок кибермошенники прибегают к услугам посредников, которых называют «гарантами» (escrow). Гаранты берут на себя ответственность за своевременное предоставление данных или услуги в соответствии с заявленными характеристиками, своевременную оплату товара или услуги, конфиденциальность личной и финансовой информации.

5. Исследование как услуга (Research-as-a-Service ReaaS). Исследования, потребляемые в качестве услуги, могут превратиться в новый интерфейс прикладного программирования цифровой эпохи, который окажет помощь компаниям в улучшении взаимодействия со своими клиентами. Информационная нестабильность заставляет кибермошенников анализировать и понимать комплекс событий в режиме реального времени, которые формируют их бизнес. Причем эта деятельность базируется не только на используемых отчетах ведущих компьютерных и программных производителей, а также исследовательских работах ведущих мировых фирм, сосредоточивших свои усилия в области информационной безопасности и борьбы с компьютерными преступлениями (например, такие как, CrowdStrike, Check Point, Kaspersky и др.). Одновременно, они используют в своей деятельности огромный объем исследовательских материалов – финансовых, рыночных и общеэкономических в целях анализа существующих проблем и управленческих решений. Повседневная практика свидетельствует об экономическом обосновании предложения и потребления исследований как услуги. В качестве примера можно привести информацию о характере уязвимостей, ошибках нулевого дня и т.д. Разработчики вредоносного ПО могут использовать основные преимущества ReaaS – масштабируемость, гибкость и экономическую заинтересованность.

6. Киберпреступность как экономика (Cybercrime-as-an-Economy CaaSE). Успех той или иной отрасли (промышленность, агробизнес, туристический бизнес и др.) зависит от состояния ее экономики – производства, распределения и использования товаров и услуг. Киберпреступность ничем не отличается от «обычной» преступности и поддерживает свою собственную экономику продуктов и услуг. Следует обратить внимание на неоспоримый факт – киберпреступность представляет собой быстро развивающуюся отрасль без признаков замедления. И все аспекты деятельности, от разработки новых способов совершения киберпреступлений и до методов и форм распространения информации, становятся все более изобретательными [64-66].

## Литература

1. Международная информационная безопасность: Теория и практика: В трех томах. / Под общ. ред. А.В. Крутских. - М.: Издательство «Аспект Пресс, 2021.- 384 с. ISBN 97805-7567-1097-7

2. Tallinn Manual on the International Law Applicable to Cyber Warfare (2013). Prepared by the International Group of Experts at the Invitation of The NATO Cooperative Cyber Defence Centre of Excellence. Cambridge University Press. ISBN 978-1-107-02443-4 <http://csef.ru/media/articles/3990/3990.pdf> (дата обращения: 04.05.24)
3. Eric Talbot Jensen. The Tallinn Manual 2.0: Highlights and Insights. *Georgetown Journal of International Law*. 2017, Vol. 48, p.735-778. <https://www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2018/05/48-3-The-Tallinn-Manual-2.0.pdf> (дата обращения: 04.05.24)
4. Ana Lenard (2016). The Nascent Law of Cyber Blockades and Zones. *New Zealand Yearbook of International Law*, Volume: 14. Pp. 94–133. ISBN: 9789004345911 [https://doi.org/10.1163/9789004345911\\_005](https://doi.org/10.1163/9789004345911_005)
5. Serghei Ohrimenco, Grigori Borta (2020). Challenges for Digital Transformation in the Manufacturing Industry/Socio-Economic Development Interdisciplinary Ecosystems Perspective. Cracow University of Economics. ISBN 978-83-8175-233-6
6. Serghei Ohrimenco, Grigori Borta (2018). The Challenges of Shadow Information Economics. / Conference on Mathematical Foundations of Informatics. Institute of Mathematics and Computer Science, July 2-6, 2018, Chisinau, Moldova. Pp.190-199. ISBN 978-9975-4237-7-9
7. Яковлева, А. В. Кибербезопасность и ее правовое регулирование (зарубежный и российский опыт) / А. В. Яковлева // Социально-политические науки. – 2021. – Т. 11. – № 4. – С. 70-81. – DOI 10.33693/2223-0092-2021-11-4-70-81.
8. Яникеева И.О. Российско-американские отношения в сфере обеспечения международной информационной безопасности / *Мировая политика*. – 2022. – № 4. – С. 1 - 15. DOI: 10.25136/2409-8671.2022.4.38897 EDN: JKNPZX URL: [https://nbpublish.com/library\\_read\\_article.php?id=38897](https://nbpublish.com/library_read_article.php?id=38897) (дата обращения: 04.05.24)
9. Зиновьева Е. С., Яникеева И. О. Эволюция взаимодействия России и США в области международной информационной безопасности в исторической ретроспективе / *Вестник Санкт-Петербургского университета. Международные отношения*. 2022. Т.15. Вып.2. С.158–173. <https://doi.org/10.21638/spbu06.2022.203>
10. Cyber sanctions. [https://en.wikipedia.org/wiki/Cyber\\_sanctions](https://en.wikipedia.org/wiki/Cyber_sanctions) (дата обращения: 04.05.24)
11. George Perkovich. Ariel E. Levite (2017). *Understanding Cyber Conflict: Fourteen Analogies*. Georgetown University Press. ISBN 9781626164994
12. Атрибуция: серьезная проблема для киберсанкций ЕС. <https://katehon.com/ru/article/atribuciya-sereznaya-problema-dlya-kibersankciy-es> (дата обращения: 04.05.24)
13. Florian J. Egloff (2020). Contested public attributions of cyber incidents and the role of academia. *Contemporary Security Policy*, DOI: 10.1080/13523260.2019.1677324
14. Egloff, Florian , Wenger, Andreas (2019). Public Attribution of Cyber Incidents. *CSS Analyses in Security Policy* 244. ETH Library. Public Attribution of Cyber

- Incidents. <https://doi.org/10.3929/ethz-b-000340841> <https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/340841/CSSAnalyse244-EN.pdf?sequence=2&isAllowed=y> (дата обращения: 04.05.24)
15. Котенко И.В., Хмыров С.С. (2022). Анализ моделей и методик, используемых для атрибуции нарушителей кибербезопасности при реализации целевых атак. Вопросы кибербезопасности. 2022. No 4(50). С.52-79. DOI:10.21681/2311-3456-2022-4-52-79 (дата обращения: 04.05.24)
  16. Florian J. Egloff, Max Smeets (2021). Publicly attributing cyber attacks: a framework. <https://www.tandfonline.com/doi/full/10.1080/01402390.2021.1895117> (дата обращения: 04.05.24).
  17. Michelle F. Wright, Takuya Yanagida, Ikuko Aoyama, Lenka Dědková, Zheng Li, Shanmukh V. Kamble, Fatih Bayraktar, Anna Ševčíková, Shruti Soudi, Hana Macháčková, Li Lei, Chang Shu (2016). Differences in Attributions for Public and Private Face-to-face and Cyber Victimization Among Adolescents in China, Cyprus, the Czech Republic, India, Japan, and the United States, *The Journal of Genetic Psychology*, <https://pubmed.ncbi.nlm.nih.gov/27379372/> DOI: 10.1080/00221325.2016.1185083 (дата обращения: 04.05.24)
  18. Jon R. Lindsay (2015). Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack. *Journal of Cybersecurity*, Volume 1, Issue 1, September 2015, Pages 53–67, <https://doi.org/10.1093/cybsec/tyv003>; [academic.oup.com/cybersecurity/article/1/1/53/2354517](http://academic.oup.com/cybersecurity/article/1/1/53/2354517) (дата обращения: 04.05.24)
  19. Sasha Romanosky, Benjamin Boudreaux (2021) Private-Sector Attribution of Cyber Incidents: Benefits and Risks to the U.S. Government, *International Journal of Intelligence and CounterIntelligence*, 34:3, 463-493, DOI: 10.1080/08850607.2020.1783877 <https://www.tandfonline.com/doi/abs/10.1080/08850607.2020.1783877> (дата обращения: 04.05.24)
  20. Andrew Grotto (2020). Deconstructing Cyber Attribution: A Proposed Framework and Lexicon. *IEEE Security & Privacy* (Volume: 18, Issue: 1, Jan.-Feb. 2020). P. 12 – 20. ISSN: 1558-4046 DOI: 10.1109/MSEC.2019.2938134
  21. Florian J Egloff, Myriam Dunn Cavelty (2021). Attribution and Knowledge Creation Assemblages in Cybersecurity Politics. / *Journal of Cybersecurity*, Volume 7, Issue 1, 2021, <https://doi.org/10.1093/cybsec/tyab002>; [academic.oup.com/cybersecurity/article/7/1/tyab002/6261798](http://academic.oup.com/cybersecurity/article/7/1/tyab002/6261798) (дата обращения: 04.05.24)
  22. Явор Колев: Руски хакери стоят зад атаката на изборите през 2015 г. <https://www.segabg.com/hot/yavor-kolev-ruski-hakeri-stoyat-zad-atakata-na-izborite-prez-2015-g?page=1> (дата обращения: 04.05.24)
  23. Ц.Цветанов: Да се защитим от кибератаки и фалшиви новини по време на евроизборите (Снимки, видео). <https://www.24chasa.bg/bulgaria/article/7339844> (дата обращения: 04.05.24)
  24. David Perera (2022). Russian Hackers Targeted Oil Refinery Firm in NATO Country ('Gamaredon,' Tied to FSB, Expands Intelligence Ops as Invasion of Ukraine Persists). <https://www.bankinfosecurity.com/russian-hackers-targeted-oil-refinery-firm-in-nato-country-a-20753> (дата обращения: 04.05.24)

25. Жан Рофе (2024). Хакеров из Китая подозревают в многолетнем шпионаже за VW. [https://www.dw.com/ru/hakerov-iz-kitaa-podozrevaut-v-mnogoletnem-spionaze-za-volkswagen/a-68879526#:~:text=Германский%20автомобильный%20концерн%20Volkswagen%20\(VW,агентства%20дра%20отказался%20предоставить%20подробности.](https://www.dw.com/ru/hakerov-iz-kitaa-podozrevaut-v-mnogoletnem-spionaze-za-volkswagen/a-68879526#:~:text=Германский%20автомобильный%20концерн%20Volkswagen%20(VW,агентства%20дра%20отказался%20предоставить%20подробности.) (дата доступа 21.04.24)
26. Архивные данные с сайта Thailand Computer Emergency Response Team (ThaiCERT), <https://www.thaicert.or.th>
27. Caltagirone, Sergio, Pendergast, Andrew, Betz, Christopher (2013), The Diamond Model of Intrusion Analysis. Center For Cyber Intelligence Analysis And Threat Research. <https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf> (дата обращения: 04.05.24)
28. Rid, Thomas & Buchanan, Ben, (2015) Attributing Cyber Attacks, Journal of Strategic Studies, 38:1-2, 4-37. [http://dx.doi.org/10.1080/01402390.2014.977382;cs.brown.edu/courses/cs180/sources/Attributing\\_Cyber\\_Attacks.pdf](http://dx.doi.org/10.1080/01402390.2014.977382;cs.brown.edu/courses/cs180/sources/Attributing_Cyber_Attacks.pdf) (дата обращения: 04.05.24)
29. European Union establishes a sanction regime for cyber-attacks. <https://ccdcoe.org/library/publications/european-union-establishes-a-sanction-regime-for-cyber-attacks/> (дата обращения: 04.05.24)
30. Яникеева И.О. Роль киберсанкций в международных отношениях. // Вестник Дипломатической Академии МИД России. Россия и мир. 2022, 1(31), с.6-33. ISSN: 2410-2415
31. Raphael S. Cohen, Nathan Chandler, Shira Efron, Bryan Frederick, Eugeniu Han, Kurt Klein, Forrest E. Morgan, Ashley L. Rhoades, Howard J. Shatz, Yuliya Shokh (2020). The Future of Warfare in 2030. RAND Corporation. ISBN: 978-1-9774-0295-0
32. Quentin E. Hodgson, Yuliya Shokh, Jonathan Balk (2022). Many Hands in the Cookie Jar. Case Studies in Response Options to Cyber Incidents Affecting U.S. Government Networks and Implications for Future Response. RAND Corporation. ISBN: 978-1-9774-0901-0 DOI: <https://doi.org/10.7249/RRA1190-1>
33. JP 3-12 Cyberspace Operations, 8 June 2018, p. 100. [https://irp.fas.org/doddir/dod/jp3\\_12.pdf](https://irp.fas.org/doddir/dod/jp3_12.pdf) (дата обращения: 04.05.24)
34. Daniel T. Kuehl. From Cyberspace to Cyberpower: Defining the Problem. <https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-02.pdf?ver=2017-06-16-115052-210> (дата обращения: 04.05.24)
35. James B. Godwin, Andrey Kulpin, Karl Frederick Rauscher and Valery Yaschenko (2014). The Russia-U.S. Bilateral on Cybersecurity – Critical Terminology Foundations, Issue 2. EastWest Institute and the Information Security Institute of Moscow State University. ISBN 978-0-9856824-4-6 <https://www.files.ethz.ch/isn/178418/terminology2.pdf> (дата обращения: 04.05.24)
36. The Joint Publication (JP) 1-02, Department of Defense Dictionary of Military and Associated Terms. [https://irp.fas.org/doddir/dod/jp1\\_02.pdf](https://irp.fas.org/doddir/dod/jp1_02.pdf) (дата обращения: 04.05.24)

37. ISO/IEC 27032:2012 Information technology — Security techniques — Guidelines for cybersecurity. <https://www.iso.org/standard/44375.html> (дата обращения: 04.05.24)
38. Международный Союз Электросвязи. Серия X: Сети передачи данных и взаимосвязь открытых систем. Безопасность электросвязи. Структура технологий безопасности для подвижной передачи данных от конца до конца. Рекомендации МСЭ-Т X.1121. <https://www.itu.int> (дата обращения: 04.05.24)
39. Ю.И. Стародубцев, П.В. Закалкин, С.А. Иванов. Техносферная война как основной способ разрешения конфликтов в условиях глобализации. / Военная Мысль. № 10. 2020, С.16-21. <https://vm.ric.mil.ru/Nomera/6/> (дата обращения: 24.11.2022)
40. Alison Lawlor Russell (2014). Cyber Blockades. Georgetown University Press. ISBN 978-1-62616-113-9
41. Международная информационная безопасность: Теория и практика: В трех томах. / Под общ. ред. А.В.Крутских.-М.: Издательство «Аспект Пресс, 2021.- 384 с. ISBN 97805-7567--1097-7
42. Alison Shirin Lawlor Russell (2012). Cyber Blockades: Towards a Theory of Informational Warfare in the Digital Era. <https://dl.tufts.edu/concern/pdfs/pv63gb62x> (дата доступа 04.05.24).
43. The economic impact of shutting down Internet and mobile phone services in Egypt. <https://www.oecd.org/countries/egypt/theeconomicimpactofshuttingdowninternetandmobilephoneservicesinegypt.htm> (дата обращения: 04.05.24)
44. Mathew Schwartz (2011). Egypt Takes \$90 Million Hit From Internet Blackout. <https://www.networkcomputing.com/egypt-takes-90-million-hit-internet-blackout>. (дата обращения 26.10.2022)
45. Nicholas Michael Sambaluk (2019). Conflict In the 21st -Century: The Impact of Cyber Warfare, Social Media, And Technology. ABC-CLIO, LLC. ISBN: 978-1-4408-6000-3
46. Aaron Franklin Brantly (2016). The Decision to Attack Military and Intelligence Cyber Decision- Making. University of Georgia Press. ISBN 9780820349190
47. Victor Sheymov (2021). Cyberspace and Security: A Fundamentally New Approach. Third Revised Edition. Cyberbooks Publishing. ISBN: 978-0-9858930-8-8
48. The Cyber Resilience Index: Advancing Organizational Cyber Resilience. White Paper, July 2022. [https://www3.weforum.org/docs/WEF\\_Cyber\\_Resilience\\_Index\\_2022.pdf](https://www3.weforum.org/docs/WEF_Cyber_Resilience_Index_2022.pdf) (дата обращения 27.07.2023)
49. Cybersecurity Capacity Maturity Model for Nations (CMM). 2021 Edition. <https://gcsc.ox.ac.uk/files/cmm2021editiondocpdf> (дата обращения 27.07.2023)
50. Global Cybersecurity Index. <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx> (дата обращения 27.07.2023)
51. Julia Voo, Irfan Hemani, Daniel Cassidy (2022). National Cyber Power Index 2022. Report September 2022. [www.belfercenter.org/project/cyber-project](http://www.belfercenter.org/project/cyber-project) (дата доступа 12.05.2024)
52. Aaron Franklin Brantly (2016). The Decision to Attack Military and Intelligence Cyber Decision- Making. University of Georgia Press. ISBN 9780820349190

53. Bruce Bueno de Mesquita, Frans N. Stokman (1994). *European Community Decision Making: Models, Applications, And Comparisons*. Yale University. ISBN 0-300-05759-8
54. Quiggin John (1993). *Generalized Expected Utility Theory: The Rank-Dependent Model*. Springer Science. ISBN 978-94-011-2182-8 DOI 10.1007/978-94-011-2182-8
55. Scott Ashworth, Christopher R. Berry, Ethan Bueno De Mesquita (2021). *Theory and Credibility: Integrating Theoretical and Empirical Social Science*. Princeton University Press. ISBN 9780691215006
56. Ethan Bueno De Mesquita, Anthony Fowler (2021). *Thinking Clearly with Data: A Guide to Quantitative Reasoning and Analysis*. Princeton University Press. ISBN 9780691214351
57. Lucas Kello (2017). *The Virtual Weapon and International Order*. Yale University Press. ISBN 9780300220230
58. Jansen van Vuuren, J.C., Leenen, L. (2018). A Model for Measuring Perceived Cyberpower. *Proceedings of the 13th International Conference on Cyber Warfare and Security, National Defence University, 8-9 March 2018, Washington D.C.*, pp. 320-327 ISBN 978-1-5108-5963-0 <http://hdl.handle.net/10204/10361> (дата обращения 13.05.2024)
59. Mike Sciandra (2018). *Cybercrime: Using Computers as Weapons*. Lucent Press. ISBN 9781534560925
60. Keman Huang, Michael Siegel, Stuart Madnick (2017). *Cybercrime-as-a-Service: Identifying Control Points to Disrupt*. Working Paper CISL# 2017-17. <https://cams.mit.edu/wp-content/uploads/2017-17.pdf> (дата доступа 05.06.2024)
61. Todd Moore (2023). *Protect Your Organization from Cybercrime-as-a-Service Attacks*. <https://cpl.thalesgroup.com/blog/encryption/cybercrime-as-a-service-caas-explained> (дата доступа 05.06.2024)
62. Rob Downs, Vicky Ray (2016). *Exploring the Cybercrime Underground: Part 1 – An Introduction*. <https://unit42.paloaltonetworks.com/unit42-exploring-the-cybercrime-underground-part-1-an-introduction/> (дата доступа 10.06.2024)
63. Abaimov S. *Understanding and Classifying Permanent Denial-of-Service Attacks // Journal of Cybersecurity and Privacy. – 2024. – Т. 4. – №. 2. – С. 324-339.* <https://doi.org/10.3390/jcp4020016>
64. Mike Sciandra (2018). *Cybercrime: using computers as weapons*. Greenhaven Press. ISBN 9781534560925
65. Ethem Ilbiz, Christian Kaunert (2023). *The Sharing Economy for Tackling Cybercrime: Uberization of Public-Private Partnerships*. Springer. ISBN – 13 9783031202735
66. Thomas J. Holt (2019). *Cybercrime Through an Interdisciplinary Lens*. Taylor & Francis. ISBN-13 978-1-315-61845-6

## ГЛАВА 6. АНАЛИЗ РЫНКА ПЕЧАТНЫХ ПЛАТ В РФ

Предлагаем рассмотреть влияние санкций на примере рынка печатных плат в РФ.

*Объем рынка печатных плат.*

В рамках рассматриваемого периода показатель видимого потребления печатных плат на внутреннем рынке в целом демонстрирует тренд поступательного увеличения, что непосредственно является результатом роста спроса со стороны основных потребляющих сегментов. В оценке четырехлетнего периода 2019-2022 годов объем рынка печатных плат увеличился на 12,3%.

По результатам 2022 года потребление печатных плат в России составило 122,0 млн. шт., что на 10,4% ниже, чем в 2021 году, когда показатель видимого потребления достиг уровня 136,2 млн. шт. Значительное снижение показателя по итогам 2022 года вызвано влиянием санкционных ограничений, в результате которых произошло существенное сокращение импортных поставок печатных плат на российский рынок.

При этом, по результатам января-сентября 2023 года потребление составило 98,3 млн. шт., что на 12,4% больше показателя за аналогичный период предыдущего года. Данная динамика свидетельствует о восстановительном тренде и возвращении рынка в зону положительных значений.

Согласно оценочным данным, объем потребления печатных плат в России по итогам 2023 года увеличится на 8,4% относительно уровня предыдущего года и составит 132,3 млн. шт.

**Основными драйверами рынка выступают:** уровень и состояние платежеспособного спроса основных сегментов потребителей, баланс спроса и предложения, уровень реальных располагаемых доходов населения и динамика их движения, общие макроэкономические индикаторы состояния российской экономики.

**Основное влияние пандемии коронавируса** отразилось в увеличении объемности российского рынка печатных плат в существенных параметрах.

**Влияние санкций на российскую экономику** беспрецедентное, при этом уровень негативного воздействия в зависимости от конкретного сегмента экономики существенно разнится. Наиболее отрицательная динамика наблюдается в сырьевых сегментах экономики.

**Введенные санкционные ограничения** оказали влияние на баланс спроса и предложения на рынке печатных плат в России, изменение параметров и их направленность обозначены ниже в рамках данного раздела исследования. Структурность продуктового предложения на рынке печатных плат также показала смещение, но данная тенденция носит положительный характер.

Цифровые показатели объемов потребления печатных плат в физических величинах на российском рынке, а также параметры

роста/сокращения в рамках рассматриваемого периода представлены в таблице ниже.

	2019	2020	2021	2022	2023
<b>Видимое потребление, млн. шт.</b>	108,7	114,6	136,2	122,0	132,3
<b>Темп роста, %</b>		5,5%	18,8%	- 10,4%	8,4%
<b>Объемы видимого потребления, январь-сентябрь, млн. шт.</b>	78,5	81,5	99,4	87,4	98,3
<b>Темп роста, янв-сен/янв-сен, %</b>		3,8%	22,0%	- 12,1%	12,4%

*Источник:* на основе данных ФСГС и ФТС РФ, таможенных деклараций

#### *Динамика индикаторов рынка печатных плат.*

Основное влияние на увеличение видимого потребления по итогам 2019-2022 годов оказал рост внутреннего производства: за данный период выпуск печатных плат отечественными производителями вырос на 90,2%. При этом импортная продукция занимает значительную долю потребления и показывает отрицательную динамику. Экспортные поставки печатных плат носят несущественный характер.

Цифровые показатели российского рынка печатных плат в физических величинах, а также параметры роста/сокращения по итогам рассматриваемого периода представлены в таблице ниже.

	2019	2020	2021	2022	2023 (янв-сен)
<b>Производство, млн. шт.</b>	21,1	31,8	37,9	40,2	30,5
<b>Темп роста, %</b>		50,4%	19,2%	6,1%	
<b>Импорт, млн. шт.</b>	88,7	84,9	100,1	83,0	68,5
<b>Темп роста, %</b>		-4,3%	17,9%	-17,1%	
<b>Экспорт, млн. шт.</b>	1,2	2,1	1,8	1,2	0,7
<b>Темп роста, %</b>		73,2%	-13,8%	-35,0%	
<b>Видимое потребление, млн. шт.</b>	108,7	114,6	136,2	122,0	98,3
<b>Темп роста, %</b>		5,5%	18,8%	-10,4%	

*Источник:* на основе данных ФСГС и ФТС РФ, таможенных деклараций

#### *Динамика и объем потребления печатных плат.*

Объем российского рынка печатных плат в стоимостной оценке в рамках всего рассматриваемого в данном исследовании периода показывает восходящую динамику. Данная тенденция непосредственно обусловлена ростом ценовых индикаторов на продукцию.

Объем потребления печатных плат в стоимостном выражении по результатам 2022 года в России составил 26909,8 млн. руб., что на 6,1% выше,



чем в 2021 году, показатель которого был зафиксирован на отметке 25371,9 млн. руб. Стоимостная оценка рынка в отличие от натуральных объемов характеризуется положительной динамикой, что вызвано корректировкой средних цен на продукцию в сторону увеличения.

По результатам января-сентября 2023 года видимое потребление составило 28331,2 млн. руб., что выше показателя за аналогичный период предыдущего года на 50,5%. Увеличение стоимостной объемности потребления связано с наращиванием физических объемов рынка вкупе с положительным движением ценовых величин на продукцию.

По прогнозным оценкам, объем потребления печатных плат в стоимостном выражении в России в 2023 году вырастет на 53,5% в сравнении с 2022 годом и составит 41303,0 млн. руб.

Цифровые показатели объемов потребления печатных плат в стоимостном выражении на российском рынке, а также параметры роста/сокращения в рамках рассматриваемого периода представлены в таблице ниже.

	2019	2020	2021	2022	2023
<b>Видимое потребление, млн. руб.</b>	14	18	25	26	41
	328,2	252,3	371,9	909,8	303,0
<b>Темп роста, %</b>		27,4%	39,0%	6,1%	53,5%
<b>Объемы видимого потребления, январь-сентябрь, млн. руб.</b>	8	9	13	18	28
	364,5	857,1	103,7	828,7	331,2
<b>Темп роста, янв-сен/янв-сен, %</b>		17,8%	32,9%	43,7%	50,5%

*Источник:* на основе данных ФСГС и ФТС РФ, таможенных деклараций

Динамика и объем продуктового предложения. В рассмотрении ретроспективной и текущей структурности продуктового предложения (импортный продукт/отечественный продукт) печатных плат на российском рынке необходимо отметить достаточную стабильность и доминирование импортного продукта.

По итогам рассматриваемого периода 2023 года объем российской продукции в разрезе продуктового предложения на рынке печатных плат в России составил 29,8 млн. шт. Объем импортной продукции составил 68,5 млн. шт.

Цифровые показатели продуктового предложения печатных плат на российском рынке, а также параметры роста/сокращения по итогам рассматриваемого периода представлены в таблице ниже.

	2019	2020	2021	2022	2023 (янв-сен)
<b>Российская продукция, млн. шт.</b>	19,9	29,7	36,1	39,1	29,8
<b>Темп роста, %</b>		49,0%	21,5%	8,2%	

	2019	2020	2021	2022	2023 (янв-сен)
<b>Импорт, млн. шт.</b>	88,7	84,9	100,1	83,0	68,5
<b>Темп роста, %</b>		-4,3%	17,9%	-17,1%	

*Источник:* на основе данных ФСГС и ФТС РФ, таможенных деклараций

В структуре внутреннего потребления преобладает импортная продукция: на ее долю по итогам рассматриваемого периода 2023 года пришлось 69,7% всей продукции на рынке. Значение данного показателя демонстрирует сокращение в рамках пятилетнего периода, но ввиду преобладающей доли именно импортной продукции, структурность потребления продукта по происхождению является устойчивой.

Как видно из данных, приведенных на диаграмме, в период с 2019 по 2023 год отечественные производители нарастили позиции на внутреннем рынке: их доля увеличилась на 12,0 процентных пункта.

Предложение печатных плат на российском рынке. В целом по итогам 2019-2022 годов объем предложения печатных плат на российском рынке показал увеличение на 12,1% с достижением в рамках 2022 года показателя в 123,2 млн. шт. При этом предложение печатных плат в предыдущем 2021 году составило 138,0 млн. шт.

Стоит отметить, что в рамках текущего временного ряда 2023 года объем предложения печатных плат был зафиксирован на уровне 98,9 млн. шт.

*Объем предложения печатных плат на российском рынке складывается из объемов выпуска данной продукции и объемов импортной продукции, поступающей из иностранных государств.*

Динамика объемов предложения печатных плат на российском рынке, а также параметры роста/сокращения по итогам рассматриваемого периода представлены в таблице ниже.

	2019	2020	2021	2022	2023 (янв-сен)
<b>Объем предложения, млн. шт.</b>	109,9	116,7	138,0	123,2	98,9
<b>Темп роста, %</b>		6,2%	18,3%	-10,8%	

*Источник:* на основе данных ФСГС и ФТС РФ, таможенных деклараций

Спрос на печатные платы на рынке. Итоговые показатели объемов спроса на печатные платы в России в рамках 2022 года составили 124,4 млн. шт., показав тем самым сокращение на 9,1% по отношению к предыдущему году, когда спрос составлял 136,9 млн. шт. При этом в рассмотрении годовых значений показателя спроса на печатные платы, в течение периода 2019-2022 годов, общая динамика характеризуется увеличением на 13,2%.

В оценке текущего временного ряда 2023 года объем спроса на печатные платы составил 100,1 млн. шт.

*Объем спроса на печатные платы на рынке России складывается из объемов продаж с учетом складских запасов и объемов экспортной продукции, отправляемой на рынки зарубежных стран.*

Динамика объемов спроса на печатные платы на рынке России, а также показатели роста/сокращения в рамках рассматриваемого периода представлены в таблице ниже.

	2019	2020	2021	2022	2023 (янв-сен)
<b>Объем спроса, млн. шт.</b>	109,8	117,0	136,9	124,4	100,1
<b>Темп роста, %</b>		6,5%	17,0%	-9,1%	

*Источник:* на основе данных ФСГС и ФТС РФ, таможенных деклараций

#### *Баланс спроса и предложения печатных плат на рынке России.*

Предложение на рынке печатных плат превышает объемы спроса в 2019 и 2021 годах, в рамках остальных периодов наблюдается обратная ситуация.

Далее, поговорим о динамике и объемах производства на рынке печатных плат.

По итогам рассматриваемого периода производственные показатели по выпуску печатных плат российскими участниками рынка показали увеличение. Так, в оценке четырехлетнего интервала 2019-2022 годов производство печатных плат в России выросло на 90,2%. Ключевым фактором увеличения объемов производства продукции российскими производителями является восходящая динамика спроса со стороны основных секторов-потребителей.

Объем производства печатных плат в России в 2022 году составил 40,2 млн. шт. Аналогичный показатель 2021 года был равен 37,9 млн. шт., таким образом, в прошлом году прирост составил 6,1%. Увеличение данного показателя продиктовано необходимостью удовлетворения растущего объема потребления на внутреннем рынке, которое происходит на фоне замещения импортной продукции российским продуктом.

В 2023 году в январе-сентябре отечественными предприятиями было выпущено 30,5 млн. шт. печатных плат, что больше прошлогоднего показателя за аналогичный период, который составил 29,6 млн. шт., на 3,0%. Положительная тенденция подтверждает общий восходящий тренд в производстве печатных плат на российском рынке. Ввиду того, что производство данной продукции является высокорентабельным и широко востребованным, наблюдается ежегодное увеличение товарного выпуска.

По оценочным данным объем производства печатных плат в России в 2022 году увеличится на 2,8% в сравнении с 2023 годом и составит 41,3 млн. шт.

**Влияние санкционных мер 2022 года** отразилось в замедлении развития экономики России; усилении волатильности рубля, инфляционном давлении на экономику; дестабилизации финансового рынка и банковской системы, которая привела к исчезновению большого количества региональных игроков,

кредитовавших малый и средний бизнес, удорожанию кредитных денег и, как следствие, росту цен на конечный продукт. Так же введенные санкции привели к оттоку крупных западных инвесторов, снижению инвестиционной активности; отказу от реализации отдельных программ вследствие сокращения расходной части бюджета; усложнению финансирования технологического перевооружения стратегически важных секторов промышленности вследствие финансового дефицита; остановке производств, зависимых от импорта.

Санкционные меры так же привели к развитию программ импортозамещения, как основного способа минимизации влияния внешних факторов на экономику в условиях сложившейся технологической зависимости; программ диверсификации российского производства, которые заключаются в расширении ассортимента выпускаемой продукции и освоении новых рынков сбыта; усилению активности России в направлении международной кооперации, в особенности в направлении стран Азии.

**Введенные санкции 2022 года в отношении РФ** проявились в корректировке производственной активности российских производителей продукта и в изменении их поведения. Кроме того, в виду наиболее масштабного санкционного давления в рамках первых месяцев отмечается корректировка цикла сезонности. Ограничения логистического характера оказали непосредственное влияние на структуру товарных потоков и привели к трансформации поточности.

Цифровые показатели объемов производства печатных плат на российском рынке в оценке соответствующего временного ряда, а также параметры роста/сокращения представлены в таблице ниже.

	2019	2020	2021	2022	2023
<b>Производство, млн. шт.</b>	21,1	31,8	37,9	40,2	41,3
<b>Темп роста, %</b>		50,4%	19,2%	6,1%	2,8%
<b>Объем производства, январь-сентябрь, млн. шт.</b>	15,2	19,8	27,5	29,6	30,5
<b>Темп роста, янв-сен/янв-сен, %</b>		30,4%	39,1%	7,6%	3,0%

*Источник:* на основе данных ФСТС РФ

*Анализ производства печатных плат по регионам, структура производства.*

В структуре производства печатных плат по федеральным округам первое место занимает Центральный федеральный округ, на долю которого приходится 64,1% по состоянию на январь-сентябрь 2023 года. Второе место занимает Сибирский федеральный округ с долевым эквивалентом в 18,7%, третье - Северо-Западный федеральный округ с долевым показателем в 12,4%. Данная структурность производства печатных плат на внутреннем рынке

обусловлена сосредоточением производственных мощностей в обозначенных регионах.

В течение 2022-2023 (январь-сентябрь) годов географическая структура производства печатных плат по федеральным округам претерпела определенные изменения:

- Центральный федеральный округ – доля округа в общем объеме производства сократилась на 6,9 процентных пункта;
- Сибирский федеральный округ – доля выросла на 2,6 процентных пункта;
- Северо-Западный федеральный округ – доля выросла на 5,0 процентных пункта;
- Приволжский федеральный округ – доля сократилась на 0,6 процентных пункта;
- Южный федеральный округ – доля не изменилась;
- Уральский федеральный округ – доля сократилась на 0,1 процентных пункта.

Рассматривая географическую структуру производства печатных плат по итогам 2019-2023 годов среди основных федеральных округов-производителей продукции стоит отметить следующее:

- доля Центрального федерального округа в общем объеме внутреннего производства увеличилась на 10,4 процентных пункта;
- при этом долевая составляющая, приходящаяся на Сибирский федеральный округ, в это же время показала сокращение на 2,4 процентных пункта;
- долевым эквивалент Северо-Западного федерального округа сократился на 2,7 процентных пункта.

В натуральных показателях изменение производства печатных плат в разрезе крупнейших федеральных округов по выпуску продукции в рамках 2019-2022 годов составило:

- объем выпуска продукции предприятиями Центрального федерального округа увеличился на 17,2 млн. шт. до уровня 28,5 млн. шт.;
- рост объемов производства продукции зафиксировано в рамках Сибирского федерального округа на 2,0 млн. шт. до отметки 6,5 млн. шт.;
- снижение объемов выпуска продемонстрировали производители в Северо-Западном федеральном округе на 0,2 млн. шт., показав значение по итогам 2022 года 3,0 млн. шт.

Цифровые показатели объемов производства печатных плат на российском рынке в оценке федеральных округов, а также параметры роста/сокращения по итогам 2022/2021 годов представлены в таблице ниже.

	2019	2020	2021	2022	2023 (янв-сен)	2022/ 2021
<b>Россия</b>	21,133	31,783	37,882	40,204	30,482	6,1%
<b>Центральный федеральный округ</b>	11,350	22,344	28,759	28,548	19,532	-0,7%

	2019	2020	2021	2022	2023 (янв-сен)	2022/ 2021
<b>Сибирский федеральный округ</b>	4,458	5,190	5,974	6,456	5,690	8,1%
<b>Северо-Западный федеральный округ</b>	3,183	2,260	2,113	2,967	3,773	40,4%
<b>Приволжский федеральный округ</b>	2,064	1,929	0,965	2,124	1,416	120,0%
<b>Южный федеральный округ</b>	0,034	0,040	0,045	0,083	0,058	82,1%
<b>Уральский федеральный округ</b>	0,044	0,020	0,025	0,026	0,012	3,5%
<b>Северо-Кавказский федеральный округ</b>	0,000	0,000	0,000	0,001	0,001	-

*Источник:* на основе данных ФСГС РФ

*Динамика и объем товарных потоков.* В рассмотрении ретроспективной и текущей объемности товарных потоков (направлений отгрузок на внутренний рынок и на экспортные направления) печатных плат на российском рынке необходимо отметить достаточную стабильность и исключительное преобладание поставок на российский рынок.

По итогам рассматриваемого периода 2023 года на внутренний рынок было поставлено 29,8 млн. шт. печатных плат. На экспорт отправлено 0,7 млн. шт. печатных плат.

Цифровые показатели направления отгрузок печатных плат, а также параметры роста/сокращения по итогам рассматриваемого периода представлены в таблице ниже.

	2019	2020	2021	2022	2023 (янв-сен)
<b>Внутренний рынок, млн. шт.</b>	19,9	29,7	36,1	39,1	29,8
<b>Темп роста, %</b>		49,0%	21,5%	8,2%	
<b>Экспорт, млн. шт.</b>	1,2	2,1	1,8	1,2	0,7
<b>Темп роста, %</b>		73,2%	-13,8%	-35,0%	

*Источник:* на основе данных ФСГС и ФТС РФ, таможенных деклараций

В структуре товарных потоков преобладают поставки на внутренний рынок: на их долю по итогам рассматриваемого периода 2023 года пришлось 97,8% всей произведенной продукции.

В общем объеме уровень поставок печатных плат на внешний рынок является незначительным и рассматривается как возможное направление развития экспортного потенциала производителей печатных плат на рынке.

Далее, рассмотрим вопрос импорта печатных плат. Импортные поставки печатных плат в натуральных показателях на отечественный рынок в рамках

рассматриваемого периода показывают в целом нисходящую динамику, с положительной корректировкой в 2021 году и с достижением по итогам 2022 года минимального показателя импорта. В рассмотрении годовых значений показателя импортных поставок, в течение периода 2019-2022 годов, общий тренд характеризуется сокращением на 6,5%. Сокращение объемов импорта печатных плат вызвано последствиями введенных санкций против России, которые в свою очередь привели к дестабилизации товаропроводящих цепочек и потребителей, а также к значительному росту цен на импортную продукцию.

В рассмотрении показателей 2022 года объем импортных поставок печатных плат составил 83,0 млн. шт., что на 17,1% меньше аналогичного показателя 2021 года, который был равен 100,1 млн. шт. Значительное падение объемов потребления в 2022 году обусловлено влиянием военно-политического кризиса, в результате которого возникли затруднения во взаиморасчетах и логистике.

В оценке текущего временного ряда 2023 года объем импортных поставок печатных плат составил 68,5 млн. шт., что на 16,4% больше показателя аналогичного периода предыдущего года. Интенсификация импортных поставок в рассматриваемом периоде 2023 года связана со значительным увеличением объемности закупок импортной продукции у поставщиков со стороны Китая.

Согласно прогнозным оценкам, объем импорта печатных плат в Россию по итогам 2023 года увеличится на 10,8% к уровню предыдущего года и составит 91,9 млн. шт.

**Основными драйверами импорта** выступают: уровень и состояние платежеспособного спроса основных сегментов потребителей, ценовой диапазон предлагаемой импортной продукции, уровень насыщенности рынка именно отечественной продукцией, общие макроэкономические индикаторы состояния российской экономики и курсовая разница национальной валюты.

**Основное влияние пандемии коронавируса** отразилось в сокращении объемности российского импорта печатных плат в существенных значениях.

**Влияние санкционных мер 2022 года на импорт** проявилось главным образом в сдерживающем воздействии и ограничении потенциала роста объемности импортных поставок, изменении торгового баланса, изменении товарной структуры импортируемой продукции и затруднении расширения номенклатуры импортируемых товаров. Так же введенные санкции оказали значительное влияние на стратегии развития отечественных компаний-импортеров.

Дефицит некоторых товаров, возникший в результате санкционных мер, привел к изменению потребительских предпочтений, переходу на более доступные аналоги и изменению уровня жизни населения в целом.

Принятые ограничения оказали ощутимое влияние на географическую структуру импорта товаров, при этом введение эмбарго в ответ на санкции поспособствовало расширению и укреплению торговых связей как с новыми

странами-партнерами, так и с уже существующими. Главным образом это страны азиатского региона, Латинской Америки и Таможенного союза.

Детальное влияние санкций можно наблюдать в каждом соответствующем разделе данного исследования, в то же время ключевыми моментами являются следующие:

- изменение объемности импортных поставок;
- корректировка сезонности импорта – временной сдвиг;
- структурные изменения в части пула стран-импортеров, изменение значимости каждого региона, усиление позиций;
- структурные изменения в части пула российских регионов, осуществляющих закупку импортной продукции.

Цифровые показатели объемов импорта печатных плат на российский рынок в натуральном выражении, а также параметры роста/сокращения в рамках соответствующих периодов представлены в таблице ниже.

	2019	2020	2021	2022	2023
<b>Импорт, млн. шт.</b>	88,7	84,9	100,1	83,0	91,9
<b>Темп роста, %</b>		-4,3%	17,9%	-17,1%	10,8%
<b>Объемы импорта, январь-сентябрь, млн. шт.</b>	64,2	63,2	72,9	58,8	68,5
<b>Темп роста, янв-сен/янв-сен, %</b>		-1,5%	15,3%	-19,3%	16,4%

*Источник:* на основе данных ФТС РФ, таможенных деклараций

В структуре импортных поставок печатных плат по происхождению доминирует продукция из стран дальнего зарубежья, на долю которой приходилось 99,5% всех поставок по состоянию по итогам рассматриваемого периода 2023 года.

Если говорить о структуре импорта, среди отдельных стран-поставщиков печатных плат в Россию лидируют следующие страны: Китай, Тайвань, Корея (Республика), Сянган (Гонконг). На долю этих стран приходится 99,5% всех поставок по состоянию на 2023 (январь-сентябрь) год. При этом наибольшая доля всех поставок печатных плат приходится на Китай - 97,7% всего импорта в натуральном выражении.

За период 2019-2023 года структура импорта печатных плат претерпела средние изменения:

- Китай - доля выросла на 10,4 процентных пункта;
- Тайвань - доля сократилась на 1,9 процентных пункта;
- Корея (Республика) - доля сократилась на 2,0 процентных пункта;
- Сянган (Гонконг) - доля сократилась на 1,4 процентных пункта;
- доля остальных импортеров сократилась на 5,0 процентных пункта.

В таблице ниже отражены цифровые значения импортных поставок печатных плат по странам в натуральных показателях в годовом эквиваленте.



	2019	2020	2021	2022	2023 (янв-сен)	2022/ 2021
<b>Все страны мира</b>	88,727	84,905	100,111	82,953	68,462	-17,1%
<b>Страны дальнего зарубежья</b>	87,552	84,020	99,262	82,636	68,149	-16,7%
<b>Страны СНГ</b>	1,174	0,885	0,849	0,317	0,313	-62,7%
<b>Китай</b>	77,449	70,596	88,236	79,082	66,854	-10,4%
<b>Тайвань</b>	2,550	1,448	1,007	0,737	0,667	-26,9%
<b>Корея (Республика)</b>	2,316	6,971	6,768	1,282	0,385	-81,1%
<b>Сянган (Гонконг)</b>	1,495	0,842	0,373	0,418	0,194	12,2%
<b>Казахстан</b>	0,098	0,072	0,378	0,065	0,154	-82,7%
<b>Беларусь</b>	1,062	0,787	0,437	0,236	0,128	-46,0%
<b>Армения</b>	0,000	0,000	0,000	0,004	0,025	-
<b>Германия</b>	0,041	0,030	0,060	0,015	0,008	-74,3%
<b>Италия</b>	0,045	0,034	0,039	0,016	0,007	-58,0%
<b>Кыргызстан</b>	0,000	0,009	0,017	0,002	0,006	-90,1%
<b>Австрия</b>	0,003	0,009	0,006	0,003	0,005	-53,1%
<b>Франция</b>	0,004	0,004	0,007	0,002	0,005	-74,5%
<b>Турция</b>	0,002	0,002	0,002	0,005	0,004	156,8%
<b>Соединенные Штаты Америки</b>	0,010	0,015	0,021	0,027	0,003	30,5%
<b>Польша</b>	0,032	0,004	0,011	0,008	0,002	-23,9%
<b>Малайзия</b>	0,003	0,002	0,002	0,001	0,002	-72,4%
<b>Япония</b>	0,216	0,003	0,093	0,002	0,002	-97,7%
<b>Финляндия</b>	0,005	0,006	0,005	0,003	0,001	-50,5%
<b>Швейцария</b>	0,005	0,004	0,005	0,004	0,001	-21,0%
<b>Литва</b>	0,001	0,004	0,003	0,000	0,001	-90,7%
<b>Испания</b>	0,001	0,002	0,002	0,001	0,001	-55,8%
<b>Таиланд</b>	3,195	2,788	2,082	0,990	0,001	-52,4%
<b>Индия</b>	0,005	0,001	0,001	0,000	0,001	-86,6%
<b>Словения</b>	0,001	0,001	0,001	0,000	0,001	-83,0%
<b>Израиль</b>	0,000	0,000	0,001	0,001	0,001	-22,0%
<b>Нидерланды</b>	0,003	0,003	0,002	0,001	0,001	-54,4%
<b>Великобритания</b>	0,058	0,032	0,029	0,001	0,000	-95,9%
<b>Мексика</b>	0,003	0,007	0,005	0,000	0,000	-97,3%
<b>Филиппины</b>	0,021	0,000	0,000	0,000	0,000	62,9%
<b>Македония</b>	0,000	0,001	0,007	0,003	0,000	-65,2%
<b>Дания</b>	0,001	0,001	0,001	0,000	0,000	-29,3%
<b>Чехия</b>	0,005	0,003	0,003	0,002	0,000	-24,4%
<b>Словакия</b>	0,006	0,003	0,005	0,002	0,000	-60,4%
<b>Болгария</b>	0,006	0,003	0,002	0,001	0,000	-30,1%

	2019	2020	2021	2022	2023 (янв-сен)	2022/ 2021
Бельгия	0,002	0,002	0,003	0,001	0,000	-79,8%
Канада	0,001	0,001	0,000	0,000	0,000	-82,2%
Румыния	0,001	0,000	0,000	0,000	0,000	-61,8%
Швеция	0,019	0,001	0,033	0,012	0,000	-62,9%
Венгрия	0,012	0,010	0,008	0,001	0,000	-81,5%
Сербия	0,011	0,008	0,009	0,004	0,000	-54,7%
Индонезия	0,016	0,000	0,000	0,000	0,000	-74,7%
Сингапур	0,001	0,001	0,000	0,001	0,000	55,8%
Вьетнам	0,000	0,001	0,007	0,000	0,000	-99,5%
Объединенные Арабские Эмираты	0,000	1,145	0,064	0,000	0,000	-
Египет	0,000	0,000	0,020	0,000	0,000	-
Пакистан	0,000	0,000	0,006	0,000	0,000	-
Страны ЕС	0,003	0,003	0,000	0,000	0,000	-

Источник: на основе данных ФТС РФ, таможенных деклараций

Наибольший объем поставок зарубежной продукции в натуральном выражении идет в Центральный федеральный округ, на долю которого по итогам рассматриваемого периода 2023 года пришлось 40,9% всего импорта печатных плат, Сибирский федеральный округ с долевым эквивалентом в 24,9%, Северо-Западный федеральный округ с долевым показателем в 24,3%.

Цифровые показатели объемов импорта печатных плат на российский рынок в оценке федеральных округов, а также параметры долевого эквивалента каждого из регионов в общей структуре импорта по натуральным показателям представлены в таблице ниже.

Наименование	2022 год		2023 (янв-сен) год	
	тыс. шт.	%	тыс. шт.	%
Центральный федеральный округ	38 193,2	46,0%	28 011,9	40,9%
Сибирский федеральный округ	16 655,0	20,1%	17 031,7	24,9%
Северо-Западный федеральный округ	18 437,6	22,2%	16 667,7	24,3%
Приволжский федеральный округ	4 931,6	5,9%	3 630,8	5,3%
Северо-Кавказский федеральный округ	2 315,4	2,8%	1 424,3	2,1%
Уральский федеральный округ	510,1	0,6%	739,6	1,1%
Дальневосточный федеральный округ	1 645,4	2,0%	708,2	1,0%
Южный федеральный округ	264,4	0,3%	247,9	0,4%

Источник: на основе данных ФТС РФ, таможенных деклараций Среди регионов России лидируют Москва, при этом долевая составляющая соответствовала показателю в 28,3% от всего импорта печатных плат в натуральном выражении, Новосибирская область (24,3%), Санкт-Петербург (21,9%).

Цифровые показатели объемов импорта печатных плат на российский рынок в оценке субъектов федеральных округов, а также параметры долевых эквивалентов каждого из регионов в общей структуре импорта по натуральным показателям представлены в таблице ниже.

Наименование	2022 год		2023 (янв-сен) год	
	тыс. шт.	%	тыс. шт.	%
Москва	22 355,0	26,9%	19 349,9	28,3%
Новосибирская область	16 040,0	19,3%	16 611,4	24,3%
Санкт-Петербург	15 063,8	18,2%	14 991,9	21,9%
Московская область	8 054,8	9,7%	5 042,8	7,4%
Калужская область	3 360,0	4,1%	1 072,6	1,6%
Ставропольский край	2 315,1	2,8%	1 424,3	2,1%
Республика Татарстан	1 858,9	2,2%	924,2	1,3%
Ленинградская область	1 455,9	1,8%	1 044,5	1,5%
Республика Мордовия	1 039,1	1,3%	1 150,3	1,7%
Владимирская область	1 180,0	1,4%	801,7	1,2%
Приморский край	1 334,0	1,6%	598,2	0,9%
Калининградская область	1 531,5	1,8%	198,9	0,3%
Ульяновская область	728,9	0,9%	697,3	1,0%
Тульская область	914,4	1,1%	461,4	0,7%
Свердловская область	440,8	0,5%	592,7	0,9%
Самарская область	752,1	0,9%	272,8	0,4%
Томская область	596,4	0,7%	372,7	0,5%
Ярославская область	998,2	1,2%	0,2	0,0%
Рязанская область	294,7	0,4%	489,4	0,7%
Псковская область	308,1	0,4%	280,3	0,4%
Орловская область	349,0	0,4%	213,7	0,3%
Нижегородская область	334,4	0,4%	179,6	0,3%
Ростовская область	236,4	0,3%	231,2	0,3%
Брянская область	246,3	0,3%	184,1	0,3%
Смоленская область	173,5	0,2%	196,5	0,3%
Хабаровский край	287,5	0,3%	99,0	0,1%
Тверская область	126,0	0,2%	170,3	0,2%
Удмуртская Республика	113,7	0,1%	167,5	0,2%
Вологодская область	77,5	0,1%	146,7	0,2%
Челябинская область	69,2	0,1%	104,2	0,2%
Воронежская область	125,0	0,2%	11,0	0,0%
Пермский край	41,9	0,1%	73,6	0,1%

Наименование	2022 год		2023 (январь-сентябрь) год	
	тыс. шт.	%	тыс. шт.	%
Чувашская Республика	24,4	0,0%	61,0	0,1%
Саратовская область	5,9	0,0%	69,1	0,1%
Тюменская область	0,1	0,0%	40,6	0,1%
Волгоградская область	20,1	0,0%	13,4	0,0%
Амурская область	22,2	0,0%	10,6	0,0%
Красноярский край	2,1	0,0%	25,5	0,0%
Кировская область	7,9	0,0%	17,0	0,0%
Пензенская область	6,3	0,0%	16,1	0,0%
Алтайский край	8,9	0,0%	12,7	0,0%
Ивановская область	0,0	0,0%	17,8	0,0%
Республика Башкортостан	17,8	0,0%	0,6	0,0%
Липецкая область	15,7	0,0%	0,4	0,0%
Иркутская область	6,0	0,0%	4,0	0,0%
Краснодарский край	5,9	0,0%	3,2	0,0%
Омская область	1,6	0,0%	5,3	0,0%
Архангельская область	0,0	0,0%	5,4	0,0%
Курганская область	0,0	0,0%	2,1	0,0%
Республика Марий Эл	0,0	0,0%	1,6	0,0%
Севастополь	1,8	0,0%	0,0	0,0%
Забайкальский край	1,4	0,0%	0,0	0,0%
Белгородская область	0,6	0,0%	0,0	0,0%
Республика Карелия	0,5	0,0%	0,0	0,0%
Оренбургская область	0,4	0,0%	0,0	0,0%
Сахалинская область	0,2	0,0%	0,2	0,0%
Республика Бурятия	0,1	0,0%	0,2	0,0%
Новгородская область	0,2	0,0%	0,1	0,0%
Республика Северная Осетия-Алания	0,2	0,0%	0,0	0,0%
Астраханская область	0,1	0,0%	0,0	0,0%
Кемеровская область	0,1	0,0%	0,0	0,0%
Курская область	0,1	0,0%	0,0	0,0%

*Источник:* на основе данных ФТС РФ, таможенных деклараций

В структуре импорта печатных плат по ассортиментным группам наибольшую долю занимают печатные платы многослойные с долевым эквивалентом 64,2%, или 44,0 млн. шт. в натуральном выражении. Затем в порядке убывания долевого эквивалента следуют печатные платы, состоящие только из токопроводящих элементов и контактов, которые занимают 29,3% (20,0 млн. шт.) общего импорта по итогам рассматриваемого периода 2023 года.

Стоит отметить увеличение долевой составляющей по ассортиментной группе печатные платы многослойные по итогам 2019-2023 годов на 2,1 процентных пункта на фоне сокращения доли печатных плат, состоящих только из токопроводящих элементов и контактов.

Цифровые показатели объемов импорта печатных плат по ассортиментным группам в натуральном выражении на российский рынок в оценке 2019-2023 годов, а также параметры динамики роста/сокращения по итогам 2022/2021 годов представлены в таблице ниже.

	2019	2020	2021	2022	2023 (янв-сен)	2022/ 2021
<b>Печатные платы многослойные</b>	55,1	55,7	66,6	52,1	44,0	-21,7%
<b>Печатные платы, состоящие только из токопроводящих элементов и контактов</b>	29,7	26,6	29,1	26,7	20,0	-8,3%
<b>Печатные платы с прочими пассивными элементами</b>	3,9	2,6	4,4	4,1	4,5	-6,4%
<b>Итого</b>	88,7	84,9	100,1	83,0	68,5	-17,1%

*Источник:* на основе данных ФТС РФ, таможенных деклараций

Стоимостная оценка импортных поставок печатных плат на российский рынок в рамках исследуемого периода показывает увеличение с достижением по итогам последнего года максимальных значений импорта. В рассмотрении годовых значений показателя стоимостной оценки импорта, в течение периода 2019-2022 годов, общий тренд характеризуется увеличением на 51,6%, что непосредственно обусловлено ростом средних контрактных цен на импортируемую продукцию.

В рассмотрении показателей 2022 года объем импортных поставок печатных плат в стоимостном выражении составил 190,3 млн. долл., что на 7,0% больше аналогичного показателя 2021 года, который составил 177,9 млн. долл. Данная динамика по результатам 2022 года вызвана значительным увеличением ценовых параметров на печатные платы.

В оценке текущего временного ряда 2023 года объем импортных поставок печатных плат в стоимостном выражении составил 166,1 млн. долл., что на 31,0% больше показателя аналогичного периода предыдущего года. Стоимостная оценка импорта в рассматриваемом периоде 2023 года демонстрирует большой темп роста в сопоставлении с физическими

объемами, что связано с корректировкой ценовых индикаторов на ввозимые печатные платы в сторону увеличения.

По прогнозным оценкам, объем импорта печатных плат в стоимостном выражении в России в 2023 году увеличится на 21,1% в сравнении с 2022 годом и составит 230,4 млн. долл.

Детализированные аспекты санкционных ограничений можно наблюдать в соответствующем разделе данного материала, в то же время генеральными моментами являются такие как:

- коррекция объемности импортных поставок;
- изменение состава в части пула мировых импортеров, корректив значимости каждого региона, перераспределение позиций;
- конфигурирование состава в части пула российских регионов, осуществляющих закупку продукции из-за рубежа;
- корректировка ценовых индикаторов на продукцию при ввозе на внутренний рынок.

Цифровые показатели объемов импорта печатных плат на российский рынок в стоимостной оценке, а также параметры темпов роста/сокращения по итогам 2019-2023 годов представлены в таблице ниже.

	2019	2020	2021	2022	2023
<b>Импорт, млн. долл.</b>	125,6	130,0	177,9	190,3	230,4
<b>Темп роста, %</b>		3,5%	36,9%	7,0%	21,1%
<b>Объемы импорта, январь-сентябрь, млн. долл.</b>	89,1	96,6	124,4	126,8	166,1
<b>Темп роста, янв-сен/янв-сен, %</b>		8,5%	28,8%	1,9%	31,0%

К наиболее крупным поставщикам печатных плат в Россию в стоимостном выражении относятся те же страны, но с некоторыми различиями в долях: Китай, Тайвань, Казахстан, Сянган (Гонконг). Совокупно перечисленные страны делят 97,6% импортных поставок печатных плат в Россию в стоимостном выражении. При этом наибольшая доля всего импорта печатных плат приходится на Китай - 86,5% всех поставок по итогам 2023 (январь-сентябрь) года.

Как показывает статистика, за 2019-2023 года структура импорта печатных плат в стоимостном выражении в отличие от структуры импорта в натуральном выражении претерпела слабые изменения:

- Китай - доля выросла на 3,3 процентных пункта;
- Тайвань - доля выросла на 3,9 процентных пункта;
- Казахстан - доля выросла на 0,4 процентных пункта;
- Сянган (Гонконг) - доля сократилась на 0,1 процентных пункта;
- доля остальных стран сократилась на 7,6 процентных пункта.

В таблице ниже отражены цифровые значения импортных поставок печатных плат по странам в стоимостных показателях в годовом эквиваленте.

	2019	2020	2021	2022	2023 (янв-сен)	2022/ 2021
<b>Все страны мира</b>	125,553	129,976	177,909	190,300	166,104	7,0%
<b>Страны дальнего зарубежья</b>	123,940	128,510	176,883	188,820	162,876	6,7%
<b>Страны СНГ</b>	1,613	1,467	1,026	1,480	3,228	44,3%
<b>Китай</b>	104,492	106,239	151,328	171,932	143,747	13,6%
<b>Тайвань</b>	6,170	3,963	4,751	8,371	14,663	76,2%
<b>Казахстан</b>	0,843	0,289	0,051	0,670	1,849	-
<b>Сянган (Гонконг)</b>	1,501	0,961	1,261	1,624	1,817	28,8%
<b>Беларусь</b>	0,546	0,535	0,471	0,464	1,131	-1,6%
<b>Корея (Республика)</b>	2,703	8,475	8,872	2,011	0,832	-77,3%
<b>Соединенные Штаты Америки</b>	0,610	1,026	1,362	1,219	0,376	-10,5%
<b>Германия</b>	0,815	0,779	1,210	0,383	0,329	-68,3%
<b>Армения</b>	0,000	0,001	0,001	0,163	0,194	-
<b>Италия</b>	0,269	0,232	0,392	0,178	0,183	-54,5%
<b>Австрия</b>	0,061	0,124	0,182	0,088	0,122	-51,8%
<b>Малайзия</b>	0,128	0,065	0,133	0,045	0,094	-66,4%
<b>Франция</b>	0,150	0,156	0,244	0,051	0,088	-79,1%
<b>Македония</b>	0,009	0,073	0,330	0,244	0,073	-26,2%
<b>Турция</b>	0,020	0,022	0,021	0,068	0,068	215,4%
<b>Финляндия</b>	0,131	0,135	0,163	0,083	0,064	-48,8%
<b>Кыргызстан</b>	0,002	0,439	0,328	0,058	0,054	-82,4%
<b>Швейцария</b>	0,561	0,301	0,625	0,181	0,054	-71,0%
<b>Япония</b>	0,618	0,246	0,497	0,098	0,054	-80,2%
<b>Индия</b>	0,113	0,113	0,030	0,021	0,053	-28,8%
<b>Нидерланды</b>	0,053	0,145	0,090	0,042	0,036	-53,7%
<b>Израиль</b>	0,004	0,005	0,013	0,076	0,032	464,0%
<b>Словения</b>	0,007	0,016	0,016	0,068	0,029	315,9%
<b>Польша</b>	0,052	0,013	0,055	0,028	0,021	-48,8%
<b>Великобритания</b>	1,394	0,725	1,290	0,096	0,017	-92,6%
<b>Швеция</b>	0,127	0,062	0,120	0,039	0,015	-67,8%
<b>Ирландия</b>	0,007	0,018	0,017	0,000	0,014	-
<b>Филиппины</b>	0,138	0,008	0,014	0,014	0,010	5,4%
<b>Испания</b>	0,023	0,027	0,041	0,043	0,009	6,8%
<b>Бельгия</b>	0,043	0,062	0,088	0,024	0,009	-73,0%
<b>Мексика</b>	0,021	0,043	0,012	0,002	0,009	-84,7%
<b>Канада</b>	0,089	0,139	0,094	0,050	0,007	-46,2%

	2019	2020	2021	2022	2023 (янв-сен)	2022/ 2021
<b>Индонезия</b>	0,044	0,067	0,030	0,021	0,007	-30,3%
<b>Дания</b>	0,048	0,028	0,023	0,008	0,006	-67,1%
<b>Румыния</b>	0,073	0,031	0,018	0,009	0,006	-49,1%
<b>Сербия</b>	0,013	0,010	0,013	0,085	0,005	558,0%
<b>Литва</b>	0,008	0,013	0,009	0,002	0,004	-72,5%
<b>Объединенные Арабские Эмираты</b>	0,000	0,908	0,047	0,011	0,003	-76,2%
<b>Таиланд</b>	2,624	2,344	1,951	1,279	0,003	-34,4%
<b>Словакия</b>	0,052	0,024	0,049	0,021	0,002	-57,5%
<b>Южно- Африканская Республика</b>	0,006	0,000	0,000	0,003	0,002	-
<b>Венгрия</b>	0,064	0,066	0,062	0,016	0,002	-74,9%
<b>Чехия</b>	0,115	0,072	0,049	0,035	0,002	-28,0%
<b>Болгария</b>	0,044	0,022	0,031	0,013	0,002	-59,3%
<b>Мальдивы</b>	0,000	0,000	0,000	0,000	0,001	-
<b>Бразилия</b>	0,001	0,005	0,001	0,001	0,001	-1,7%
<b>Греция</b>	0,001	0,000	0,003	0,001	0,001	-76,7%
<b>Австралия</b>	0,000	0,000	0,001	0,000	0,001	-
<b>Хорватия</b>	0,001	0,000	0,000	0,000	0,001	-
<b>Сингапур</b>	0,030	0,020	0,003	0,023	0,001	576,3%
<b>Португалия</b>	0,001	0,002	0,001	0,001	0,000	-8,4%
<b>Аргентина</b>	0,002	0,000	0,000	0,000	0,000	166,8%
<b>Вьетнам</b>	0,008	0,005	0,011	0,000	0,000	-96,5%
<b>Молдова</b>	0,002	0,000	0,000	0,000	0,000	-
<b>Грузия</b>	0,000	0,000	0,001	0,000	0,000	-
<b>Пакистан</b>	0,000	0,000	0,010	0,000	0,000	-
<b>Эквадор</b>	0,018	0,000	0,000	0,000	0,000	-
<b>Мальта</b>	0,000	0,001	0,000	0,000	0,000	-
<b>Египет</b>	0,002	0,000	0,021	0,000	0,000	-

*Источник:* на основе данных ФТС РФ, таможенных деклараций

В стоимостном выражении лидерами по покупке импортной продукции среди федеральных округов являются Центральный федеральный округ, на территорию которого по итогам рассматриваемого периода 2023 года было ввезено 47,7% всего импорта печатных плат, Северо-Западный федеральный округ с долевым эквивалентом в 29,5%, Сибирский федеральный округ с долевым показателем в 16,1%.

Цифровые показатели объемов импорта печатных плат на российский рынок в оценке округов-потребителей, а также параметры долевого эквивалента представлены в таблице ниже.



Наименование	2022 год		2023 (янв-сен) год	
	тыс.	%	тыс.	%
	долл.		долл.	
Центральный федеральный округ	93 912,7	49,3%	79 186,5	47,7%
Северо-Западный федеральный округ	54 733,7	28,8%	48 951,6	29,5%
Сибирский федеральный округ	27 999,5	14,7%	26 700,4	16,1%
Приволжский федеральный округ	6 878,0	3,6%	6 747,2	4,1%
Северо-Кавказский федеральный округ	3 229,6	1,7%	1 594,8	1,0%
Уральский федеральный округ	2 069,6	1,1%	2 170,0	1,3%
Дальневосточный федеральный округ	1 232,6	0,6%	488,1	0,3%
Южный федеральный округ	244,3	0,1%	265,4	0,2%

Источник: на основе данных ФТС РФ, таможенных деклараций

Крупнейшими регионами-потребителями импортной продукции являются Москва с долевой составляющей в 37,5% от всего импорта в стоимостном выражении по итогам рассматриваемого периода 2023 года, Санкт-Петербург (28,2%), Новосибирская область (15,6%).

Цифровые показатели объемов импорта печатных плат на российский рынок в оценке субъектов РФ, а также параметры долевых эквивалентов представлены в таблице ниже.

Наименование	2022 год		2023 (янв-сен) год	
	тыс.	%	тыс.	%
	долл.		долл.	
Москва	61 324,3	32,2%	62 302,6	37,5%
Санкт-Петербург	49 336,9	25,9%	46 816,3	28,2%
Новосибирская область	27 231,0	14,3%	25 844,4	15,6%
Московская область	12 131,7	6,4%	8 434,5	5,1%
Тульская область	7 610,8	4,0%	2 292,8	1,4%
Калужская область	6 223,4	3,3%	2 526,3	1,5%
Республика Татарстан	2 908,2	1,5%	2 446,1	1,5%
Ставропольский край	3 226,5	1,7%	1 594,8	1,0%
Свердловская область	1 955,8	1,0%	2 003,7	1,2%
Калининградская область	3 431,8	1,8%	439,2	0,3%
Нижегородская область	1 255,0	0,7%	1 505,1	0,9%
Ленинградская область	1 330,3	0,7%	910,7	0,5%
Владимирская область	1 377,4	0,7%	856,4	0,5%
Пермский край	929,0	0,5%	956,6	0,6%
Воронежская область	1 850,7	1,0%	122,8	0,1%
Смоленская область	423,8	0,2%	998,1	0,6%

Наименование	2022 год		2023 (янв-сен) год	
	тыс.	%	тыс.	%
	долл.		долл.	
Республика Мордовия	605,3	0,3%	485,8	0,3%
Приморский край	748,7	0,4%	330,2	0,2%
Ярославская область	1 119,6	0,6%	5,9	0,0%
Ульяновская область	505,4	0,3%	526,5	0,3%
Орловская область	595,5	0,3%	435,7	0,3%
Рязанская область	431,5	0,2%	568,1	0,3%
Псковская область	492,6	0,3%	513,5	0,3%
Томская область	368,3	0,2%	433,7	0,3%
Брянская область	413,6	0,2%	337,3	0,2%
Тверская область	356,2	0,2%	248,4	0,1%
Самарская область	339,4	0,2%	234,7	0,1%
Хабаровский край	429,6	0,2%	97,5	0,1%
Красноярский край	209,5	0,1%	237,8	0,1%
Ростовская область	208,7	0,1%	211,3	0,1%
Вологодская область	126,9	0,1%	258,0	0,2%
Удмуртская Республика	80,5	0,0%	279,1	0,2%
Челябинская область	99,2	0,1%	134,9	0,1%
Омская область	80,9	0,0%	81,9	0,0%
Иркутская область	57,4	0,0%	63,9	0,0%
Республика Башкортостан	87,7	0,0%	29,1	0,0%
Оренбургская область	73,8	0,0%	33,2	0,0%
Саратовская область	11,9	0,0%	87,1	0,1%
Сахалинская область	48,0	0,0%	46,5	0,0%
Пензенская область	35,9	0,0%	48,9	0,0%
Кировская область	25,5	0,0%	52,9	0,0%
Чувашская Республика	20,3	0,0%	45,3	0,0%
Липецкая область	36,7	0,0%	30,0	0,0%
Кемеровская область	49,8	0,0%	4,0	0,0%
Краснодарский край	13,9	0,0%	32,3	0,0%
Волгоградская область	18,0	0,0%	21,6	0,0%
Алтайский край	2,7	0,0%	34,7	0,0%
Тюменская область	3,8	0,0%	25,8	0,0%
Ивановская область	4,5	0,0%	24,0	0,0%
Республика Марий Эл	0,2	0,0%	17,0	0,0%
Новгородская область	6,3	0,0%	9,3	0,0%
Амурская область	2,5	0,0%	7,6	0,0%
Ханты-Мансийский автономный округ	10,7	0,0%	0,0	0,0%
Курская область	6,3	0,0%	0,1	0,0%
Курганская область	0,0	0,0%	5,5	0,0%
Костромская область	6,1	0,0%	0,1	0,0%
Камчатский край	0,3	0,0%	4,6	0,0%
Республика Коми	5,6	0,0%	0,0	0,0%

Наименование	2022 год		2023 (янв-сен) год	
	тыс.	%	тыс.	%
	долл.		долл.	
Архангельская область	0,0	0,0%	4,6	0,0%
Республика Саха (Якутия)	3,2	0,0%	1,6	0,0%
Белгородская область	0,5	0,0%	3,4	0,0%
Севастополь	3,5	0,0%	0,0	0,0%
Республика Северная Осетия-Алания	3,1	0,0%	0,0	0,0%
Республика Карелия	2,0	0,0%	0,0	0,0%
Мурманская область	1,4	0,0%	0,0	0,0%
Астраханская область	0,1	0,0%	0,2	0,0%
Республика Бурятия	0,1	0,0%	0,0	0,0%
Забайкальский край	0,1	0,0%	0,0	0,0%

*Источник:* на основе данных ФТС РФ, таможенных деклараций

В стоимостной структуре импорта печатных плат по ассортиментным группам наибольшую долю занимают печатные платы многослойные с долевым эквивалентом 75,3%, или 125,1 млн. долл. в денежном выражении. Затем в порядке убывания долевого эквивалента следуют печатные платы, состоящие только из токопроводящих элементов и контактов, которые занимают 14,1% (23,4 млн. долл.) общего импорта в стоимостном выражении по итогам рассматриваемого периода 2023 года.

Цифровые показатели объемов импорта печатных плат по ассортиментным группам в стоимостном выражении на российский рынок в оценке 2019-2023 годов, а также параметры динамики роста/сокращения по итогам 2022/2021 годов представлены в таблице ниже.

	2019	2020	2021	2022	2023 (янв-сен)	2022/ 2021
<b>Печатные платы многослойные</b>	87,7	96,0	134,1	143,7	125,1	7,2%
<b>Печатные платы, состоящие только из токопроводящих элементов и контактов</b>	29,6	26,5	32,3	32,0	23,4	-1,1%
<b>Печатные платы с прочими пассивными элементами</b>	8,2	7,5	11,5	14,6	17,6	26,5%
<b>Итого</b>	125,6	130,0	177,9	190,3	166,1	7,0%

*Источник:* на основе данных ФТС РФ, таможенных деклараций

*О динамике средних цен на импортируемую продукцию.*

Период январь-сентябрь 2023 года охарактеризовался ростом цен на импортную продукцию. Средние импортные цены на печатные платы выросли на 132,14 долл./тыс. шт. (5,8%): с 2294,08 в 2022 году до 2426,22 в 2023 (январь-сентябрь) году.

Среди десяти крупнейших импортеров самые низкие цены по итогам рассматриваемого периода 2023 года наблюдаются на продукцию, импортируемую из таких стран, как:

- Китай - 2150,16 долл./тыс. шт.;
- Корея (Республика) - 2160,22 долл./тыс. шт.;
- Армения - 7648,07 долл./тыс. шт.

Самая дорогая импортная продукция поступает из следующих стран:

- Германия - 42537,31 долл./тыс. шт.;
- Италия - 26902,77 долл./тыс. шт.;
- Тайвань - 21987,07 долл./тыс. шт.

Цифровые показатели средних цен импорта на рынке печатных плат в разрезе основных стран-импортеров представлены в таблице ниже.

	2019	2020	2021	2022	2023 (янв-сен)	2022 к 2021
<b>Среднее значение</b>	1415,05	1530,85	1777,12	2294,08	2426,22	132,14
<b>Китай</b>	1349,17	1504,88	1715,03	2174,11	2150,16	-23,94
<b>Тайвань</b>	2419,34	2736,76	4717,02	11365,95	21987,07	10621,12
<b>Корея (Республика)</b>	1166,85	1215,72	1310,82	1568,31	2160,22	591,91
<b>Сянган (Гонконг)</b>	1003,79	1141,03	3382,92	3882,87	9361,68	5478,82
<b>Казахстан</b>	8589,50	4019,96	134,28	10233,35	11985,85	1752,50
<b>Беларусь</b>	514,54	680,16	1077,60	1963,76	8835,04	6871,28
<b>Армения</b>	-	3487,87	5087,31	37905,92	7648,07	-30257,85
<b>Германия</b>	19862,16	26395,42	20185,46	24881,31	42537,31	17656,00
<b>Италия</b>	6020,38	6790,64	10049,37	10867,62	26902,77	16035,14
<b>Кыргызстан</b>	85602,67	51463,51	18766,38	33204,80	9434,34	-23770,46

*Источник:* на основе данных ФТС РФ, таможенных деклараций

Средние импортные цены на рынке печатных плат в рублевом эквиваленте в разрезе основных стран-импортеров представлены в таблице ниже.

	2019	2020	2021	2022	2023 (янв-сен)	2022 к 2021
<b>Среднее значение</b>	91603	110402	130470	157328	199112	41784
<b>Китай</b>	87339	97419	111023	140741	139191	-1550
<b>Тайвань</b>	156616	177165	305356	735776	1423335	687559

	2019	2020	2021	2022	2023 (янв-сен)	2022 к 2021
<b>Корея (Республика)</b>	75536	78700	84856	101525	139842	38317
<b>Сянган (Гонконг)</b>	64980	73865	218994	251358	606029	354672
<b>Казахстан</b>	556042	260233	8693	662457	775905	113448
<b>Беларусь</b>	33309	44030	69758	127124	571937	444813
<b>Армения</b>	-	225787	329328	2453843	495098	- 1958745
<b>Германия</b>	1285778	1708710	1306707	1610694	2753656	1142962
<b>Италия</b>	389730	439593	650547	703517	1741553	1038036
<b>Кыргызстан</b>	5541496	3331495	1214843	2149515	610733	- 1538783

*Источник:* на основе данных ФТС РФ, таможенных деклараций

*Экспорт печатных плат.* После значительного увеличения в 2020 году, в рамках последующих периодов экспортные поставки печатных плат российского производства в натуральных показателях на рынки зарубежных стран показывают нисходящую динамику с достижением по итогам 2022 года минимального показателя экспорта. В рассмотрении годовых значений показателя экспортных поставок, в течение периода 2019-2022 годов, общий тренд характеризуется снижением на 3,0%, что главным образом связано с снижением спроса на печатные платы российского производства на мировом рынке.

В рассмотрении показателей 2022 года объем экспортных поставок печатных плат составил 1,154 млн. шт., что на 35,0% меньше аналогичного показателя 2021 года, который был равен 1,776 млн. шт. Введенные санкционные ограничения отразились в нарушении логистических цепочек и падении объемов экспортных отгрузок в такие страны как Беларусь, Литва, Украина, Вьетнам и Польша.

В оценке индикаторов 2023 года российскими компаниями было экспортировано 0,662 млн. шт. продукции, что ниже аналогичного показателя прошлого года на 32,1%. Данная тенденция вызвана продолжением снижения потребления продукции российского производства в зарубежных странах.

По оценочным данным объем экспорта печатных плат из России в 2023 году составит 0,933 млн. шт., что ниже на 19,2% итоговых результатов предыдущего года.

*Влияние санкционных мер 2022 года на экспортную активность* отразилось в сдерживающем воздействии на отечественную экономику и ограничении потенциала роста за счет снижения внешнего спроса, что привело к изменению товарной структуры экспортируемой продукции; снижению диверсификации отечественного экспорта; затруднению расширения номенклатуры экспортируемых товаров в результате синергетического

эффекта внешних негативных факторов; снижению результативности внешней торговли России, снижению валютной выручки и, как следствие, снижению рентабельности и маржинальности в экспортоориентированных отраслях.

Санкции также привели к смене приоритетов государства и переориентации экспортных потоков на новые рынки с вектором развития внешней торговли в сторону развивающихся стран, прежде всего азиатского региона, при этом становление и расширение связей с новыми партнерами поспособствовало развитию российских платежных и финансово-информационных систем.

Ключевыми моментами анализа влияния санкций являются следующие:

- колебание объемности экспортных поставок;
- смещение сезонности экспорта – временной сдвиг;
- структурные изменения в части пула стран-экспортеров, изменение значимости каждого региона, усиление позиций;
- структурные изменения в части пула российских регионов, осуществляющих отгрузку экспортной продукции.

Среди отдельных импортеров печатных плат из России лидируют следующие страны: Беларусь, Казахстан, Азербайджан, Турция, Узбекистан, Армения, Кыргызстан. На долю этих стран приходится 99,8% всех экспортных операций по состоянию на 2023 (январь-сентябрь) год. При этом наибольшая доля поставок печатных плат с российской территории приходится на Беларусь - 75,2% всего экспорта в натуральном выражении.

Из приведенных данных видно, что за 2019-2023 года структура экспорта печатных плат претерпела заметные изменения:

- Беларусь - доля выросла на 44,2 процентных пункта;
- Казахстан - доля выросла на 10,9 процентных пункта;
- Азербайджан - доля выросла на 4,4 процентных пункта;
- Турция - доля сократилась на 0,1 процентных пункта;
- Узбекистан - доля выросла на 0,5 процентных пункта;
- Армения - доля сократилась на 0,3 процентных пункта;
- Кыргызстан - доля выросла на 0,2 процентных пункта;
- доля остальных стран-потребителей сократилась на 59,7 процентных пункта.

В таблице отражены цифровые значения экспортных поставок печатных плат по странам в натуральных показателях в годовом эквиваленте.

	2019	2020	2021	2022	2023 (январь-сентябрь)	2022/ 2021
<b>Все страны мира</b>	1,190	2,060	1,776	1,154	0,662	-35,0%
<b>Страны СНГ</b>	0,502	0,577	1,179	1,130	0,655	-4,1%
<b>Страны дальнего зарубежья</b>	0,688	1,484	0,597	0,024	0,007	-96,0%
<b>Беларусь</b>	0,370	0,402	0,747	0,496	0,498	-33,6%

	2019	2020	2021	2022	2023 (янв-сен)	2022/ 2021
<b>Казахстан</b>	0,069	0,082	0,128	0,214	0,110	67,6%
<b>Азербайджан</b>	0,019	0,033	0,037	0,028	0,039	-22,5%
<b>Турция</b>	0,011	0,018	0,015	0,015	0,006	1,5%
<b>Узбекистан</b>	0,000	0,000	0,001	0,000	0,004	-70,5%
<b>Армения</b>	0,009	0,002	0,004	0,006	0,003	38,3%
<b>Кыргызстан</b>	0,000	0,001	0,197	0,376	0,001	91,2%
<b>Грузия</b>	0,002	0,001	0,002	0,000	0,001	-86,3%
<b>Таджикистан</b>	0,000	0,000	0,000	0,000	0,000	-
<b>Индия</b>	0,003	0,001	0,002	0,002	0,000	-16,5%
<b>Алжир</b>	0,000	0,000	0,000	0,000	0,000	-83,1%
<b>Китай</b>	0,001	0,000	0,001	0,001	0,000	1,8%
<b>Объединенные Арабские Эмираты</b>	0,000	0,000	0,000	0,000	0,000	313,1%
<b>Сянган (Гонконг)</b>	0,045	0,031	0,018	0,000	0,000	-
<b>Соединенные Штаты Америки</b>	0,003	0,000	0,000	0,000	0,000	-86,2%
<b>Колумбия</b>	0,000	0,000	0,000	0,000	0,000	-
<b>Чехия</b>	0,000	0,000	0,001	0,000	0,000	-90,5%
<b>Вьетнам</b>	0,000	0,001	0,144	0,002	0,000	-98,9%
<b>Финляндия</b>	0,005	0,006	0,002	0,000	0,000	-74,3%
<b>Великобритания</b>	0,000	0,075	0,000	0,000	0,000	-88,2%
<b>Словакия</b>	0,000	0,000	0,001	0,000	0,000	-
<b>Венгрия</b>	0,019	0,019	0,000	0,000	0,000	-
<b>Литва</b>	0,535	1,133	0,179	0,000	0,000	-99,8%
<b>Болгария</b>	0,003	0,000	0,000	0,000	0,000	-
<b>Египет</b>	0,001	0,000	0,050	0,000	0,000	-
<b>Тайвань</b>	0,001	0,000	0,000	0,000	0,000	-
<b>Франция</b>	0,000	0,004	0,000	0,000	0,000	-98,0%
<b>Корея (Республика)</b>	0,009	0,171	0,000	0,000	0,000	-
<b>Куба</b>	0,002	0,000	0,000	0,000	0,000	-
<b>Эстония</b>	0,000	0,000	0,001	0,000	0,000	-75,6%
<b>Ливан</b>	0,003	0,000	0,000	0,000	0,000	-
<b>Молдова</b>	0,004	0,003	0,005	0,003	0,000	-47,2%
<b>Нидерланды</b>	0,001	0,006	0,000	0,000	0,000	-
<b>Германия</b>	0,041	0,000	0,001	0,000	0,000	-75,1%
<b>Индонезия</b>	0,000	0,003	0,000	0,000	0,000	-20,0%

*Источник:* на основе данных ФТС РФ, таможенных деклараций

Как итог, следует разделять процесс производства печатных плат и монтаж печатных плат. В монтаже импортозамещение уже происходит — очень многие заказчики из тех, кто раньше заказывал монтаж и сборку в Китае сейчас активно переводят заказы либо на мощности российских контрактных

производителей, либо инвестируют в собственные производственные участки. Ни по стоимости, ни по качеству российские контрактные производители уже не уступают китайским, а по срокам значительно их превосходят.

Что же касается производства печатных плат, то только рыночными методами соревноваться в стоимости с китайскими производителями пока невозможно. Сказывается целый ряд факторов, но прежде всего надо говорить об экономическом эффекте масштаба. Российский рынок печатных плат — это менее 0.4% мирового производства, в то время как Китайский — более 50%. К тому же в России исторически большое количество очень небольших заводов, что также не позволяет говорить об оптимизации себестоимости. Интересный факт — в России больше заводов по производству печатных плат, чем на Тайване, но при этом Тайвань — это 12.5% мирового производства плат. Завод по производству печатных плат на Тайване, в среднем, в 40 раз больше среднего завода в России.

Для осуществления реальной ценовой конкуренции с китайскими производителями в сегменте mass-production, нужно строить завод с очень высоким уровнем автоматизации процессов и с производственной мощностью — не менее 30-40 миллионов квадратных дециметров в год. Пока на такой объём в стране попросту нет заказов. Таким образом, для того, чтобы можно было полноценно говорить о конкуренции с Китаем, российскому рынку нужно вырасти в разы.

По результатам маркетингового анализа «Рынок печатных плат (с видами) в России, анализ развития с прогнозом 2029 г.», проведенного маркетинговым агентством Роиф Эксперт в 2024 году, рост объема российского производства печатных плат составил + 3 млн. штук, при этом в прогнозном периоде рынок продолжит показывать существенную динамику.

Совокупный объем российского рынка печатных плат формируется преимущественной за счет импортной продукции, и в рамках периода российским производителям фактически не удалось удержать свои позиции, вновь отмечается уменьшение доли российских печатных плат в общем объеме рынка несмотря на наращивание внутреннего выпуска.



## ВЫВОДЫ

Не смотря на то обстоятельство, что были собраны, изучены и проанализированы большие по объему данные, в основном монографического характера, авторы не считают до конца решенными поставленные в начале монографии цели и задачи. Это можно объяснить несколькими обстоятельствами.

Во-первых, сложность оценки воздействия: выявленные трудности в количественной оценке точных потерь и ущерба от санкций в ИТ-секторе подчеркивают сложность таких оценок. Это связано с отсутствием всеобъемлющих статистических данных и секретной природой многих релевантных документов, недоступных в настоящее время. Книга проводит глубокий анализ политических и экономических санкций, с фокусом на ИТ-секторе в контексте СССР и РФ. Основное внимание уделяется анализу санкционных мероприятий и их влиянию на экономику, политику и общество. Особое внимание уделено неудачам в поиске статистических данных о несостоявшихся проектах и контрактах, что подчеркивает сложность оценки воздействия санкций в этих сферах. Несмотря на обширные исследования, точное определение потерь и ущерба, понесенного в результате санкций в области информационных технологий, оказалось невозможным. Сложность оценки обусловлена отсутствием достаточной статистической информации и секретностью многих документов.

Во-вторых, исторические прецеденты и их влияние: конкретные случаи санкций, такие как запрет на поставку стальных труб в СССР, демонстрируют глубокое влияние этих действий как на экономическую политику, так и на международные отношения. Описывается исторический контекст санкций и их принципы, включая случаи противостояния и сотрудничества отдельных стран.

В-третьих, переход к внешнему анализу: из-за недостаточности внутренних данных и архивной информации исследование было переориентировано на анализ оценок эффективности санкций американскими и европейскими учеными и аналитиками.

Следует обратить внимание на последствия для будущих исследований и формирования политики. В первую очередь, это необходимость улучшения методов сбора данных: трудности в получении точных данных подчеркивают необходимость разработки более эффективных методов сбора и анализа данных в контексте политических и экономических санкций.

Затем следует определить влияние на политическую и экономическую динамику: исследование подчеркивает значительное влияние санкций на геополитические, экономические и технологические тенденции, требующие адаптивных стратегий в международных делах. Приведены

характерные примеры санкций против Южной Африки, Кубы, Ирака и других, подчеркивающие различные аспекты и последствия санкционных политик.

Авторы специально выделяют важность междисциплинарного подхода: для полного понимания эффективности и последствий санкций требуется междисциплинарный подход, объединяющий политическую экономию, историю, международные отношения и технологические исследования, построение соответствующих экономико-математических моделей и их адаптацию к резко изменяющейся цифровой среде. Содержание книги демонстрирует примеры успешного междисциплинарного сотрудничества в исследовании санкций. Интеграция данных и методов из различных областей, включая экономику, политологию, историю и право, способствует более глубокому пониманию и оценке санкционных мероприятий. Анализ предсказательных моделей для санкций выявляет их потенциал в прогнозировании экономических и политических последствий. Модели могут быть использованы для оценки будущих войн и конфликтов, основываясь на исторических данных и текущих геополитических тенденциях.

Считаем необходимым сфокусировать усилия и рекомендации для будущих исследований. Прежде всего, улучшение прозрачности и доступности данных, поскольку именно это будет способствовать развитию международного сотрудничества для улучшения прозрачности и доступности данных, связанных с санкциями и их последствиями. Отдельная нерешенная до настоящего времени проблема - разработка предсказательных моделей: необходимо инвестировать в разработку предсказательных моделей для лучшего прогнозирования результатов санкционной политики. А также содействовать междисциплинарным коллаборациям для более тонкого и всестороннего понимания многогранной природы санкций.

Данное исследование освещает сложную природу оценки воздействия международных санкций. Оно подчеркивает важность продолжения аналитических усилий в этой области для информирования будущих политических решений и академических запросов.

Авторы надеются, что представленная монография будет интересна и полезна читателям, которые занимаются изучением проблем эффективности политических и экономических санкций.

## ***Сведения об авторах***

***Охрименко Сергей Антонович***, доктор экономических наук, профессор, Молдавская Экономическая Академия, заведующий Лабораторией информационной безопасности (*Кишинев, Молдова*);

***Силаков Алексей Викторович***, доктор экономических наук, профессор, РГУ им. А.Н. Косыгина, проректор по науке и инновациям (*Москва, Россия*);

***Орлова Динара Рустемовна***, доктор экономических наук, профессор Кафедры экономической теории Финансового университета при Правительстве Российской Федерации (*Москва, Россия*);

***Сенков Валерий Александрович***, кандидат экономических наук, доцент, РГУ им. А.Н. Косыгина, заведующий Кафедрой Экономической безопасности (*Москва, Россия*);

***Черней Валерий Андреевич***, эксперт в области аудита и информационной безопасности Партнер BSD Management (*Кишинев, Молдова*)

Охрименко Сергей Антонович, Силаков Алексей Викторович,  
Орлова Динара Рустемовна, Сенков Валерий Александрович,  
Черней Валерий Андреевич

ЭКОНОМИЧЕСКИЕ САНКЦИИ  
В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Научное издание

Печатается в авторской редакции

Подготовка макета к печати  
Николаева Н.А.

Подписано в печать                      Формат бумаги 60x84/16  
Бумага множ.    Усл.печ.л.    Заказ                      Тираж 500

Редакционно-издательский отдел РГУ им. А.Н. Косыгина  
115035, Москва, ул. Садовническая, 33, стр. 1  
e-mail: riomgudt@mail.ru

Отпечатано в РИО ФГБОУ ВО «РГУ им. А.Н. Косыгина»