

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Институт экономики и управления

Направление подготовки

Профиль

Кафедра «Социология, экономическая
теория и международные процессы»

41.03.05 «Международные отношения»

Мировая политика и международный
бизнес

БАКАЛАВРСКАЯ РАБОТА

на тему

**Современные вызовы международной безопасности: от традиционных
угроз к гибридным формам конфликтов**

Студент

Савинкина
Виктория
Сергеевна

подпись, дата

Руководитель

Дубина А. Ш.

подпись, дата

Нормоконтролер

Влазнева С. А.

подпись, дата

Работа допущена к защите (протокол заседания кафедры от _____ № _____)

Заведующий кафедрой

Рожкова Л. В.

подпись, дата

Работа защищена с отметкой _____ (протокол ГЭК от _____ № _____)

Секретарь ГЭК

Рассказова Н. В.

подпись, дата

Пенза 2026

ФГБОУ ВО «Пензенский государственный университет»
Институт экономики и управления
Кафедра «Социология, экономическая теория и международные процессы»
Направление подготовки 41.03.05 «Международные отношения», профиль
«Мировая политика и международный бизнес»

«УТВЕРЖДАЮ»:
Зав. кафедрой
д.с.н., профессор Рожкова Л. В.

« ____ » _____ 20__ г.

ЗАДАНИЕ
НА БАКАЛАВРСКУЮ РАБОТУ

студенту Савинкиной В. С., группа 22ЭА1, обучение очное

1 Тема бакалаврской работы: Современные вызовы международной безопасности: от традиционных угроз к гибридным формам конфликтов

утверждена приказом по университету

от « ____ » _____ 20__ г . № _____

2 Срок сдачи студентом законченной бакалаврской работы: 8.06.2026.

3 Исходные данные к бакалаврской работе: нормативно-правовая база, научная и справочная литература, данные сети Интернет.

4 Перечень подлежащих разработке вопросов: трансформация международной безопасности в условиях современных угроз; противодействие гибридным угрозам и перспективы международной безопасности.

5 Перечень графического материала: таблицы, рисунки.

6 Дата выдачи задания: 25.10.2025.

График подготовки бакалаврской работы

№ п/п	Содержание работы	Срок выполнения	Дата выполнения, подпись руководителя
1	Составление плана ВКР	25.10.2025 – 10.11.2025	
2	Изучение исходных данных к бакалаврской работе	11.11.2025 – 25.12.2025	
3	Написание Главы 1	26.12.2025 – 26.02.2026	
4	Написание Главы 2	27.02.2026 – 29.04.2026	
5	Написание введения и заключения	30.04.2026 – 11.05.2026	
6	Оформление ВКР	12.05.2026 – 24.05.2026	
7	Сдача ВКР нормоконтролю, проверка в системе «антиплагиат.вуз»	25.05.2026 – 5.06.2026	
8	Ознакомление с отзывом руководителя	6.06.2026	
9	Представление законченной бакалаврской работы, передача в ГЭК	8.06.2026	

Руководитель _____ / А. Ш. Дубина /
(подпись) (инициалы, фамилия)

Задание принял к исполнению студент _____ / В. С. Савинкина /
(подпись) (инициалы, фамилия)

Реферат

Бакалаврская работа 62 с., 2 ч., 9 рис., 10 табл., 59 источников, 3 прил.

МЕЖДУНАРОДНАЯ БЕЗОПАСНОСТЬ, ГИБРИДНЫЕ УГРОЗЫ, ВООРУЖЁННЫЕ КОНФЛИКТЫ, КИБЕРБЕЗОПАСНОСТЬ, ЦИФРОВАЯ ТРАНСФОРМАЦИЯ

Объект исследования – современная система международной безопасности.

Целью исследования является анализ трансформации традиционных угроз международной безопасности и становления гибридных форм противоборства как нового вызова современной мировой политики.

Методологической основой исследования послужили общенаучные методы научного познания – анализ, синтез, индукция, дедукция, а также специальные методы исследования – системный анализ, сравнительно-политический метод, кейс-анализ, контент-анализ и элементы прогностического анализа.

Результаты работы: рассмотрены теоретико-методологические подходы к исследованию международной безопасности; проанализирована эволюция традиционных и нетрадиционных угроз в современных международных отношениях; систематизированы основные виды гибридных угроз и особенности их классификации; исследована трансформация традиционных угроз на примере современных вооружённых конфликтов; проведён анализ гибридных конфликтов и атак на объекты критической инфраструктуры; определена роль цифровых технологий и негосударственных акторов в трансформации современных механизмов международного противоборства; выявлены ключевые тенденции развития международной безопасности в условиях цифровизации и распространения гибридных форм конфликтов.

Рекомендации по внедрению. Для повышения эффективности противодействия современным угрозам международной безопасности рекомендуется совершенствовать механизмы международного сотрудничества в сфере кибербезопасности, развивать системы мониторинга и раннего предупреждения гибридных угроз, укреплять защиту объектов критической инфраструктуры, а также

адаптировать национальные и международные механизмы стратегического планирования к условиям цифровой трансформации.

Теоретическая значимость работы заключается в развитии научных представлений о трансформации международной безопасности и систематизации гибридных угроз, а практическая – в возможности использования её выводов для корректировки национальных стратегий кибербезопасности и совершенствования механизмов противодействия гибридным угрозам в условиях цифровой трансформации мировой политики.

Прогнозные предложения о развитии объекта исследования. В перспективе значение цифровых технологий, искусственного интеллекта, автоматизированных систем управления, киберопераций и негосударственных акторов в международном противоборстве будет возрастать. Одновременно будет усиливаться взаимосвязь между традиционными военными угрозами и невоенными инструментами стратегического воздействия. В этих условиях развитие международной безопасности будет связано с адаптацией существующих механизмов международного регулирования, усилением международного сотрудничества в цифровой сфере и формированием новых моделей противодействия гибридным угрозам.

Summary

Bachelor's thesis 62 p., 2 parts, 9 drawings, 10 tables, 59 sources, 3 applications.

INTERNATIONAL SECURITY, HYBRID THREATS, ARMED CONFLICTS,
CYBERSECURITY, DIGITAL TRANSFORMATION

The object of research is the modern system of international security.

The purpose of the study is to analyze the transformation of traditional threats to international security and the emergence of hybrid forms of confrontation as a new challenge to modern world politics.

The methodological basis of the research was general scientific methods of scientific cognition – analysis, synthesis, induction, deduction, as well as special research methods – system analysis, comparative political method, case analysis, content analysis and elements of predictive analysis.

The results of the work: theoretical and methodological approaches to the study of international security are considered; the evolution of traditional and non-traditional threats in modern international relations is analyzed; the main types of hybrid threats and their classification features are systematized; the transformation of traditional threats using the example of modern armed conflicts is investigated; hybrid conflicts and attacks on critical infrastructure are analyzed; the role of digital technologies and non-State actors in the transformation of modern mechanisms of international confrontation; The key trends in the development of international security in the context of digitalization and the spread of hybrid forms of conflict have been identified.

Recommendations for implementation. To increase the effectiveness of countering modern threats to international security, it is recommended to improve the mechanisms of international cooperation in the field of cybersecurity, develop systems for monitoring and early warning of hybrid threats, strengthen the protection of critical infrastructure facilities, and adapt national and international strategic planning mechanisms to the conditions of digital transformation.

The theoretical significance of the work lies in the development of scientific ideas about the transformation of international security and the systematization of hybrid threats,

while the practical significance lies in the possibility of using its findings to adjust national cybersecurity strategies and improve mechanisms for countering hybrid threats in the context of the digital transformation of world politics.

Forward-looking proposals on the development of the research object. In the future, the importance of digital technologies, artificial intelligence, automated control systems, cyber operations and non-state actors in the international confrontation will increase. At the same time, the relationship between traditional military threats and non-military instruments of strategic influence will be strengthened. Under these conditions, the development of international security will be associated with the adaptation of existing international regulatory mechanisms, strengthening international cooperation in the digital sphere and the formation of new models to counter hybrid threats.

Abstract

Bachelor 62 C., 2 H., 9 fig., 10 tableau., 59 sources, 3 applications.

SÉCURITÉ INTERNATIONALE, MENACES HYBRIDES, CONFLITS ARMÉS,
CYBERSÉCURITÉ, TRANSFORMATION NUMÉRIQUE

L'objet de l'étude est le système moderne de sécurité internationale.

L'objectif de l'étude est d'analyser la transformation des menaces traditionnelles à la sécurité internationale et l'émergence de formes hybrides de confrontation en tant que nouveau défi pour la politique mondiale moderne.

La base méthodologique de l'étude était les méthodes scientifiques générales de la cognition scientifique – analyse, synthèse, induction, déduction, ainsi que des méthodes spéciales de recherche – analyse systémique, méthode comparativement politique, analyse de cas, analyse de contenu et éléments d'analyse prédictive.

Résultats du travail: les approches théoriques et méthodologiques de l'étude de la sécurité internationale ont été examinées; l'évolution des menaces traditionnelles et non traditionnelles dans les relations internationales modernes a été analysée; les principaux types de menaces hybrides et les caractéristiques de leur classification ont été systématisés; la transformation des menaces traditionnelles a été étudiée à l'aide de l'exemple des conflits armés modernes; les conflits hybrides et les attaques contre les infrastructures critiques ont été analysés; le rôle des technologies numériques et des acteurs non étatiques dans la transformation des mécanismes modernes de confrontation internationale a été identifié; les principales tendances du développement de la sécurité internationale dans le contexte de la numérisation et de la prolifération des formes hybrides de conflits ont été identifiées.

Recommandations de mise en œuvre. Afin de mieux faire face aux menaces actuelles à la sécurité internationale, il est recommandé d'améliorer les mécanismes de coopération internationale en matière de cybersécurité, de développer les systèmes de surveillance et d'alerte rapide des menaces hybrides, de renforcer la protection des infrastructures critiques et d'adapter les mécanismes nationaux et internationaux de planification stratégique à la transformation numérique.

L'importance théorique du travail est de développer des idées scientifiques sur la transformation de la sécurité internationale et la systématisation des menaces hybrides, et pratique – la possibilité d'utiliser ses conclusions pour ajuster les stratégies nationales de cybersécurité et améliorer les mécanismes de lutte contre les menaces hybrides dans le contexte de la transformation numérique de la politique mondiale.

Propositions prospectives sur le développement de l'objet de l'étude. À l'avenir, l'importance des technologies numériques, de l'intelligence artificielle, des systèmes de contrôle automatisés, des Cyber-opérations et des acteurs non étatiques dans la confrontation internationale augmentera. Dans le même temps, les liens entre les menaces militaires traditionnelles et les instruments stratégiques non militaires seront renforcés. Dans ce contexte, le développement de la sécurité internationale passe par l'adaptation des mécanismes existants de réglementation internationale, le renforcement de la coopération internationale dans le domaine numérique et la mise en place de nouveaux modèles pour faire face aux menaces hybrides.

Оглавление

Введение.....	6
Глава 1 Трансформация международной безопасности в условиях современных угроз.....	7
1.1 Понятие международной безопасности и эволюция представлений о безопасности.....	7
1.2 Традиционные и современные угрозы международной безопасности.....	10
1.3 Гибридные конфликты как новая форма международного противоборства (на примере сирийского конфликта и кибератак на критическую инфраструктуру).....	16
Глава 2 Противодействие гибридным угрозам и перспективы международной безопасности.....	27
2.1 Роль ООН, НАТО и ЕС в обеспечении безопасности и противодействии гибридным угрозам.....	27
2.2 Сравнительный анализ стратегий противодействия гибридным угрозам (США, ЕС и Россия).....	32
2.3 Цифровые технологии, негосударственные акторы и перспективы развития международной безопасности до 2035 года.....	37
Заключение.....	50
Список использованных источников.....	53
Приложение А	58
Приложение Б	60
Приложение В	62

Введение

Актуальность темы определяется кардинальной трансформацией современной системы международной безопасности. Традиционные формы межгосударственного соперничества – вооружённые конфликты, гонка вооружений, стратегическое сдерживание по-прежнему остаются одними из важнейших способов ведения конфликтов, однако в современном мире они перестали быть доминирующими. На первый план выходят немилитаризованные инструменты воздействия: целенаправленные информационные кампании, кибератаки на критическую инфраструктуру, экономические санкции как средство политического давления, а также деятельность негосударственных акторов. Ключевое отличие нового этапа в том, что подобные методы позволяют подрывать стабильность государств без прямого применения военной силы. Эмпирическим подтверждением данного тренда служат события последних лет: конфликт на Украине, беспрецедентные по масштабу кибератаки и развёрнутое санкционное противостояние. Эти кейсы наглядно свидетельствуют о переходе от классического военно-политического противоборства к гибридным моделям достижения внешнеполитических целей.

Подобная трансформация международной среды приводит к снижению чёткости границ между состояниями войны и мира, а также между традиционными и нетрадиционными формами противостояния. Гибридные конфликты, сочетающие военные, политические, экономические, информационные и технологические инструменты воздействия, становятся одной из ключевых форм современной международной конфликтности. В этих условиях возрастает необходимость комплексного исследования эволюции международной безопасности, механизмов трансформации угроз и особенностей формирования гибридных форм противоборства.

Степень научной разработанности проблемы можно охарактеризовать как достаточно высокую. Теоретические основы международной безопасности получили широкое освещение в рамках классических и современных теорий международных отношений. Значительный вклад в исследование вопросов безопасности внесли Ганс

Моргентау, рассматривавший безопасность через призму национального интереса и баланса сил, Кеннет Уолтц, связывавший поведение государств с особенностями структуры международной системы, Роберт Кеохейн, исследовавший роль международных институтов и режимов в обеспечении стабильности мировой политики, а также Александр Вендт, акцентировавший внимание на влиянии идентичности, восприятия угроз и политического дискурса на международные отношения [41, с. 13; 58, с. 11].

Отдельное направление исследований посвящено изучению гибридных конфликтов и гибридных угроз. Существенный вклад в развитие данной проблематики внесли Фрэнк Хоффман, сформулировавший концепцию гибридной войны как сочетания традиционных и нетрадиционных способов противоборства, Эндрю Монаган, исследовавший особенности современных гибридных стратегий, а также ряд российских исследователей, рассматривающих вопросы информационного противоборства, кибербезопасности и трансформации современных конфликтов. В отечественной научной литературе проблемы гибридных угроз нашли отражение в работах А. Д. Богатурова, А. В. Манойло, В. А. Батюка, В. И. Пантиной и других авторов [8, с. 43].

Несмотря на значительное количество исследований, в научной литературе до настоящего времени отсутствует единый подход к определению сущности гибридных угроз и их места в системе международной безопасности. Недостаточно изученными остаются вопросы взаимосвязи традиционных и нетрадиционных угроз, влияния цифровых технологий и негосударственных акторов на трансформацию современных конфликтов, а также перспектив развития международной безопасности в условиях дальнейшей гибридизации международного противоборства. Именно данные аспекты обуславливают актуальность и научную значимость настоящего исследования.

Объектом исследования является современная система международной безопасности.

Предметом исследования выступают гибридные угрозы как фактор трансформации современной системы международной безопасности.

Целью исследования является анализ трансформации традиционных угроз международной безопасности и становления гибридных форм противоборства как нового вызова современной мировой политики.

Для достижения поставленной цели сформулированы следующие задачи:

- выявить особенности эволюции понятия международной безопасности и основных теоретических подходов к её исследованию;
- систематизировать традиционные и современные угрозы международной безопасности, определить их основные характеристики и принципы классификации;
- раскрыть сущность гибридных конфликтов как новой формы международного противоборства и определить методологические подходы к их исследованию;
- проанализировать роль международных организаций в противодействии гибридным угрозам и обеспечении международной безопасности;
- провести сравнительный анализ подходов США, Европейского союза и Российской Федерации к противодействию гибридным угрозам;
- определить влияние цифровых технологий и негосударственных акторов на трансформацию современных конфликтов и сформировать прогноз развития международной безопасности до 2035 г.

Гипотеза исследования заключается в том, что распространение гибридных угроз способствует трансформации существующих механизмов обеспечения международной безопасности и требует формирования новых моделей международного взаимодействия.

Методологическую основу исследования составляют реалистический, либеральный и конструктивистский концепции. В качестве методов исследования используются кейс-анализ, сравнительно-политический анализ, контент-анализ и элементы прогностического анализа. Кейс-анализ используется для изучения сирийского конфликта и кибератак на критическую инфраструктуру; сравнительно-политический анализ – для сопоставления подходов России, США и ЕС; контент-анализ – для исследования стратегий и официальных документов.

Теоретическая и практическая значимость исследования заключается в развитии научных представлений о трансформации международной безопасности и современных гибридных угрозах, уточнении методологических подходов к анализу гибридных конфликтов, а также в возможности использования полученных результатов при исследовании современных международных конфликтов, разработке мер противодействия гибридным угрозам и в образовательном процессе при подготовке специалистов в области международных отношений, международной безопасности и мировой политики.

Эмпирическую базу исследования составили документы ООН, НАТО и Европейского союза, стратегии национальной безопасности государств, аналитические доклады международных организаций, статистические материалы и публикации российских и зарубежных исследовательских центров.

Теоретическую базу исследования составили труды российских и зарубежных специалистов в области международной безопасности, международных отношений и исследований гибридных конфликтов.

Структура работы включает введение, две главы, заключение, список использованных источников и приложения. Первая глава посвящена теоретическим аспектам международной безопасности, вторая – анализу гибридных конфликтов и перспективам развития международной безопасности и механизмам противодействия гибридным угрозам

Глава 1 Трансформация международной безопасности в условиях современных угроз

1.1 Понятие международной безопасности и эволюция представлений о безопасности

Понятие международной безопасности формировалось одновременно с развитием системы международных отношений, отражая изменения в структуре мировой политики, характере взаимодействия государств и содержании возникающих угроз. На ранних этапах развития политической науки безопасность рассматривалась преимущественно через военно-политическое измерение, а её обеспечение связывалось с сохранением государственного суверенитета, защитой территориальной целостности и поддержанием баланса сил в условиях международной анархии [29, с. 46].

Значительный вклад в формирование данного подхода внёс Ганс Моргентау, заложивший основы классического политического реализма и рассматривавший международную политику как постоянную борьбу государств за власть, влияние и защиту национальных интересов. Безопасность в рамках данной концепции определяется способностью государства сохранять устойчивое положение в системе международных отношений и противодействовать внешнему давлению [43, с. 30].

Дальнейшее развитие реалистической традиции получила в работах Кеннета Уолтца. Исследователь сформировал основы структурного реализма, сосредоточив внимание на влиянии международной системы на поведение государств. Согласно его концепции, уровень безопасности определяется не только внутренними ресурсами государства, но и распределением силы в международной среде. Вместе с тем реалистическая теория ориентирован преимущественно на военно-стратегическое измерение международных отношений. Это ограничивает его применение при анализе современных немилитаризованных форм противостояния, в частности информационных и кибернетических форм воздействия [57, с. 128].

Развитие процессов глобализации, усиление экономической взаимозависимости и институционализация международного взаимодействия способствовали формированию либерального подхода. Существенный вклад в его развитие внёс Роберт Кеохейн, исследовавший роль международных институтов, режимов и механизмов сотрудничества в обеспечении устойчивости мировой политической системы. В рамках либеральной концепции исследование международной безопасности расширяется за счёт учёта институциональных механизмов, дипломатического взаимодействия и многостороннего сотрудничества. Вместе с тем данная парадигма ограниченно учитывает скрытые формы давления, асимметричные стратегии и деятельность негосударственных участников современных конфликтов [37, с. 43].

Существенное расширение исследовательских возможностей связано с развитием конструктивистской теории. Его ключевым представителем является Александр Вендт. В своих работах он рассматривал международную безопасность как социально конструируемое явление, формируемое под влиянием идентичности, ценностей, норм и восприятия угроз. Особое внимание в рамках данного подхода уделяется политическому дискурсу, информационному воздействию и интерпретации международных процессов участниками мировой политики. Это позволяет учитывать когнитивное и информационное измерения современных конфликтов [58, с. 321].

Сравнение основных теоретических концепций показывает, что каждый из них раскрывает отдельные аспекты международной безопасности. Реализм фокусируется на силовом противоборстве и балансе мощи. Либерализм, напротив, выводит на первый план международные институты и кооперацию. Конструктивизм же добавляет измерение идентичности, восприятия и информационной среды. Каждый из подходов сам по себе не охватывает феномен гибридных угроз – именно поэтому возникает необходимость в их синтезе.

Анализ научных подходов позволяет установить, что содержание международной безопасности не оставалось неизменным и последовательно расширялось по мере развития международных отношений. Изменение

представлений о безопасности от военно-политической модели к комплексному пониманию данной категории целесообразно представить в виде схемы (рисунок 1).

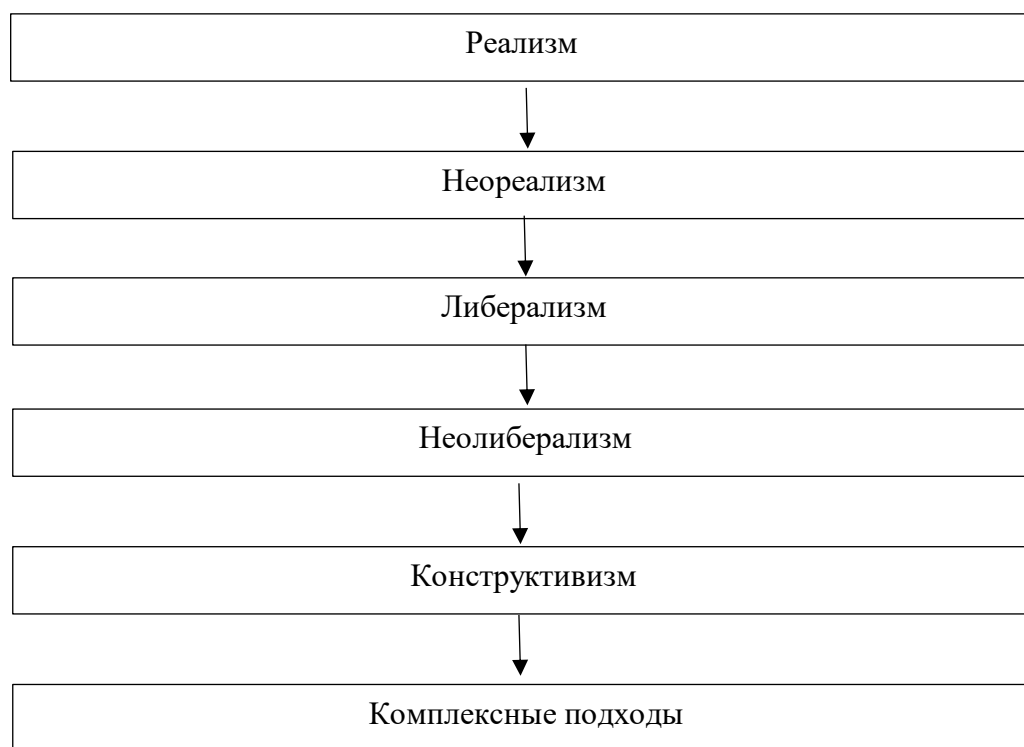


Рисунок 1 – Эволюция подходов к международной безопасности [17, с. 21]

Рассмотренные этапы развития научных представлений свидетельствуют о существенном усложнении содержания категории международной безопасности. Наряду с традиционными военно-политическими аспектами в её структуру были включены новые измерения, связанные с информационной, экономической и технологической сферами. В результате сформировалась теоретическая база, позволяющая анализировать современные гибридные угрозы в контексте взаимосвязи различных форм международного воздействия.

Эволюция на рисунке 1 – это не просто смена теорий, а ответ на усложнение самой международной реальности. Реализм объяснял силу, но не институты. Либерализм добавил институты, но упустил идентичность. Конструктивизм вплёл идентичность, но слаб в анализе материальных факторов. Именно поэтому

гибридные угрозы не может объяснить ни одна из теорий по отдельности – нужен синтез. В этом и состоит методологический вызов, который схема фиксирует, но не решает.

Таким образом, за спором теоретиков (реализм против либерализма, либерализм против конструктивизма) скрывается более простая проблема: каждый из подходов видит только часть реальности, а гибридные угрозы требуют объёмного зрения. Это означает, что на практике исследователи гибридных конфликтов будут использовать межпарадигмальный синтез, даже если не называют его вслух. Именно так построена дальнейшая работа: сначала классификация угроз, затем разбор кейсов, где прослеживаются и силовые, и институциональные, и когнитивные измерения.

1.2 Традиционные и современные угрозы международной безопасности

Развитие международных отношений сопровождается расширением спектра угроз, способных оказывать влияние на устойчивость мировой политической системы. Если ранее ключевое внимание уделялось преимущественно военным рискам, то в настоящее время возрастает роль политических, экономических, информационных и технологических факторов дестабилизации. Это требует систематизации существующих угроз и определения критериев их научной классификации [19, с. 9].

Традиционно угрозы международной безопасности подразделяются на традиционные и нетрадиционные. К традиционным угрозам относятся межгосударственные вооружённые конфликты, территориальные споры, гонка вооружений и ядерное противостояние, отличительной особенностью которых является применение военной силы либо угроза её использования [26, с. 53].

Нетрадиционные угрозы формируются в иных сферах международного взаимодействия и включают экономическое давление, санкционные механизмы, информационно-психологическое воздействие, кибератаки, технологическое вмешательство и деятельность транснациональных структур. Их реализация может происходить без прямого вооружённого столкновения, однако последствия способны

оказывать существенное влияние на политическую и социальную устойчивость государств [29, с. 53].

При более детальном рассмотрении становится очевидным, что перечисленные группы угроз не существуют изолированно, а формируют взаимосвязанную систему. Для более чёткого представления их характеристик и особенностей целесообразно рассмотреть их в структурированном виде (таблица 1).

Таблица 1 – Классификация угроз международной безопасности [7, с. 16]

Критерий классификации	Вид угроз	Содержание угроз
По способу реализации	Традиционные	Вооруженные конфликты, военные интервенции, гонка вооружений, ядерное сдерживание
	Нетрадиционные	Кибератаки, терроризм, информационные войны, экономическое давление
По сфере проявления	Военные	Прямое применение вооруженной силы, военные конфликты
	Политические	Дестабилизация политических систем, вмешательство во внутренние дела
	Экономические	Санкции, торговые войны, финансовое давление
	Информационные	Пропаганда, дезинформация, информационные операции
	Технологические	Киберугрозы, использование ИИ, беспилотные системы
По источнику	Государственные	Действия государств в рамках внешней политики
	Негосударственные	Террористические организации, ТНК, частные военные компании

Из представленной классификации следует, что современные угрозы не существуют изолированно. Военные, политические, экономические, информационные и технологические инструменты всё чаще применяются одновременно, усиливая общий эффект воздействия. При этом традиционное деление угроз на «внешние» и «внутренние» теряет смысл – негосударственные акторы действуют вне государственных границ, а кибератаки могут запускаться с территории любого государства. Главный вывод из таблицы заключается в том, что система международной безопасности сегодня сталкивается не с отдельными рисками, а с их

комплексными сочетаниями. Это требует от государств не точечных мер, а выработки интегрированных стратегий реагирования.

Наиболее отчётливо данные изменения прослеживаются на примере сирийского конфликта, вооружённого противостояния в Нагорном Карабахе в 2020 г., а также военно-политического соперничества в Азиатско-Тихоокеанском регионе. Несмотря на различия в масштабах и составе участников, указанные кейсы позволяют выявить общую тенденцию – переход от преимущественно силовой модели противоборства к многоуровневым конфликтам, сочетающим военные, технологические и политические инструменты воздействия.

Сирийский конфликт показал переход от локального вооружённого противостояния к многоуровневому международному конфликту с участием внешних акторов [28, с. 8; 53].

Вооружённый конфликт в Нагорном Карабахе в 2020 г. выявил качественные изменения в тактике ведения боевых действий. Активное применение беспилотных авиационных комплексов *Bayraktar TB2*, барражирующих боеприпасов, спутниковой разведки и средств радиоэлектронной борьбы серьёзно изменило соотношение сил на поле боя. По оценкам военных аналитиков *International Institute for Strategic Studies*, именно беспилотные комплексы обеспечили поражение значительной части бронетехники и средств ПВО противника. Тем самым фиксируется переход от массового применения бронетехники к высокоточным дистанционным ударам – а это, в свою очередь, корректирует устоявшиеся представления о балансе сил в региональных войнах [51].

Отдельное значение для анализа трансформации традиционных угроз имеет военно-политическое соперничество в Азиатско-Тихоокеанском регионе. Усиление напряжённости вокруг Тайваня, милитаризация Южно-Китайского моря, формирование военно-политического партнёрства *AUKUS*, развитие стратегического диалога в формате *QUAD*, а также проведение Китаем испытаний гиперзвуковых систем свидетельствуют о росте стратегической конкуренции между США и КНР [10, с. 46]. В отличие от классических вооружённых конфликтов, противоборство в данном регионе развивается преимущественно в формате стратегического

сдерживания, однако ключевое значение всё в большей степени приобретают технологическое превосходство, развитие искусственного интеллекта, спутниковых систем, средств кибербезопасности и высокоточного вооружения. Исследование показывает, что в современных условиях Азиатско-Тихоокеанский регион становится одним из ключевых центров формирования новой модели глобального военно-политического баланса, в которой традиционная гонка вооружений всё теснее связана с цифровой и технологической конкуренцией [9, с. 40; 46].

Для более детального выявления ключевых изменений целесообразно сопоставить основные характеристики рассматриваемых конфликтов (таблица 2).

Таблица 2 – Трансформация традиционных угроз на примере современных конфликтов [29, с. 55]

Конфликт	Ключевые участники	Традиционные элементы	Новые элементы противоборства	Основной результат	Ключевая тенденция
Сирия (2011–н.в.)	Сирия, Россия, США, Турция, Иран	Авиаудары, сухопутные операции, борьба за территории	Санкции, информационные кампании, прокси-группы	Интернационализация конфликта	Расширение состава участников и интеграция не прямых форм воздействия
Нагорный Карабах (2020)	Армения, Азербайджан, Турция	Артиллерия, бронетехника, сухопутные операции	Беспилотные системы, цифровая разведка, РЭБ	Изменение тактики ведения войны	Переход к высокоточному дистанционному поражению
АТР (2015–н.в.)	Китай, США, союзники	Военно-морское соперничество, стратегическое сдерживание	Кибероперации, спутниковые технологии, ИИ	Технологизация стратегического баланса	Смещение конкуренции в цифровую и технологическую сферу

Сравнение трёх конфликтов – сирийского, карабахского и соперничества в АТР – показывает общую закономерность: традиционная военная сила не исчезает, но её применение всё чаще дополняется новыми элементами. В Сирии ключевую роль сыграла интернационализация и санкционное давление, в Карабахе – беспилотные системы и цифровая разведка, в АТР – технологическая конкуренция и кибероперации. Это свидетельствует о переходе от «чисто военных» конфликтов к многоуровневым противостояниям, в которых исход определяется не только

успехами на поле боя, но и способностью контролировать информационную, экономическую и технологическую сферы. Важно подчеркнуть, что каждая из этих сфер может стать самостоятельной ареной противоборства [20, с. 35].

Выявленные тенденции позволяют сделать вывод о том, что традиционные угрозы не исчезают, а адаптируются к новым условиям международного противоборства, приобретая более сложный, многоуровневый и технологически насыщенный характер. Для наглядного отражения основных направлений данной трансформации представим их в виде схемы (рисунок 2).

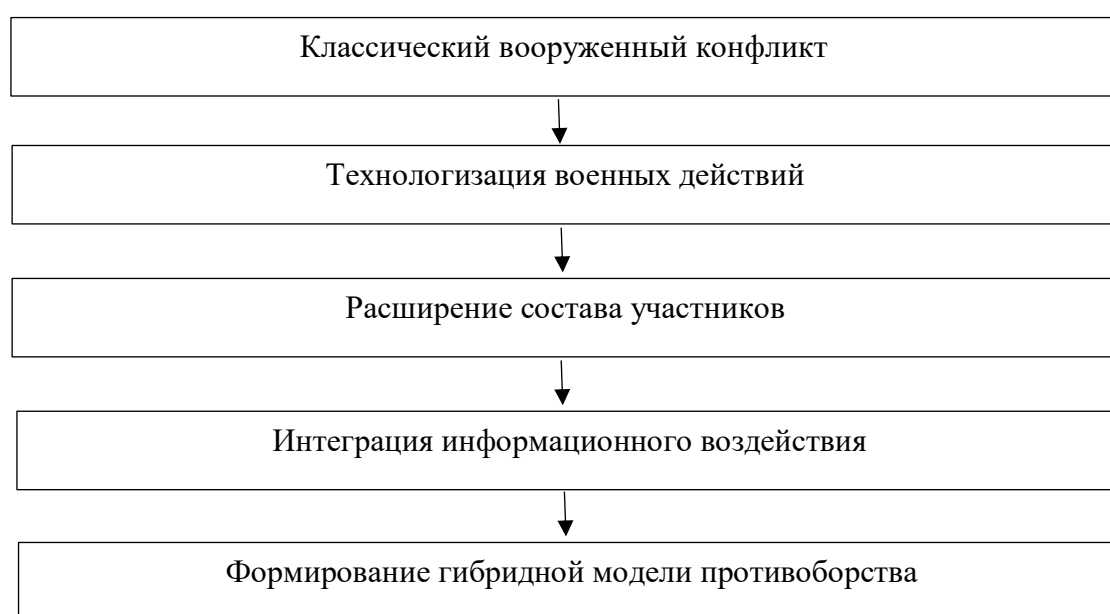


Рисунок 2 – Основные направления трансформации традиционных угроз в XXI в.
[20, с. 44]

Анализ этих процессов позволяют сделать вывод о постепенном усложнении среды международной безопасности. Если ранее основное внимание государств было сосредоточено на противодействии конкретным военным угрозам, то в современных условиях возрастает значение способности адаптироваться к быстро меняющимся условиям стратегической конкуренции.

В результате конкурентные преимущества всё чаще определяются не только объёмом имеющихся ресурсов, но и скоростью внедрения инноваций, уровнем координации различных инструментов воздействия и способностью прогнозировать

изменения международной обстановки. Это свидетельствует о переходе от преимущественно силовой модели обеспечения безопасности к более комплексному подходу, основанному на сочетании военных, технологических, информационных и организационных возможностей государства. Следует учитывать, что представленные направления трансформации развивались параллельно и взаимно усиливали друг друга. Можно предположить, что технологическая конкуренция будет играть всё более значимую роль среди факторов международной нестабильности [21, с. 10]. Схема показывают не просто «направления изменений», а системную ловушку для государств. Технологизация без информационной интеграции бесполезна. Расширение состава участников без гибридной модели ведёт к хаосу. Все четыре процесса запущены одновременно, и задержка хотя бы по одному из них делает всю систему уязвимой.

Количественным подтверждением сохранения высокой значимости традиционного силового фактора выступает динамика мировых военных расходов, отражающая усиление стратегической конкуренции между ведущими центрами силы, модернизацию вооружённых сил и рост инвестиций в высокотехнологичные системы вооружения (рисунок 3).

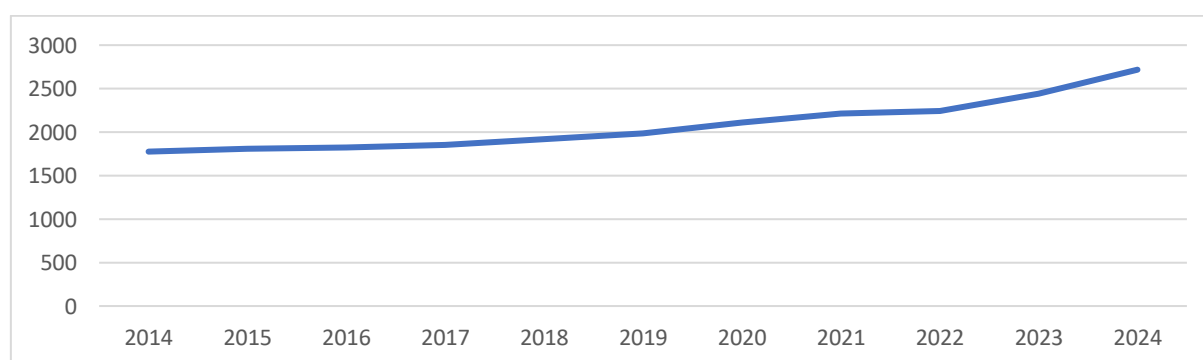


Рисунок 3 – Динамика мировых военных расходов в 2014–2024 гг., млрд долл. США [59]

Анализ показывает устойчивый рост мировых военных расходов на протяжении рассматриваемого периода. По данным *Stockholm International Peace Research Institute*, в 2014 г. совокупные мировые расходы составляли 1776 млрд долл.

США, тогда как к 2024 г. данный показатель достиг 2718 млрд долл., увеличившись более чем на 50 %. Наиболее интенсивный рост наблюдается после 2020 г., что связано с обострением региональных конфликтов, модернизацией вооружённых сил и ускоренным развитием высокотехнологичных систем вооружения. Полученные результаты свидетельствуют о том, что традиционный силовой фактор не утрачивает значения, а адаптируется к новым технологическим условиям международного противоборства [51].

Полученные данные позволяют усомниться в тезисе о «снижении роли военной силы» в условиях гибридизации конфликтов. Скорее, можно говорить о перераспределении военных расходов в пользу высокотехнологичных компонентов при сохранении их общего объёма. Следовательно, для оценки стратегического потенциала государства недостаточно анализировать только кибербезопасность или только традиционные вооружения – необходим комплексный учёт обоих факторов.

Таким образом, классификация угроз по отдельным сферам (военные, политические, экономические, информационные) сегодня работает плохо – в реальных конфликтах они не встречаются поодиночке. Следовательно, традиционные институты, заточенные под одну сферу (например, министерство обороны – под военные угрозы, а ведомство по цифровому развитию — под кибератаки), заведомо проигрывают тем, кто умеет наносить удары одновременно по нескольким направлениям. Дальнейший анализ на конкретных кейсах покажет, как эта «межведомственная уязвимость» эксплуатируется на практике.

1.3 Гибридные конфликты как новая форма международного противоборства (на примере сирийского конфликта и кибератак на критическую инфраструктуру)

Трансформация международной конфликтности в XXI в. привела к формированию новых моделей противоборства, в рамках которых применение вооружённой силы сочетается с политическим давлением, информационным воздействием, экономическими ограничениями и цифровыми операциями. В научной

литературе подобные формы противостояния получили определение гибридных конфликтов. Существенный вклад в развитие данной концепции внёс Фрэнк Хоффман, определявший гибридный конфликт как сочетание регулярных и нерегулярных форм ведения борьбы, информационных операций, экономического давления и асимметричных инструментов воздействия [39, с. 66]. Аналогичные выводы содержатся в аналитических докладах *RAND Corporation*, согласно которым современные конфликты всё чаще развиваются как многоуровневые системы политического, информационного и технологического давления [46].

Специфика гибридного конфликта заключается не только в разнообразии применяемых инструментов, но и в изменении самой логики международного противоборства. В отличие от классических вооружённых столкновений, гибридное влияние ориентировано не исключительно на военное поражение противника, а на постепенное снижение его политической устойчивости, управляемости, экономической стабильности и способности к принятию стратегических решений. При этом воздействие может осуществляться одновременно в физическом, информационном, экономическом и цифровом пространствах [26, с. 2].

Для выявления ключевых характеристик гибридного противоборства наиболее показателен сирийский конфликт, начавшийся в 2011 г. Первоначально кризис развивался как внутреннее политическое противостояние, вызванное социально-экономическими и внутривнутриполитическими противоречиями. Однако уже на ранних этапах конфликт приобрёл международный характер, что привело к вовлечению внешних государств, негосударственных вооружённых формирований, частных военных структур и международных коалиций [53].

В различные периоды прямое либо косвенное участие в конфликте принимали Сирия, Россия, США, Турция, Иран, а также многочисленные вооружённые формирования. Военные операции сопровождались дипломатическим давлением, санкционными механизмами, борьбой за контроль над энергетической инфраструктурой, информационным противоборством и активным использованием не прямых форм политического влияния [29, с. 6].

Особенностью сирийского конфликта стало одновременное использование широкого спектра инструментов воздействия различными международными акторами. В сентябре 2015 г. Россия начала военную операцию Воздушно-космических сил по поддержке правительства Башара Асада, что существенно изменило соотношение сил на театре военных действий. Параллельно на территории Сирии действовала международная коалиция во главе с США, осуществлявшая операции против террористической организации ИГИЛ (запрещена в Российской Федерации). Кроме того, Турция проводила собственные военные операции в приграничных районах, мотивируя их необходимостью обеспечения национальной безопасности и противодействия курдским вооружённым формированиям [52]

Военное противоборство сопровождалось активным использованием экономических инструментов давления. В частности, в 2020 г. Соединённые Штаты ввели пакет санкций в рамках так называемого *Caesar Act*, предусматривающий ограничения в отношении сирийских государственных структур, компаний и иностранных организаций, сотрудничающих с правительством Сирии. Санкционная политика дополняла военные и дипломатические меры, оказывая долгосрочное влияние на социально-экономическое положение страны [56]

Не менее важным элементом конфликта стало информационное противоборство. Различные участники конфликта активно использовали международные СМИ, цифровые платформы и социальные сети для формирования выгодной интерпретации происходящих событий. В результате борьба за контроль над информационной повесткой стала самостоятельным направлением противоборства наряду с вооружёнными действиями.

Военные операции в Сирии органично дополнялись дипломатической изоляцией, санкционными режимами, информационными кампаниями и задействованием прокси-сил. Такая комбинация инструментов позволила внешним акторам влиять на ход событий, не прибегая к полномасштабному военному присутствию. Для определения структуры гибридного воздействия в сирийском конфликте целесообразно систематизировать основные применявшиеся инструменты (таблица 3).

Таблица 3 – Инструменты гибридного воздействия в сирийском конфликте [53]

Направление воздействия	Основные инструменты	Примеры
Военное	Авиационные удары, специальные операции, поставки вооружения	Операции ВКС России, действия международных коалиций
Политико-дипломатическое	Переговорные форматы, международное давление, резолюции	Астанинский процесс, обсуждение в СБ ООН
Экономическое	Санкционные ограничения, контроль ресурсной инфраструктуры	Ограничения против сирийских государственных структур
Информационное	Медиасопровождение, цифровые кампании, информационные нарративы	Международные медиаплатформы, социальные сети
Непрямое воздействие	Прокси-группы, нерегулярные вооруженные формирования	Участие союзных вооруженных структур

Сравнение направлений воздействия позволяет установить, что гибридный конфликт представляет собой не совокупность отдельных инструментов воздействия, а целостную систему взаимосвязанных политических, военных, экономических и информационных механизмов. Военная сила в современных условиях перестаёт выступать единственным инструментом достижения стратегических целей и всё чаще интегрируется в более широкую архитектуру непрямого воздействия.

Сирийский конфликт показывает: ни один из перечисленных инструментов в отдельности не решил бы задачу. Авиаудары без санкций не остановили бы внешнее финансирование оппозиции. Информационные кампании без дипломатического давления не легитимизировали бы действия внешних сил. Только одновременное применение всех пяти направлений создало тот эффект, который сделал сирийскую модель образцом для последующих гибридных конфликтов.

Особый интерес представляет распределение функций между различными инструментами давления. Военные операции обеспечивали изменение контроля над территориями, дипломатические механизмы формировали международную легитимацию действий, санкционные ограничения создавали экономическое давление, а информационные кампании влияли на интерпретацию конфликта в

глобальном медиапространстве. Использование прокси-групп дополнительно снижало уровень прямой политической ответственности внешних акторов [16, с. 30].

Выявленная взаимосвязь позволяет представить сирийский конфликт как многоуровневую систему гибридного воздействия, в которой каждый элемент выполняет самостоятельную функцию, усиливая общий стратегический эффект (рисунок 4).

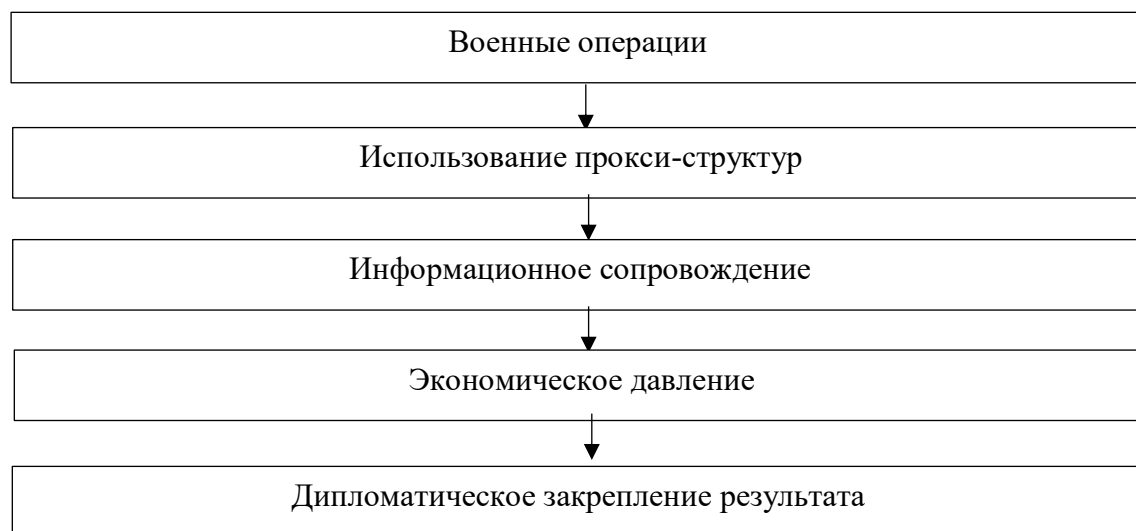


Рисунок 4 – Структура гибридного воздействия в сирийском конфликте [24]

Представленная структура позволяет сделать вывод о том, что сирийский конфликт фактически стал одной из первых масштабных моделей гибридного противоборства современного типа. Военные действия в нём развивались в тесной взаимосвязи с санкционным давлением, дипломатической конкуренцией, деятельностью негосударственных вооружённых формирований и информационными кампаниями. При этом эффективность каждого отдельного инструмента определялась не самостоятельным применением, а его включённостью в единую систему воздействия. Сирийский кейс демонстрирует, что достижение политических целей в современных конфликтах всё чаще обеспечивается сочетанием военных и невоенных методов, границы между которыми становятся всё менее чёткими [53]. Важно подчеркнуть, что эффективность сирийской модели гибридного воздействия во многом обеспечивалась внешними условиями – длительностью

конфликта, отсутствием единого фронта оппозиции, заинтересованностью региональных акторов. Это значит, что прямое перенесение сирийского опыта на другие конфликты вряд ли возможно. Каждый гибридный конфликт, вероятно, будет иметь уникальную конфигурацию инструментов, определяемую локальным контекстом.

Наряду с военно-политическими механизмами существенное место в современных гибридных конфликтах занимают атаки на объекты критической инфраструктуры. Их стратегическое значение определяется тем, что нарушение функционирования энергетических систем, транспортных узлов, телекоммуникационных сетей, финансовой инфраструктуры и цифровых платформ государственного управления оказывает комплексное воздействие на устойчивость государства без непосредственного применения вооружённой силы [14, с. 63].

В отличие от традиционных форм силового давления, кибероперации характеризуются высокой скрытностью, относительной экономической доступностью и возможностью дистанционного применения. При этом последствия подобных атак затрагивают одновременно экономическую сферу, систему государственного управления, информационное пространство и социальную стабильность.

Для выявления закономерностей подобного воздействия целесообразно сопоставить наиболее значимые случаи атак на объекты критической инфраструктуры (таблица 4).

Таблица 4 – Крупнейшие кибератаки на объекты критической инфраструктуры [9, с. 34]

Год	Объект воздействия	Использованный инструмент	Основные последствия
1	2	3	4
2010	Ядерный комплекс в Натанзе (Иран)	Вредоносные ПО <i>Stuxnet</i>	Нарушение работы центрифуг и технологических процессов
2015	Энергосистема Украины (Киев)	Вредоносное ПО <i>BlackEnergy</i>	Масштабные перебои в энергоснабжении

1	2	3	4
2016	Промышленные системы управления	Вредоносный комплекс <i>Industroyer</i>	Нарушение автоматизированного управления
2021	Трубопровод <i>Colonial Pipeline</i> (США)	<i>Ransomware</i> -атака <i>DarkSide</i>	Временная остановка поставок топлива на восточном побережье США
2023	Порт Нагоя (Япония)	<i>Ransomware</i> -атака <i>LockBit</i>	Временная остановка работы одного из крупнейших морских портов Японии и нарушение логистических цепочек

Результаты исследования подтверждают, что кибератаки на объекты критической инфраструктуры в последние годы приобретают устойчивый и системный характер. Объектами воздействия становятся стратегически значимые системы, обеспечивающие функционирование энергетики, промышленности, транспорта и цифрового государственного управления. По оценкам *NATO Cooperative Cyber Defence Centre of Excellence*, критическая инфраструктура становится одной из приоритетных целей современных киберопераций вследствие её прямого влияния на устойчивость государственного управления, экономические процессы и социальную стабильность [44].

Эволюция целей в таблице 4 важнее, чем кажется на первый взгляд. Переход от иранского ядерного объекта к американскому трубопроводу означает не просто смену мишени, а смену логики: от шпионажа и саботажа к прямому экономическому ущербу и публичному шантажу. Ещё показательнее смена исполнителя: *Stuxnet* разрабатывался государством, *DarkSide* – коммерческой группой. Доступность такого оружия для негосударственных акторов, пожалуй, более тревожный сигнал, чем сам факт атак.

Если на ранних этапах развития киберугроз подобные операции были направлены преимущественно на отдельные технологические элементы, то в дальнейшем наблюдается переход к комплексным операциям, затрагивающим целые инфраструктурные отрасли. Одним из наиболее показательных примеров стала атака на *Colonial Pipeline* в 2021 г., вызвавшая перебои поставок топлива на восточном

побережье США и продемонстрировавшая уязвимость даже высокоразвитой частной энергетической инфраструктуры [33].

Существенной проблемой в условиях роста числа атак на объекты критической инфраструктуры остаётся несовершенство международно-правового регулирования в цифровой сфере. Несмотря на активное обсуждение вопросов кибербезопасности на площадках ООН, НАТО и ОБСЕ, универсальные механизмы квалификации кибератак и определения юридической ответственности государств за действия негосударственных акторов до настоящего времени остаются ограниченными. Сложность атрибуции цифровых атак, использование распределённой инфраструктуры, прокси-групп и транснациональных сетевых платформ существенно затрудняют применение традиционных норм международного права. Это формирует ситуацию правовой неопределённости, в которой киберпространство всё чаще используется как относительно низкорисковая среда для реализации стратегического давления [50]. Эти особенности позволяют перейти к рассмотрению типовой последовательности реализации киберопераций против объектов критической инфраструктуры (рисунок 5).

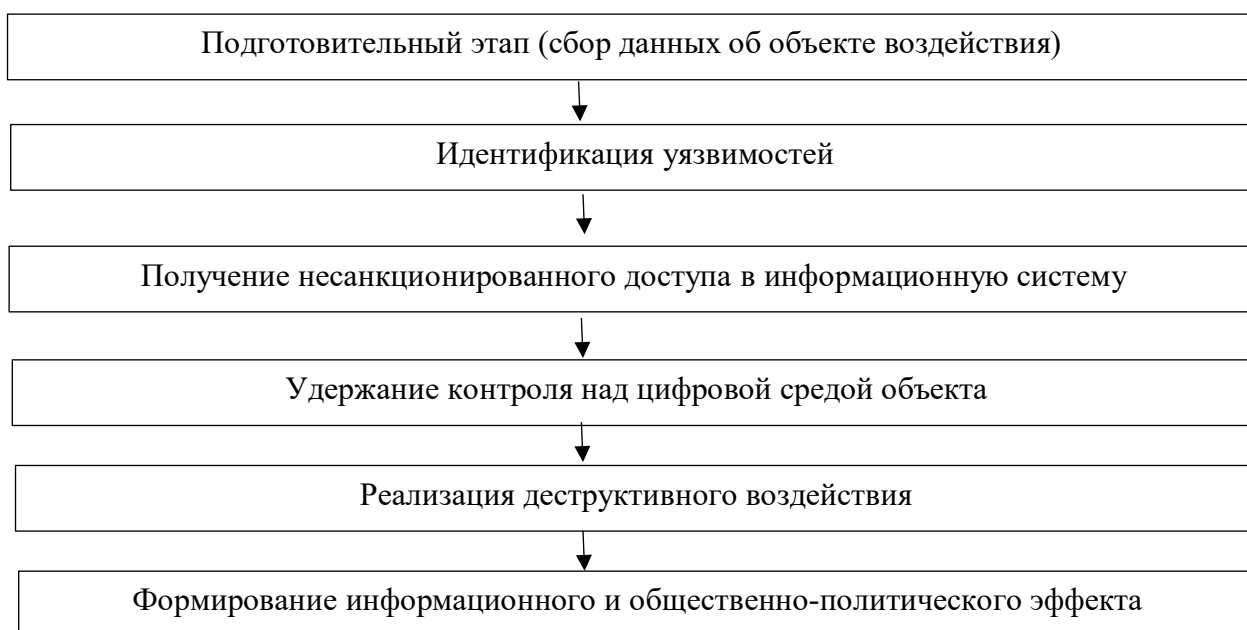


Рисунок 5 – Этапы проведения кибератаки на объекты критической инфраструктуры [6, с. 231]

Схема показывает, что кибератака на объекты критической инфраструктуры представляет собой многоэтапный процесс, включающий не только техническое получение несанкционированного доступа в информационные системы, но и длительное скрытое присутствие внутри инфраструктуры, управление процессами и последующее влияние на функционирование критически значимых объектов. Подобные кибератаки носят поэтапный характер: каждая стадия создаёт условия для следующей, что одновременно повышает эффективность воздействия и затрудняет обнаружение атаки [26, с. 30]. Особое значение имеет этап закрепления в поражённой системе – именно он позволяет долгое время сохранять контроль над инфраструктурой, оставаясь незамеченным. Это даёт возможность для выборочного или синхронизированного воздействия на отдельные элементы, что кратно увеличивает потенциальный ущерб.

С точки зрения обороны, вложение ресурсов в предотвращение взлома может быть менее эффективным, чем инвестиции в обнаружение закрепления и восстановление контроля. При современном уровне технологий абсолютно непроницаемых систем не существует. Рациональнее признать неизбежность отдельных успешных атак и сосредоточиться на сокращении времени обнаружения и минимизации последствий, однако такой подход редко встречается в национальных стратегиях кибербезопасности».

Кибератаки на критическую инфраструктуру превратились в устойчивый, воспроизводимый инструмент гибридного воздействия – гибкий и легко масштабируемый. Их развитие приобрело не эпизодический, а системный характер: растёт частота инцидентов и расширяется круг целей.

Рост числа кибератак на объекты критической инфраструктуры давно перестал быть случайностью и превратился в устойчивый тренд. Важно не только то, что атаки учащаются, но и то, как меняется их характер: они становятся более скоординированными, целенаправленными и разрушительными. Количественная динамика подобных атак позволяет оценить масштабы их распространения и подтвердить переход киберпространства в категорию самостоятельной сферы международного противоборства (рисунок 6).

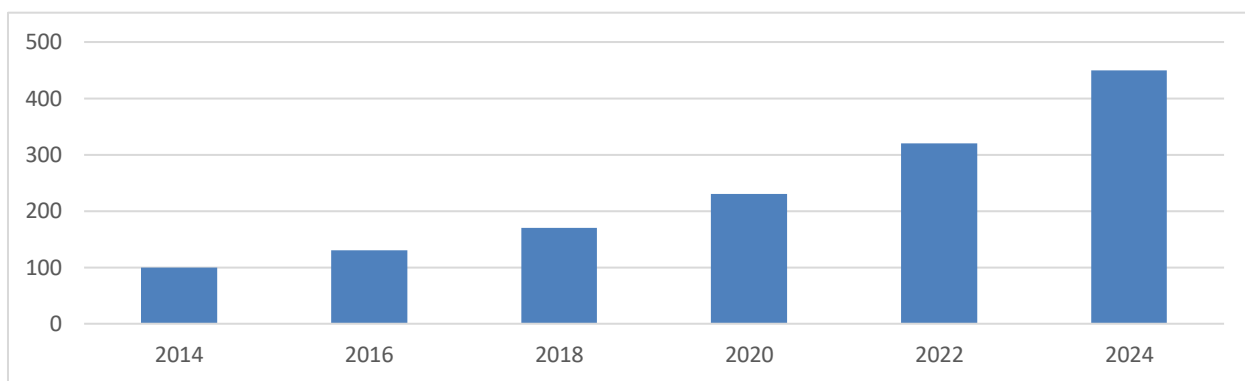


Рисунок 6 – Индексная динамика киберинцидентов в отношении объектов критической инфраструктуры (2014=100) [54]

Исследование демонстрирует устойчивую восходящую динамику киберинцидентов в отношении объектов критической инфраструктуры в период 2014–2024 гг. Использование индексного подхода позволяет выявить не абсолютные значения атак, а общую тенденцию их ускоренного роста, что является более корректным с научной точки зрения ввиду ограниченной сопоставимости открытых статистических источников.

С 2014 по 2019 гг. наблюдается постепенное увеличение индекса с 100 до 195 пунктов, что отражает этап становления киберпространства как отдельной сферы международной конфликтности. В этот период атаки носят преимущественно локальный и экспериментальный характер, затрагивая отдельные элементы цифровой и промышленной инфраструктуры [15, с. 38].

Начиная с 2020 г. фиксируется ускорение роста киберинцидентов, что связано с усилением цифровизации критически важных систем и ростом геополитической напряжённости. К 2024 г. индекс достигает 450 пунктов, что свидетельствует о более чем четырёхкратном увеличении интенсивности киберугроз по сравнению с базовым уровнем.

Приведённые данные ставят под сомнение распространённый тезис о том, что киберугрозы носят преимущественно «точечный» или «локальный» характер. Четырёхкратный рост за десятилетие свидетельствует о системной, а не эпизодической природе явления. С методологической точки зрения важно другое:

традиционные методы прогнозирования, экстраполирующие прошлые тренды, могут оказаться бесполезными в условиях, когда сам характер угроз меняется быстрее, чем успевают обновляться статистические модели. Поэтому ориентация исключительно на количественные показатели без качественного анализа трансформации атак представляется рискованной

Таким образом, рассмотренные кейсы обнаруживают не просто расширение набора инструментов, а принципиально иную логику: в гибридных конфликтах победа достигается не уничтожением армии противника, а разрушением его способности координировать собственные действия. Атака на трубопровод не убивает солдат, но парализует экономику. Информационная кампания не захватывает территорию, но подрывает доверие к власти. Это означает, что традиционные критерии «выигрыша» и «проигрыша» в войне перестают работать. Государство может не проиграть ни одного сражения и при этом потерять управление, устойчивость и легитимность. Данное обстоятельство меняет само понятие безопасности: она теперь зависит не столько от военной силы, сколько от способности сохранять координацию между армией, экономикой, информационным пространством и цифровой инфраструктурой в условиях одновременного давления по всем направлениям.

Глава 2 Противодействие гибридным угрозам и перспективы международной безопасности

2.1 Роль ООН, НАТО и ЕС в обеспечении безопасности и противодействии гибридным угрозам

Распространение гибридных конфликтов, рост числа кибератак, развитие цифровых платформ и усиление роли негосударственных акторов привели к существенной трансформации механизмов международной безопасности. Если в конце XX века ключевыми задачами международных организаций оставались предотвращение вооружённых конфликтов, контроль над вооружениями и миротворческое посредничество, то в современных условиях приоритет всё в большей степени смещается в сферу противодействия информационным операциям, защите критической инфраструктуры, регулированию цифрового пространства и предотвращению киберэскалации [34].

Анализ современных конфликтов показывает, что гибридные угрозы характеризуются высокой скоростью распространения, сложностью идентификации источника воздействия и сочетанием военных и невоенных инструментов давления. В этих условиях особое значение приобретает способность международных институтов адаптироваться к новым форматам противоборства и формировать многоуровневые механизмы коллективного реагирования. Наиболее значимую роль в данном процессе играют Организация Объединённых Наций, Организация Североатлантического договора и Европейский союз [54].

На глобальном уровне ключевую нормативно-правовую функцию продолжает выполнять Организация Объединённых Наций. В условиях роста цифровых угроз деятельность организации была существенно расширена за счёт включения вопросов международной информационной безопасности в повестку Генеральной Ассамблеи и Совета Безопасности. В период с 2018 по 2024 гг. в рамках рабочих групп ООН по вопросам кибербезопасности было проведено более 40 межгосударственных

консультационных сессий, посвящённых вопросам защиты критической инфраструктуры, предотвращения киберэскалации и выработки принципов ответственного поведения государств в цифровой среде. Существенное значение в данном направлении имеют доклады Группы правительственных экспертов ООН, закрепившие базовые нормы международного взаимодействия в киберпространстве [56].

Несмотря на высокий уровень международной легитимности, эффективность механизмов ООН в противодействии гибридным угрозам остаётся ограниченной. Ключевой проблемой выступает сложность достижения консенсуса между постоянными членами Совета Безопасности по вопросам атрибуции кибератак, определения ответственности государств и применения коллективных мер реагирования. В результате организация сохраняет высокий потенциал в сфере нормотворчества, однако её возможности в части оперативного реагирования на быстроразвивающиеся гибридные угрозы остаются ограниченными [1; 59].

В отличие от ООН, Организация Североатлантического договора ориентируется преимущественно на практические механизмы оперативного реагирования. Поворотным моментом стали масштабные кибератаки на Эстонию в 2007 г., после которых в Таллине был создан Центр передового опыта НАТО по сотрудничеству в области киберобороны. Последующее развитие цифровой стратегии альянса привело к признанию киберпространства самостоятельной операционной средой наряду с сушей, морем, воздухом и космосом. По официальным данным НАТО, совокупные расходы стран альянса на развитие киберкомандований, цифровых систем защиты и информационной инфраструктуры в период 2016–2024 гг. увеличились более чем в 2,3 раза [31].

Дополнительным индикатором институциональной адаптации НАТО выступает расширение масштабов международных киберучений. Если в учениях *Locked Shields* в 2014 г. принимали участие представители 16 государств, то в 2024 г. число участников превысило 40 стран, а общее количество специалистов составило более 4000 человек. Подобная динамика свидетельствует о переходе

кибербезопасности из вспомогательного направления в число приоритетных компонентов коллективной обороны [49].

Особое место в системе противодействия гибридным угрозам занимает Европейский союз, формирующий комплексную модель реагирования, сочетающую цифровое регулирование, санкционную политику и стратегические коммуникации. После 2014 г. институты Европейского союза существенно усилили внимание к вопросам противодействия дезинформации, киберугрозам и внешнему информационному воздействию. В 2015 г. была создана группа *East StratCom Task Force*, специализирующаяся на мониторинге информационных операций, а в 2019 г. начал действовать механизм *Cyber Diplomacy Toolbox*, предусматривающий возможность применения ограничительных мер в отношении субъектов, причастных к масштабным кибератакам [50].

По данным Европейского агентства по кибербезопасности, только в 2023 г. в странах Европейского союза было зафиксировано более 330 крупных инцидентов, затронувших энергетическую, финансовую, транспортную и телекоммуникационную инфраструктуру. Наиболее уязвимыми направлениями стали государственные цифровые сервисы, логистические сети и медицинская инфраструктура. Выявленная динамика подтверждает, что цифровая устойчивость становится одним из ключевых элементов современной европейской безопасности [47].

Для более детального сопоставления подходов рассматриваемых организаций целесообразно систематизировать их ключевые механизмы противодействия гибридным угрозам (таблица 5).

Таблица 5 – Сравнительный анализ механизмов противодействия гибридным угрозам в деятельности международных организаций [55]

Организация	Основные инструменты	Практические материалы	Ограничения	Ключевая тенденция
1	2	3	4	5
ООН	Резолюции, экспертные группы, международные соглашения	Нормотворчество, дипломатическое посредничество	Сложность консенсуса, низкая оперативность	Правовая институционализация

1	2	3	4	5
НАТО	Коллективная оборона, киберучения, разведывательная координация	<i>Locked Shields, CCCDCOE, совместные кибероперации</i>	Ограниченность рамками альянса	Милитаризация киберзащиты
ЕС	Санкционные механизмы, цифровое регулирование, стратегические коммуникации	<i>ENISA, East StratCom, Cyber Diplomacy Toolbox</i>	Ограниченный единый военный потенциал	Интеграция цифровой безопасности

Сопоставление характеристик свидетельствует о существенных различиях в институциональных моделях реагирования. Деятельность ООН ориентирована преимущественно на формирование международно-правовых норм, что обеспечивает высокий уровень политической легитимности, однако снижает скорость принятия решений в условиях быстро меняющейся цифровой среды. НАТО демонстрирует наиболее высокий уровень оперативной адаптации, концентрируясь на практической подготовке, коллективной киберзащите и интеграции цифровых угроз в военное планирование. Европейский союз занимает промежуточное положение, сочетая инструменты нормативного регулирования, санкционного давления и защиты цифровой инфраструктуры [45].

Таким образом, ООН хороша для долгосрочных норм, но бесполезна при срочной атаке. НАТО оперативна, но только для своих членов. ЕС создаёт правила, но не может их защитить силой. Каждая организация закрывает свой сегмент, но их усилия не складываются в единую систему. Пока сохраняется этот разрыв, государства будут полагаться на собственные силы, а гибридные атаки – оставаться эффективными.

Различия в подходах находят количественное и организационное выражение в показателях активности за 2025 г. Сравнение масштабов учений, бюджетов и итоговых механизмов позволяет оценить практическую отдачу каждой из институциональных моделей (таблица 6).

Таблица 6 – Масштаб оперативной и институциональной активности международных организаций в сфере кибербезопасности и гибридных угроз (2025 г.) [44]

Параметр	НАТО	Евросоюз (ЕС)	ООН
Крупнейшее киберобучение года	<i>Cyber Coalition 2025</i> 1300 участников из 29 стран НАТО и 7 стран-партнеров	<i>Cyber Europe</i>	Отсутствуют (не проводят боевые учения)
Бюджет на внутреннюю безопасность/устойчивость	Входит в оборонный бюджет (около 2 % ВВП)	6, 84 млрд евро (предлагается мый бюджет Фонда внутренней безопасности на 2028-2034 гг.)	Специализированного бюджета нет
Ключевой механизм/Результат 2025 г.	Кибератаки на критическую инфраструктуру (отработка защиты энергосетей и космоса)	«Оборонные технологии» (добавлены в программу <i>Horizon Europe</i> как 4-й сектор, финансирование двойного назначения)	Глобальный механизм (<i>Global Mechanism</i>) (создан по итогам работы группы <i>OEWG</i> , первый постоянный механизм ООН по кибербезопасности)

Исследуемые данные подтверждают специализацию организаций. НАТО делает ставку на масштабируемую оперативную подготовку (учения с участием 1300 военных и гражданских специалистов), отрабатывая защиту критической инфраструктуры. Евросоюз, в свою очередь, концентрируется на финансовой и регуляторной адаптации, перенаправляя миллиарды евро (6,84 млрд евро на следующие 7 лет) и программы *Horizon Europe* под задачи «двойного назначения» и оборонных технологий. ООН, оставаясь в рамках дипломатической парадигмы, завершила 4-летний цикл переговоров созданием нового «Глобального механизма», что демонстрирует способность достигать консенсуса даже в условиях геополитического кризиса [31].

Таким образом, анализ деятельности ООН, НАТО и ЕС выявляет фрагментарность международного реагирования на гибридные угрозы. Каждая из организаций обладает собственной специализацией: ООН – в нормотворчестве, НАТО – в оперативной подготовке, ЕС – в регуляторных механизмах. Однако ни одна из них не имеет полного набора инструментов для эффективного противодействия, а их усилия не скоординированы между собой. Это подводит к необходимости рассмотрения национальных стратегий, поскольку именно на уровне государств

формируются конкретные механизмы защиты критической инфраструктуры и обеспечения цифрового суверенитета.

2.2 Сравнительный анализ стратегий противодействия гибридным угрозам (США, ЕС и Россия)

Гибридизация современных конфликтов привела к формированию различных национальных моделей обеспечения безопасности. США, Европейский союз и Российская Федерация рассматривают гибридные угрозы как один из ключевых вызовов современности, однако используют различные подходы к их предупреждению и нейтрализации. Различия проявляются в понимании источников угроз, выборе приоритетных инструментов реагирования, уровне вовлечения государственных и негосударственных структур, а также в соотношении оборонительных и наступательных мер [11, с. 24].

Наиболее институционально развитая система противодействия гибридным угрозам сформирована в Соединённых Штатах Америки. Существенный пересмотр американского подхода начался после масштабных киберинцидентов 2016–2017 гг., а также атаки на топливную инфраструктуру *Colonial Pipeline* в 2021 г. В обновлённой Национальной стратегии кибербезопасности США особый акцент был сделан на проактивное выявление угроз, защиту критической инфраструктуры, развитие наступательных кибервозможностей и интеграцию частного сектора в систему национальной безопасности. По данным Агентства по кибербезопасности и инфраструктурной безопасности США, только в 2024 г. объём федеральных инвестиций в цифровую безопасность превысил 13 млрд долл. [56].

Американская модель характеризуется высокой степенью интеграции разведывательных структур, оборонного сектора и технологических корпораций. Существенную роль играют Агентство национальной безопасности, Киберкомандование США, Министерство внутренней безопасности, а также крупнейшие частные IT-компании, участвующие в обмене данными об угрозах в режиме реального времени. Ключевым преимуществом американской модели

является возможность оперативного объединения военных, разведывательных и гражданских ресурсов в рамках единой системы реагирования [14, с. 55].

Европейский союз формирует иную модель противодействия, ориентированную преимущественно на повышение устойчивости цифровой среды, защиту инфраструктуры и нормативное регулирование цифрового пространства. После серии масштабных атак на энергетические и транспортные системы стран Европы в период 2020–2023 гг. были существенно расширены полномочия Европейского агентства по кибербезопасности, а также приняты обновлённые директивы *NIS2* и *Cyber Resilience Act*. По данным Европейской комиссии, совокупный объём инвестиций государств ЕС в развитие цифровой устойчивости и защиту критической инфраструктуры в 2023 г. превысил 11 млрд евро [30].

В отличие от США, европейская стратегия в меньшей степени ориентирована на наступательные инструменты и делает акцент на превентивное регулирование, стандартизацию цифровой инфраструктуры и снижение уязвимости частного сектора. Анализ европейской модели свидетельствует о том, что её сильной стороной выступает высокий уровень правовой детализации и межгосударственной координации, однако сложность согласования решений между государствами-членами может снижать скорость практического реагирования [12, с. 62].

Российская Федерация формирует стратегию противодействия гибридным угрозам на основе комплексного сочетания военных, информационных, технологических и нормативно-правовых инструментов. Базовыми документами в данной сфере выступают Стратегия национальной безопасности Российской Федерации, Доктрина информационной безопасности и Концепция внешней политики Российской Федерации. Особое внимание уделяется защите информационного суверенитета, устойчивости государственных цифровых систем, импортонезависимости программного обеспечения и развитию национальной криптографической инфраструктуры [1; 2].

Результаты исследования свидетельствуют о том, что все три модели имеют критический недостаток – они ориентированы на внутреннюю или блоковую логику

и не создают механизмов для глобальной координации, что и является главным вызовом.

По данным Министерства цифрового развития Российской Федерации, в 2024 г. количество отражённых атак на государственные информационные ресурсы превысило 95 тыс., что почти в 2 раза выше уровня 2021 г. [5]. Одновременно фиксируется рост инвестиций в развитие отечественных платформ, защищённых коммуникационных систем и технологий искусственного интеллекта, применяемых в сфере мониторинга угроз. Анализ российской модели показывает, что её ключевой особенностью выступает высокий уровень централизации управления и ориентация на обеспечение цифрового суверенитета в условиях внешнего санкционного давления.

Исследование стратегий противодействия гибридным угрозам позволяет выявить ключевые различия в институциональных подходах к противодействию гибридным угрозам (таблица 7).

Таблица 7 – Сравнительный анализ стратегий противодействия гибридным угрозам США, ЕС и РФ [7, с. 15]

Государство/ объединение	Ключевые документы	Приоритетные инструменты	Сильные стороны	Основные ограничения	Доминирующая стратегия
США	Национальная стратегия кибербезопасности <i>National Defense Strategy</i>	Киберкомандование, разведка, частный сектор, наступательные операции	Высокая скорость реагирования, технологическое лидерство	Высокая зависимость от частных корпораций	Проактивное сдерживание
ЕС	<i>Cybersecurity Strategy, NIS2, Cyber Resilience Act</i>	Регулирование, стандартизация, санкции, инфраструктурная защита	Высокая нормативная устойчивость	Медленное согласование решений	Институциональная устойчивость
РФ	Стратегия национальной безопасности, Доктрина информационной безопасности	Централизованное управление, цифровой суверенитет, криптозащита	Высокая управляемость и автономность	Технологические ограничения внешней среды	Суверенная цифровая безопасность

Сравнение выявляет, что различия между стратегиями обусловлены не только технологическими возможностями, но и особенностями политико-институционального устройства. Американская модель строится на принципе упреждающего реагирования и допускает использование наступательных цифровых инструментов. Европейский союз концентрируется на минимизации уязвимостей через нормативное регулирование и коллективную координацию. Российская модель ориентирована на обеспечение внутренней устойчивости, контроль критически важных цифровых систем и снижение внешней технологической зависимости.

Для более наглядного понимания стратегических приоритетов целесообразно сопоставить распределение ресурсов по основным направлениям противодействия гибридным угрозам (рисунок 7).

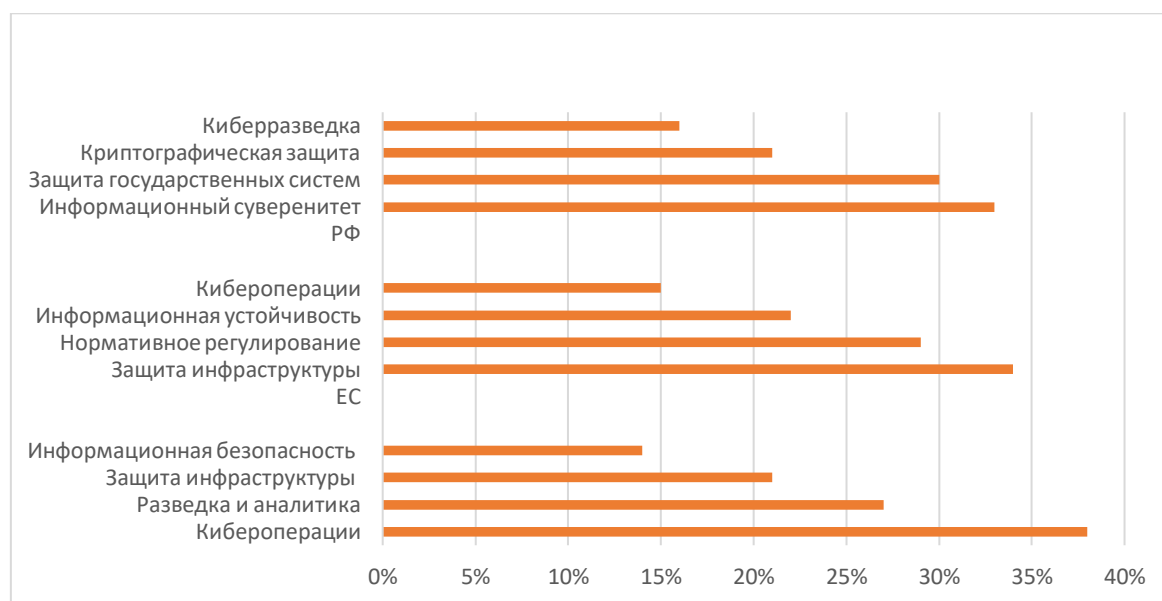


Рисунок 7 – Приоритетные направления стратегий противодействия гибридным угрозам [19, с. 11]

Из этого следует, что каждая из рассматриваемых моделей отражает собственное понимание природы гибридных угроз. В США приоритет смещён в сторону активного выявления и нейтрализации угроз ещё на этапе их формирования, что соответствует концепции *forward defense*. Европейский союз делает ставку на снижение системной уязвимости за счёт нормативного регулирования и повышения

цифровой устойчивости инфраструктуры. Российская Федерация концентрирует усилия на защите информационного суверенитета, автономности цифровых платформ и устойчивости государственных систем управления. Выявленные различия свидетельствуют о постепенном формировании нескольких конкурирующих моделей цифровой безопасности, каждая из которых отражает особенности политической организации, технологической базы и внешнеполитических приоритетов [16, с. 26].

Важно отметить, что представленные на рисунке 7 различия не являются недостатками сами по себе – каждая модель адекватна политическим и технологическим реалиям своего субъекта. Однако в условиях глобальной цифровой взаимозависимости именно отсутствие совместимости между этими подходами создаёт системный риск. Проактивное сдерживание США может вступать в противоречие с требованиями цифрового суверенитета России, а европейское регулирование – не учитывать реалии киберпространства как глобальной среды. Следовательно, разработка механизмов межмодельной координации становится задачей не менее важной, чем совершенствование каждой из моделей в отдельности.

Таким образом, международные организации производят впечатление активности, но их усилия складываются в мозаику без единого узора. ООН создаёт правила, которые никто не может принудительно исполнить. НАТО тренирует киберзащиту, но только для своих членов и только в рамках военной логики. ЕС разрабатывает регуляции, но не имеет механизмов их силовой защиты. В результате каждая организация закрывает свой сегмент проблемы, но ни одна не охватывает её целиком. Главный вывод здесь не в том, что они плохи или хороши, а в том, что их специализация не компенсирует отсутствие координации. Проблема гибридных угроз не имеет «ведомственной прописки» – она одновременно военная, правовая, технологическая и информационная. А существующие институты, каждый в своей «коробке», не умеют работать на стыках. Пока этот разрыв сохраняется, государства будут полагаться на собственные силы, а гибридные атаки – оставаться эффективным инструментом давления.

2.3 Цифровые технологии, негосударственные акторы и перспективы развития международной безопасности до 2035 года

В современных конфликтах цифровая среда перестала быть исключительно каналом передачи информации и превратилась в самостоятельное пространство политического давления, информационного противоборства и координации различных форм гибридного воздействия. Как отмечает Мануэль Кастельс, в условиях формирования сетевого общества информационные потоки становятся одним из ключевых источников политического влияния и перераспределения власти. Усиление роли цифровых платформ связано прежде всего с изменением модели потребления информации: значительная часть аудитории получает новости не через традиционные средства массовой информации, а через *Telegram*, *TikTok*, *YouTube* и социальные сети. Это ускорило распространение политического контента и одновременно усложнило контроль над информационными потоками [32, с. 144].

Наиболее заметно данная тенденция проявилась после 2020 г. Международные события последних лет показали, что информационная повестка всё чаще формируется не официальными источниками, а цифровыми платформами и сетевыми сообществами. В условиях высокой скорости распространения контента даже локальные информационные поводы способны за короткое время приобретать глобальный масштаб. Дополнительную роль играют алгоритмы платформ, автоматически продвигающие материалы с высоким уровнем эмоциональной реакции пользователей [21, с. 43].

В результате информационное воздействие постепенно становится сопоставимым по значимости с традиционными инструментами политического давления. Особенно активно цифровые технологии используются для формирования общественных настроений, усиления социальной поляризации и распространения дезинформации. При этом информационные кампании редко существуют отдельно от других форм гибридного воздействия. Как правило, они сопровождаются кибератаками, анализом цифрового поведения аудитории и автоматизированным продвижением контента [18, с. 36].

Наиболее распространённые цифровые инструменты, используемые в современных гибридных конфликтах, представлены в таблице 8.

Таблица 8 – Использование цифровых технологий в гибридных конфликтах [12, с. 62]

Направление	Используемые инструменты	Практический эффект
Информационные операции	<i>Telegram, X, YouTube, TikTok</i>	Быстрое распространение политического контента
Кибероперации	DDoS-атаки, вредоносное ПО, взлом сетей	Нарушение работы цифровой инфраструктуры
Анализ поведения аудитории	<i>Big Data</i> , алгоритмы ИИ	Выявление уязвимых информационных групп
Автоматизированное продвижение	Бот-сети, алгоритмические рекомендации	Искусственное увеличение охвата публикаций
Цифровая разведка	<i>OSINT</i> , спутниковые сервисы, геолокация	Сбор оперативной информации

Цифровые технологии наиболее эффективно функционируют не изолированно, а в рамках единой информационно-кибернетической кампании. Сочетание социальных платформ, алгоритмического продвижения, анализа больших данных и киберопераций позволяет воздействовать одновременно на информационную среду, общественные настроения и критическую инфраструктуру.

Цифровые инструменты работают как система, а не как набор опций. Отдельно взятая DDoS-атака или фейковая кампания в соцсетях редко приводит к результату. Но когда кибератака подкрепляется информационным сопровождением, а анализ данных позволяет точно бить по уязвимой группе, эффективность многократно возрастает. Противодействие поэтому должно быть не отраслевым, а межведомственным – пока же оно остаётся фрагментированным

Информационная кампания в период президентских выборов в США в 2016 г. включала использование фальшивых аккаунтов, таргетированной рекламы и автоматизированных бот-сетей. Анализ этой кампании указывает на переход от массового информационного воздействия к персонализированным моделям цифрового влияния, ориентированным на конкретные социальные и политические группы [13, с. 68].

Технологии искусственного интеллекта существенно трансформируют гибридные конфликты. Алгоритмы машинного обучения уже применяются для анализа поведения аудитории, прогнозирования общественных реакций и автоматического создания контента, включая дипфейки и сфабрикованные видеообращения. Это повышает точность воздействия и позволяет адаптировать цифровые кампании под конкретные социальные группы, при этом верификация источников информации значительно затрудняется.

В военной сфере влияние ИИ также приобретает особое значение. Алгоритмы используются в системах управления беспилотными летательными аппаратами как разведывательного, так и ударного назначения. В результате происходит постепенное стирание границ между традиционными военными действиями и цифровыми формами противоборства [35].

Конфликт в Нагорном Карабахе (2020) наглядно продемонстрировал трансформацию роли БПЛА. Азербайджанская сторона применяла турецкие *Bayraktar TB2* и израильские дроны-камикадзе *IAI Harop* для поражения армянских зенитных комплексов, танков и артиллерии. Видеозаписи ударов оперативно распространялись через *Telegram*-каналы и *X*, что выполняло не только информационную, но и психологическую функцию: деморализация противника и формирование образа технологического превосходства. При этом сами дроны управлялись с использованием спутниковой сети и цифровых каналов связи, а операторы находились вне зоны боевых действий. Такой способ ведения войны снижает порог эскалации: применение БПЛА не требует ввода наземных сил и долгое время остаётся в «серой зоне» международно-правовой квалификации [36].

Рассмотренный кейс показывает, что цифровые технологии всё чаще используются не только непосредственно на поле боя, но и в качестве самостоятельного инструмента воздействия на противника. Наряду с применением беспилотных систем существенное значение приобретают кибероперации, позволяющие оказывать давление на государственные институты, объекты критической инфраструктуры и информационное пространство без прямого использования вооружённой силы. В результате киберпространство постепенно

превращается в отдельную сферу международного противоборства, в рамках которой последствия атак могут быть сопоставимы с результатами традиционных военных действий [22, с. 726].

Показательным примером являются кибератаки на Эстонию (2007), которые часто рассматриваются как первый случай киберкомпонента в межгосударственном конфликте на уровне НАТО. После переноса памятника «Бронзовый солдат» в Таллине последовали массированные DDoS-атаки на сайты парламента, банков, министерств и средств массовой информации. Трафик шёл из десятков стран, причём значительная его часть генерировалась бот-сетями из заражённых домашних компьютеров. Эстония, одна из самых цифровизированных стран мира, оказалась парализованной в своей электронной администрации на несколько недель. Аналитическая значимость этого кейса заключается в том, что он выявил «слепую зону» коллективной обороны: атака не достигала порога вооружённого нападения по статье 5 Вашингтонского договора, но наносила реальный ущерб государственным функциям [35].

Для понимания механизмов, через которые цифровая среда трансформирует конфликты, необходимо рассмотреть последовательность этапов информационно-кибернетического воздействия (рисунок 8).

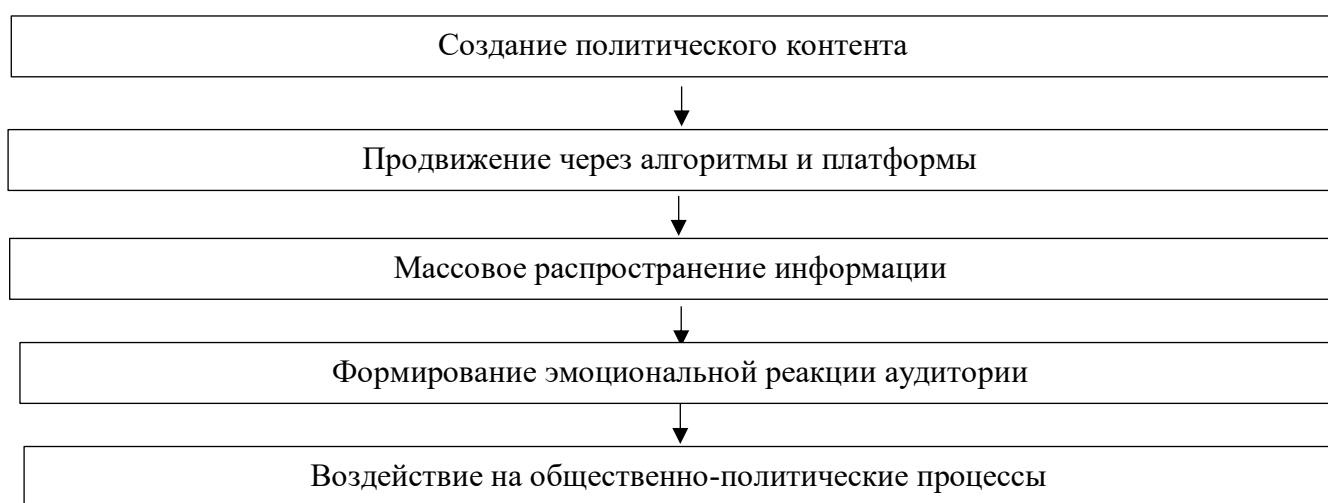


Рисунок 8 – Механизм информационного воздействия в цифровой среде [14, с. 58]

Схема показывает, что ключевой особенностью цифровой среды является наличие положительной обратной связи между пользовательской активностью и алгоритмическим продвижением контента. Исследования *Massachusetts Institute of Technology* показывают, что эмоционально насыщенные и конфликтогенные сообщения распространяются в цифровых сетях значительно быстрее нейтрального информационного контента [42].

Алгоритмы цифровых платформ ориентированы на увеличение пользовательской вовлечённости. В результате приоритет получают материалы, вызывающие сильную эмоциональную реакцию аудитории. Это создаёт условия для ускоренного распространения конфликтогенного контента, формирования информационных пузырей и усиления социальной поляризации даже при отсутствии централизованной координации со стороны конкретных политических акторов [23, с. 327].

Технологические компании, разрабатывающие алгоритмы рекомендаций, объективно участвуют в формировании конфликтного потенциала, независимо от своих намерений. Однако ни национальное законодательство, ни международные соглашения пока не предлагают механизмов регуляции этой сферы, оставляя цифровые платформы в положении «невольных соучастников» гибридных кампаний.

Кризис в Мьянме в 2017 г. стал одним из наиболее показательных примеров влияния цифровых платформ на развитие социально-политической эскалации. Согласно докладом Организации Объединённых Наций, алгоритмы платформы *Meta Platforms* способствовали распространению радикального контента, дезинформации и материалов, содержащих признаки разжигания межэтнической вражды. Существенным фактором стала ограниченность механизмов локальной модерации и недостаточная адаптация платформы к языковым и культурным особенностям региона. Это затруднило своевременное выявление и ограничение конфликтогенного контента.

Данный пример свидетельствует о том, что цифровые платформы способны выступать не только каналом распространения информации, но и самостоятельным фактором усиления конфликтных процессов и социальной напряжённости [38].

Распространение цифровых технологий оказывает влияние не только на инструменты ведения современных конфликтов, но и на состав их участников. Если ранее ключевую роль в международном противоборстве играли преимущественно государства и их вооружённые силы, то развитие информационных платформ, цифровых коммуникаций и киберпространства существенно расширило возможности негосударственных акторов. Новые технологические решения позволяют частным структурам, хакерским группам и сетевым сообществам осуществлять деятельность, масштабы которой в отдельных случаях сопоставимы с возможностями государственных институтов. В результате трансформация технологий сопровождается изменением субъектной структуры международной безопасности и усилением роли негосударственных участников конфликтов.

Растёт значение частных военных компаний (ЧВК). В регионе Сахель (Мали, Нигер, Буркина-Фасо) частная военная компания «Вагнер» и связанные с ней структуры (впоследствии – «Африканский корпус»), выполняли функции, традиционно закреплённые за регулярными армиями: охрана объектов, сопровождение колонн, подготовка местных формирований, разведка [40].

В гибридных конфликтах ЧВК позволяют государству сохранять двусмысленность участия. Данный механизм, известный как «правдоподобное отрицание» (*plausible deniability*), снижает политические и юридические риски, поскольку официальные структуры могут отрицать непосредственное участие в конфликте при формальном использовании частных организаций.

Деятельность современных ЧВК тесно связана с цифровыми технологиями и включает применение OSINT-разведки, защищённых каналов связи, спутниковых систем и цифровых средств координации действий [42].

Транснациональные сети формируют новую архитектуру власти, в которой влияние всё меньше зависит от государственных границ. Хакерские группы способны оказывать воздействие на критически важные объекты инфраструктуры. Так, в 2021 г. группа *DarkSide* атаковала *Colonial Pipeline*. В результате был временно остановлен крупнейший топливный трубопровод восточного побережья США, что

привело к перебоям в поставках топлива, росту цен и введению режима чрезвычайной ситуации в ряде штатов.

Атака показала не только экономические последствия кибератак, но и их политическое значение. Дополнительный интерес представляет организационная модель *DarkSide*, которая фактически функционировала как коммерческая структура – с технической поддержкой, системой переговоров и распределением прибыли между участниками [47].

Сегодня хакерские группы сопоставимы по своим возможностям с крупными государствами. Современные технологии радикально снизили барьеры входа: группа из нескольких человек, использующая модель «вымогательство-как-услуга» (*ransomware-as-a-service*), способна нанести ущерб в миллиарды долларов – кейс *Colonial Pipeline* служит тому подтверждением. Сетевые сообщества могут мобилизовать тысячи добровольцев для скоординированных действий без формальной иерархии и явных командиров. Сравнительный анализ ключевых типов таких акторов представлен в таблице 9.

Таблица 9 – Сравнительный анализ негосударственных акторов в гибридных конфликтах [44]

Тип актора	Примеры	Основные функции	Специфика воздействия
Хакерские группы	<i>DarkSide (Colonial Pipeline), Anonymous</i>	Кибератаки, взлом, вымогательство	Паралич критической инфраструктуры; коммерческая мотивация
Частные военные компании (ЧВК)	«Вагнер» (Сахель), <i>Blackwater</i> (Ирак)	Охрана, разведка, боевые операции	Правдоподобное отрицание; обход официальных ограничений
Транснациональные платформы	<i>Facebook</i> (Мьянма), <i>Telegram, TikTok</i>	Алгоритмическое продвижение, модерация	Непреднамеренная эскалация; уязвимость к захвату повестки
Сетевые сообщества	<i>4chan, Reddit</i>	Мобилизация, координация, распространение	Отсутствие иерархии, низкий порог радикализации
OSINT-сети	<i>Bellingcat, Conflict Intelligence Team</i>	Цифровая разведка, верификация	Независимая верификация данных и повышение прозрачности конфликтов

Субъектная структура современных конфликтов постепенно меняется. Если ранее ключевыми участниками международного противоборства выступали преимущественно государства, то в цифровую эпоху существенное влияние начинают оказывать частные военные компании, хакерские сообщества, цифровые платформы и распределённые сетевые структуры.

Из этого следует, что традиционные механизмы международной безопасности, ориентированные исключительно на государства, перестают охватывать реальный спектр участников конфликтов. Хакерские группы и частные военные компании действуют вне рамок международно-правовых режимов, а цифровые платформы влияют на политические процессы без формальной ответственности. Указанные акторы не вписаны в существующую архитектуру безопасности, что создаёт зону правовой и институциональной неопределённости. Без выработки новых механизмов регулирования их деятельности гибридные угрозы будут только усиливаться.

Эта тенденция указывает на снижение чёткости границ между государственными и негосударственными формами воздействия. Частные структуры способны выполнять функции, традиционно характерные для государственных институтов, а цифровые платформы и сетевые сообщества получают возможность оказывать влияние на политические процессы, общественные настроения и информационную повестку в глобальном масштабе [27, с. 55].

Эффективность противодействия гибридным угрозам снижается прямо пропорционально степени изоляции каждого актора в отдельности. Государственные институты традиционно организованы по вертикальному иерархическому принципу – дипломатия, разведка, армия, правоохранительные органы. Однако цифровая среда и действующие в ней негосударственные сети функционируют по горизонтальным, децентрализованным алгоритмам. Это несоответствие структур и есть основная уязвимость. Пока официальные институты вырабатывают консолидированный ответ (что требует времени и согласования), информационно-кибернетическое воздействие уже достигает своих целей. Эстонский кризис 2007 г. – классическая иллюстрация: страна – член НАТО с передовым уровнем цифровизации не смогла оперативно

отреагировать на DDoS-атаки именно потому, что процедуры коллективной обороны не предусматривали подобного сценария [48].

Современная система международных отношений вступает в этап глубокой структурной перестройки. Усиление технологической конкуренции, рост числа киберинцидентов, распространение искусственного интеллекта, развитие автономных систем вооружения и увеличение роли негосударственных акторов формируют качественно новую архитектуру международного противоборства. В отличие от предшествующих этапов, когда ключевым индикатором стратегической мощи выступали численность вооружённых сил и объём традиционных вооружений, в ближайшие десятилетия определяющее значение всё в большей степени будет принадлежать цифровому суверенитету, технологической автономности и способности государств защищать критическую инфраструктуру в условиях постоянного сетевого давления [25, с. 342].

Согласно данным Стокгольмского международного института исследования проблем мира, в 2024 г. мировые военные расходы достигли рекордного уровня и превысили 2,7 трлн долл., продемонстрировав крупнейший прирост за последнее десятилетие. Одновременно, по оценкам аналитических центров НАТО и Европейского агентства по кибербезопасности, количество крупных киберинцидентов в отношении объектов критической инфраструктуры за период 2015–2024 гг. увеличилось более чем в четыре раза. Данная динамика указывает на то, что к 2035 г. традиционные и цифровые компоненты безопасности будут окончательно интегрированы в единую систему стратегического планирования [52].

Особое влияние на дальнейшую трансформацию международной безопасности будет оказывать развитие искусственного интеллекта. Уже в настоящее время алгоритмы машинного обучения применяются для анализа разведывательных данных, автоматического распознавания целей, прогнозирования информационных кампаний и управления беспилотными платформами. По прогнозам международных аналитических агентств, к 2030 г. более 60 % ведущих армий мира будут использовать элементы автономного принятия решений в системах разведки, логистики и боевого управления. Это означает, что к середине следующего

десятилетия технологическое превосходство будет определяться не только количеством вооружений, но и уровнем алгоритмической интеграции военных систем.

Не менее значимой тенденцией выступает рост зависимости государств от цифровой инфраструктуры. Развитие умных энергосетей, цифрового государственного управления, облачных платформ и распределённых коммуникационных систем повышает эффективность государственного управления, однако одновременно увеличивает потенциальную уязвимость перед внешним воздействием. По оценкам Всемирного экономического форума, к 2030 г. более 75 % критически важных инфраструктурных процессов будут напрямую зависеть от сетевых цифровых систем, что существенно расширит спектр потенциальных целей для гибридного воздействия [59].

Для систематизации ключевых факторов, способных определить развитие международной безопасности в долгосрочной перспективе, целесообразно выделить основные прогнозные направления трансформации (таблица 10).

Таблица 10 – Ключевые направления трансформации международной безопасности до 2035 г. [28, с. 325]

Направления	Прогнозируемые изменения	Потенциальные последствия	Ключевая тенденция
Искусственный интеллект	Интеграция ИИ в системы управления, разведки и анализа	Сокращение времени принятия решений, рост автономности	Алгоритмизация безопасности
Беспилотные системы	Массовое применение автономных платформ	Снижение порога применения силы	Дистанционное противоборство
Киберпространство	Рост атак на критическую инфраструктуру	Экономическая дестабилизация, кризисы управления	Цифровизация конфликтов
Информационная среда	Распространение дипфейков и ИИ-контента	Снижение доверия к институтам	Алгоритмическая дезинформация
Негосударственные акторы	Усиление влияния ЧВК, платформ, хакерских групп	Размывание монополии государства на применение силы	Сетевая конфликтность
Международное право	Разработка новых цифровых норм	Формирование новых режимов регулирования	Правовая адаптация

Ключевой особенностью прогнозируемого периода станет одновременное усиление технологической взаимозависимости и рост системной уязвимости государств. Если ранее военная мощь ассоциировалась преимущественно с материальными ресурсами и численностью вооружённых сил, то в перспективе до 2035 г. стратегическое преимущество всё в большей степени будет зависеть от способности государств защищать собственную цифровую экосистему, контролировать критически важные данные и обеспечивать устойчивость информационного пространства [55].

Отдельного внимания заслуживает прогноз изменения структуры международной конфликтности. Анализ современных кейсов – от кибератак на энергетическую инфраструктуру до информационных операций в социальных сетях позволяет предположить, что к 2035 г. доля конфликтов, сопровождаемых выраженным цифровым компонентом, продолжит устойчиво расти. Для более наглядного отражения данной тенденции целесообразно сопоставить прогнозируемое изменение структуры международных угроз (рисунок 9).

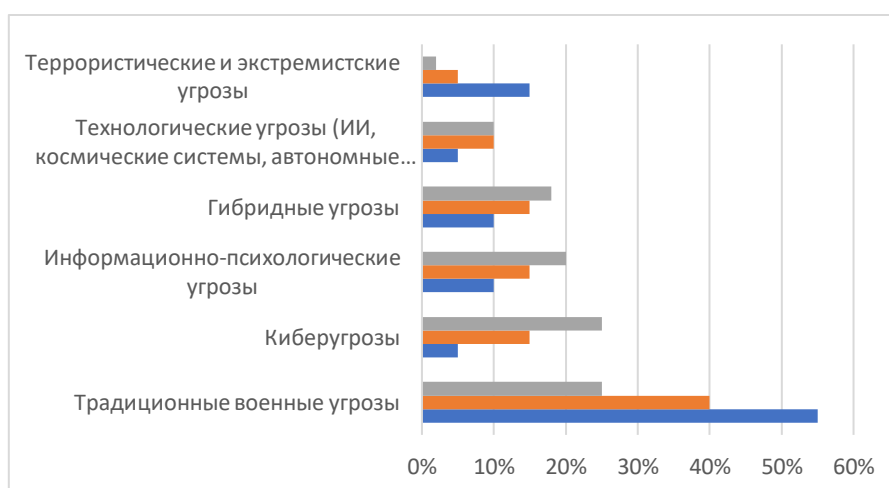


Рисунок 9 – Прогноз изменения структуры международных угроз до 2035 г., % [34]

Согласно прогнозу, в течение ближайшего десятилетия удельный вес традиционных вооружённых угроз в общей структуре международной конфликтности будет постепенно снижаться, уступая место гибридным и цифровым формам противоборства. При этом речь не идёт об исчезновении классической

военной силы. Напротив, вооружённый компонент сохранит стратегическое значение, однако его применение всё чаще будет сопровождаться кибероперациями, информационным воздействием, экономическим давлением и использованием автономных цифровых платформ. Динамика свидетельствует о формировании многоуровневой модели конфликтности, в которой физическое, информационное и цифровое пространство окончательно интегрируются в единую среду международного противоборства [20, с. 230].

Предложенный прогноз основан на экстраполяции текущих трендов и не учитывает фактор «чёрных лебедей» – технологических прорывов или геополитических катаклизмов, способных радикально изменить представленную динамику. Тем не менее даже в рамках инерционного сценария очевидно, что традиционные вооружённые силы не исчезнут, но их роль трансформируется: они станут «силовым аргументом», применяемым только в связке с кибернетическими и информационными инструментами. Государства, которые продолжают готовиться к войнам XX в., рискуют оказаться неготовыми к конфликтам, где главные события разворачиваются не на поле боя, а в цифровом и информационном пространствах.

Не менее существенным фактором становится трансформация роли международных институтов. Анализ деятельности Организации Объединённых Наций, Организации Североатлантического договора и Европейского союза показывает, что существующие механизмы коллективной безопасности во многом создавались для реагирования на межгосударственные вооружённые конфликты XX в. Однако развитие анонимных киберопераций, алгоритмических информационных кампаний и деятельности транснациональных цифровых платформ формирует принципиально новые вызовы, требующие адаптации международно-правовых режимов, механизмов атрибуции и процедур коллективного реагирования [45].

Таким образом, современная система международной безопасности развивается в условиях усложнения структуры угроз и постепенного перехода от преимущественно государственно-центричной модели противоборства к многоуровневой системе взаимодействия государственных и негосударственных

акторов. Цифровые технологии, искусственный интеллект, беспилотные системы и сетевые коммуникации расширяют арсенал гибридного воздействия. Появляются новые каналы для политического, информационного и кибернетического давления. Рассмотренные примеры показывают: цифровое пространство уже не просто вспомогательная среда, а самостоятельная арена международного противоборства. Оно влияет на политическую стабильность, работу критической инфраструктуры и общественные настроения. Растёт и роль негосударственных акторов — частных военных компаний, хакерских сообществ, цифровых платформ, сетевых объединений. Их возможности порой сопоставимы с потенциалом небольших государств.

Ожидается дальнейшее усиление процессов цифровизации конфликтов, распространении автономных технологий и расширении практики применения гибридных инструментов воздействия. В этих условиях обеспечение международной безопасности всё в большей степени будет зависеть не только от военного потенциала государств, но и от их способности обеспечивать устойчивость цифровой инфраструктуры, эффективно противодействовать информационным и киберугрозам, а также адаптировать существующие механизмы международного сотрудничества к новым формам конфликтности. Это подтверждает необходимость совершенствования международных и национальных механизмов реагирования на гибридные угрозы в условиях продолжающейся трансформации мировой политической системы

Заключение

Международная безопасность представляет собой сложную и динамично развивающуюся систему, содержание которой изменялось вместе с трансформацией международных отношений. Проведённое исследование показало, что эволюция представлений о безопасности сопровождалась расширением круга угроз и переходом от преимущественно военно-политического понимания безопасности к комплексному подходу, учитывающему политические, экономические, информационные, технологические и гуманитарные факторы. Анализ основных теоретических подходов позволил установить, что современные концепции международной безопасности всё в большей степени ориентированы на изучение взаимосвязи традиционных и нетрадиционных угроз в условиях глобальной взаимозависимости государств.

Исследование современных угроз международной безопасности показало, что наряду с традиционными вооружёнными конфликтами возрастающее значение приобретают кибератаки, информационные операции, экономическое давление, международный терроризм и иные формы гибридного воздействия. Систематизация угроз позволила выявить их многоуровневый характер и установить, что современные риски всё чаще носят комплексный характер, сочетая инструменты различных сфер воздействия и затрудняя их своевременное выявление и нейтрализацию.

Основные подходы к исследованию гибридных конфликтов имеют как методологические возможности, так и ограничения. Установлено, что существующие концепции достаточно эффективно объясняют сочетание военных и невоенных методов воздействия, однако до настоящего времени отсутствует единый общепринятый подход к определению сущности гибридных угроз и их места в системе международной безопасности. Это свидетельствует о необходимости дальнейшего развития теоретико-методологических основ исследования гибридной конфликтности.

На основе анализа современных международных конфликтов выявлено, что традиционные угрозы претерпевают существенную трансформацию. Вооружённая сила остаётся важнейшим инструментом международного противоборства. Однако сегодня её применение почти всегда дополняется информационными кампаниями, экономическим давлением, кибероперациями и подключением негосударственных акторов. Особенно отчётливо эта тенденция видна на фоне растущей геополитической конкуренции между ведущими центрами силы.

Сирийский конфликт позволяет выделить ключевые черты современных гибридных войн. В них одновременно задействуются военные, политические, экономические, информационные и дипломатические рычаги. Кибератаки на критическую инфраструктуру – ещё одно подтверждение того, что цифровое пространство стало самостоятельной ареной борьбы. Оно напрямую влияет на устойчивость государств и работу стратегически важных систем.

Цифровые технологии и негосударственные акторы выходят на передний план. Искусственный интеллект, большие данные, социальные сети, беспилотники и цифровые платформы серьёзно расширяют возможности для информационного и кибернетического давления. Растёт и роль новых игроков: хакерских групп, частных военных компаний, сетевых сообществ, транснациональных платформ. Они способны влиять на международные процессы вне традиционной государственной политики.

ООН, НАТО и ЕС – каждая из этих организаций адаптирует свои механизмы безопасности к новым вызовам. Тем не менее сохраняются серьёзные ограничения. Сложно атрибутировать гибридные атаки, различаются национальные подходы, а международно-правовое регулирование цифровой сферы пока недостаточно эффективно.

Стратегии США, ЕС и России в области противодействия гибридным угрозам имеют как общие черты, так и заметные различия. Это показывает, что единого подхода сегодня не существует. Общей тенденцией является признание возрастающей роли кибербезопасности, защиты критической инфраструктуры и противодействия информационным воздействиям. В то же время различия

обусловлены особенностями внешнеполитических интересов, институциональной структуры и стратегических приоритетов каждого из рассматриваемых субъектов.

Прогноз развития международной безопасности до 2035 г. указывает на дальнейшее усиление процессов гибридизации международных конфликтов. Ожидается рост значения искусственного интеллекта, автономных систем вооружения, цифровых платформ и киберпространства как самостоятельной сферы противоборства. В этих условиях обеспечение международной безопасности будет всё в большей степени зависеть от способности государств адаптироваться к новым технологическим реалиям, обеспечивать устойчивость критической инфраструктуры и совершенствовать механизмы международного сотрудничества в сфере противодействия гибридным угрозам.

Практическая значимость работы видится в возможности использовать её выводы для корректировки национальных стратегий кибербезопасности, особенно в части противодействия децентрализованным негосударственным акторам.

Таким образом, проведённое исследование подтверждает, что гибридные угрозы становятся одним из ключевых факторов трансформации современной системы международной безопасности. Их комплексный и многоуровневый характер требует совершенствования существующих подходов к обеспечению безопасности как на национальном, так и на международном уровнях, а также дальнейшего развития международно-правовых и институциональных механизмов реагирования на новые вызовы глобальной безопасности

Список использованных источников

- 1 Устав Организации Объединённых Наций: подписан 26 июня 1945 г. // Организация Объединённых Наций. URL: <https://www.un.org/ru/about-us/un-charter> (дата обращения 19.04.2026).
- 2 Конституция Российской Федерации от 12 декабря 1993 г. (с учетом поправок, внесенных законами РФ о поправках в Конституции РФ от 30 декабря 2008 г. № 6-ФКЗ, от 30 декабря 2008 г. № 7-ФКЗ, от 5 февраля 2014 г. № 2-ФКЗ, от 01 июля 2020 г. № 11-ФКЗ, от 06 октября 2022 г.) // Собрание законодательства Российской Федерации. – 2020. – № 31, ст. 4412.
- 3 Концепция внешней политики Российской Федерации: Указ Президента РФ от 31 марта 2023 г. № 229 // Собрание законодательства Российской Федерации. – 2023. – № 14, ст. 2406.
- 4 О Стратегии национальной безопасности Российской Федерации: Указ Президента РФ от 2 июля 2021 г. № 400 // Собрание законодательства Российской Федерации. – 2021. – № 27 ч. II, ст. 5351.
- 5 Военная доктрина Российской Федерации: утв. Президентом РФ 25 декабря 2014 г. № Пр-2976 // Российская газета. 2014. – 30 декабря.
- 6 Арбатов А. Г. Международная безопасность в эпоху технологических изменений. М. : ИМЭМО РАН, 2022. 384 с.
- 7 Барановский В. Г. Современные международные угрозы и безопасность // Мировая экономика и международные отношения. 2021. Т. 65, № 8. С. 5–17.
- 8 Богатуров А. Д. Международные отношения и мировая политика: учебник. М. : Аспект Пресс, 2021. 512 с.
- 9 Воскресенский А. Д. Азиатско-Тихоокеанский регион в мировой политике // Полис. Политические исследования. 2022. № 4. С. 26–41.
- 10 Дугин А. Г. Геополитические изменения в XXI веке // Международная жизнь. 2022. № 7. С. 44–59.
- 11 Иванов С. А. Киберугрозы критической инфраструктуре государства // Вопросы кибербезопасности. 2021. № 3. С. 12–24.

- 12 Ильин М. В. Цифровизация международных конфликтов // Политическая наука. 2023. № 2. С. 61–79.
- 13 Кокошин А. А. Технологический фактор в военной стратегии // Национальная оборона. 2022. № 7. С. 22–35.
- 14 Коргунюк Ю. Г. Информационная безопасность и политические риски // Полис. 2021. № 5. С. 55–70.
- 15 КОРТУНОВ А. В. Гибридные угрозы как фактор международной нестабильности // Международная аналитика. 2021. Т. 12, № 4. С. 24–39.
- 16 Косолапов Н. А. Эволюция конфликтности в мировой политике // Полис. 2020. № 6. С. 17–31.
- 17 Лукьянов Ф. А. Трансформация международного порядка в XXI веке // Россия в глобальной политике. 2022. № 3. С. 8–21.
- 18 Манойло А. В. Гибридные войны в системе современных международных отношений // Вестник Московского университета. Серия 12. 2021. № 5. С. 34–48.
- 19 Манойло А. В. Информационные войны и психологические операции. М. : Горячая линия Телеком, 2020. 382 с.
- 20 Никитин А. И. Киберпространство как новая сфера международного противоборства // Международные процессы. 2021. Т. 19, № 2. С. 32–49.
- 21 Петров В. Н. Киберпространство как новая среда международного противоборства // Вопросы безопасности. 2022. № 6. С. 41–58.
- 22 Пивоваров Ю. С. Международная безопасность в условиях кризиса глобализации // Вестник РАН. 2022. Т. 92, № 8. С. 725–738.
- 23 Примаков Е. М. Мир без России? К чему ведет политическая близорукость. М. : Центрполиграф, 2020. 415 с.
- 24 Российский совет по международным делам. URL: <https://russiancouncil.ru> (дата обращения: 17.04.2026).
- 25 Сунгуров А. Ю. Информационное воздействие как инструмент внешней политики // Власть. 2021. № 4. С. 52–63.
- 26 Торкунов А. В. Современные международные отношения: учебник. М. : Аспект Пресс, 2022. 688 с.

- 27 Тренин Д. В. Международная безопасность после 2020 года М. : Московский центр Карнеги, 2021. С. 1–34.
- 28 Хрусталёв М. А. Международная безопасность и новые технологии // Международные процессы. 2023. № 1. С. 41–57.
- 29 Цыганков П. А. Теория международных отношений: учебное пособие. М. : Гардарики, 2021. 557 с.
- 30 The EU's Cybersecurity Strategy for the Digital Decade // European Commission. Brussels. 2020. URL: <https://digital-strategy.ec.europa.eu/en/library/eu-cybersecurity-strategy> (дата обращения: 12.04.2026).
- 31 NATO 2022 Strategic Concept // North Atlantic Treaty Organization. Madrid. 2022. URL: <https://www.nato.int/strategic-concept> (дата обращения: 11.04.2026).
- 32 Castells M. Networks of Outrage and Hope. Cambridge: Polity Press. 2015. 328 p.
- 33 Colonial Pipeline Official Statement. URL: <https://www.colpipe.com/news> (дата обращения: 17.03.2026).
- 34 ENISA Threat Landscape 2024. URL: <https://www.enisa.europa.eu> (дата обращения: 12.03.2026).
- 35 Estonian Information System Authority Reports. URL: <https://www.ria.ee/en> (дата обращения: 17.04.2026).
- 36 EU DisinfoLab Annual Report. URL: <https://www.disinfo.eu> (дата обращения: 17.05.2026).
- 37 European External Action Service. Hybrid Threats. URL: <https://www.eeas.europa.eu> (дата обращения: 17.04.2026).
- 38 Facebook Human Rights Report. URL: <https://about.fb.com> (дата обращения: 20.03.2026).
- 39 Hoffman F. G. Conflict in the 21st Century: The Rise of Hybrid Wars. Arlington: Potomac Institute. 2007. 72 p.
- 40 International Institute for Strategic Studies. Military Balance 2024. URL: <https://www.iiss.org> (дата обращения: 20.04.2026).

- 41 Keohane R. O. After Hegemony. Princeton: Princeton University Press. 2005. 320 p.
- 42 MIT News. Study: False news spreads faster than truth. URL: <https://news.mit.edu/2018/false-news-spreads-faster-truth-twitter-0308> (дата обращения: 11.04.2026).
- 43 Morgenthau H. J. Politics Among Nations: The Struggle for Power and Peace. 7th ed. New York: McGraw-Hill. 2006. 752 p.
- 44 NATO Cooperative Cyber Defence Centre of Excellence. Cyber Threat Report 2024. URL: <https://ccdcoc.org/library/publications> (дата обращения: 17.04.2026).
- 45 NATO Hybrid Threats URL: https://www.nato.int/cps/en/natohq/topics_156338.htm (дата обращения: 10.04.2026).
- 46 RAND Corporation. Countering Hybrid Warfare. URL: <https://www.rand.org> (дата обращения: 17.04.2026).
- 47 RAND Corporation. Modern Political Warfare URL: https://www.rand.org/pubs/research_reports/RR1772.html (дата обращения: 17.04.2026).
- 48 SIPRI Military Expenditure Database. URL: <https://milex.sipri.org> (дата обращения: 18.04.2026).
- 49 SIPRI. Trends in World Military Expenditure 2024. URL: <https://www.sipri.org/publications/2025/trends-world-military-expenditure-2024> (дата обращения: 18.04.2026).
- 50 Statista. Global cybercrime statistics. URL: <https://www.statista.com> (дата обращения: 18.04.2026).
- 51 Stockholm International Peace Research Institute Database. URL: <https://www.sipri.org/databases> (дата обращения: 19.04.2026).
- 52 The World Bank. Digital Development Reports. URL: <https://www.worldbank.org/en/topic/digitaldevelopment> (дата обращения: 19.04.2026).
- 53 UNHCR Syria Emergency. URL: <https://www.unhcr.org/syria-emergency.html> (дата обращения: 19.04.2026).
- 54 United Nations Digital Cooperation Report. URL: <https://www.un.org/en/digital-cooperation-roadmap> (дата обращения: 17.03.2026).

55 United Nations Peacekeeping Data. URL: <https://peacekeeping.un.org/en/data> (дата обращения: 17.04.2026).

56 United Nations Security Council Reports on Syria. URL: <https://www-securitycouncilreport.org> (дата обращения: 17.04.2026).

57 Waltz K. N. Theory of International Politics. Long Grove: Waveland Press. 2010. 251 p.

58 Wendt A. Social Theory of International Politics. Cambridge: Cambridge University Press. 1999. 429 p.

59 World Bank Data: Military expenditure. URL: <https://data.worldbank.org> (дата обращения: 17.04.2026).

Приложение А

Хронология трансформации международных угроз (1945–2025 гг.)

Таблица А.1 – Хронология трансформации международных угроз (1945–2025 гг.)

Год	Событие	Характер угрозы	Значение для развития международной безопасности
1	2	3	4
1945	Создание ООН и завершение Второй мировой войны	Межгосударственные военные угрозы	Формирование послевоенной системы коллективной безопасности
1949	Создание НАТО	Военно-политическое противостояние	Институционализация системы коллективной обороны западных государств
1955	Создание Организации Варшавского договора	Блоковое противостояние	Усиление биполярной структуры международных отношений
1962	Карибский кризис	Ядерная угроза	Демонстрация риска глобального ядерного конфликта
1968	Подписание Договора о нераспространении ядерного оружия	Ядерная безопасность	Формирование международного режима контроля над ядерным оружием
1979	Ввод советских войск в Афганистан	Региональные вооружённые конфликты	Рост значения локальных конфликтов в мировой политике
1986	Авария на Чернобыльской АЭС	Техногенная угроза	Осознание трансграничного характера экологических и техногенных рисков
1991	Распад СССР	Геополитическая трансформация	Изменение структуры мирового порядка и системы международной безопасности
1991	Операция «Буря в пустыне»	Высокотехнологичная война	Демонстрация возможностей высокоточного оружия и современных систем управления
1999	Военная операция НАТО против Югославии	Гуманитарные интервенции	Изменение подходов к использованию военной силы в международных отношениях
2001	Террористические атаки 11 сентября в США	Международный терроризм	Формирование глобальной антитеррористической повестки
2003	Военная операция США в Ираке	Асимметричные угрозы	Рост значения нерегулярных форм вооружённого противоборства

Продолжение таблицы А.1

1	2	3	4
2007	Кибератаки на Эстонию	Киберугрозы	Первое масштабное применение киберинструментов против государства
2008	Вооружённый конфликт в Южной Осетии	Информационно-военное противоборство	Усиление роли информационного сопровождения военных действий
2010	Кибероперация Stuxnet против ядерной программы Ирана	Кибервойна	Демонстрация возможности цифрового воздействия на физические объекты
2011	Начало сирийского конфликта	Гибридные угрозы	Сочетание военных, информационных, экономических и политических инструментов воздействия
2014	Украинский кризис и санкционное противостояние	Гибридное противоборство	Рост значения экономических ограничений и информационных кампаний
2015	Начало операции ВКС России в Сирии	Международный вооружённый конфликт	Интернационализация региональных конфликтов и расширение круга участников
2015	Кибератака на энергосистему Украины	Угрозы критической инфраструктуре	Подтверждение уязвимости энергетических объектов перед цифровыми атаками
2020	Конфликт в Нагорном Карабахе	Технологизированная война	Демонстрация эффективности БПЛА и цифровой разведки
2021	Кибератака на Colonial Pipeline (США)	Киберугрозы критической инфраструктуре	Подтверждение высокой зависимости экономики от цифровых систем управления
2022	Активизация использования искусственного интеллекта в военной сфере	Технологическое соперничество	Начало масштабной интеграции ИИ в системы безопасности и обороны
2023	Рост атак на государственные цифровые платформы	Цифровые угрозы	Усиление значения киберустойчивости государственного управления
2024	Рекордный уровень мировых военных расходов	Комплексные угрозы	Сочетание традиционной гонки вооружений и технологической конкуренции

2025	Расширение программ развития автономных боевых систем и военного ИИ	Цифрово-технологические угрозы	Формирование нового этапа трансформации международной безопасности
------	---	--------------------------------	--

Приложение Б

Негосударственные акторы в современных международных конфликтах

Таблица Б.1 – Негосударственные акторы в современных международных конфликтах

Актор	Тип	Регион деятельности	Конфликты участия	Основные инструменты воздействия	Значение для международной безопасности
1	2	3	4	5	6
<i>Wagner Group</i>	ЧВК	Африка, Ближний Восток	Сирия, Ливия, ЦАР, Мали	Военная поддержка, охрана объектов	Расширение роли частных военных структур
<i>Academi (Blackwater)</i>	ЧВК	Ближний Восток	Ирак, Афганистан	Охранные и логистические функции	Коммерциализация военной деятельности
<i>Hezbollah</i>	Военно-политическая организация	Ближний Восток	Сирия, Ливан	Ракетные системы, информационные операции	Сочетание политических и военных методов
<i>Houthis</i>	Вооружённое движение	Йемен	Йеменский конфликт	БПЛА, ракетные удары	Рост значения асимметричных угроз
<i>Namas</i>	Военно-политическая организация	Ближний Восток	Палестино-израильский конфликт	Ракетные удары, информационные кампании	Использование гибридных методов борьбы
<i>ISIS</i>	Террористическая организация (запрещена на территории РФ)	Ближний Восток, Африка	Сирия, Ирак	Терроризм, цифровая пропаганда	Транснациональный характер угроз
<i>Al-Qaeda</i>	Террористическая сеть (запрещена на территории РФ)	Глобально	Афганистан, Йемен, Африка	Террористические методы	Сетевая структура управления

1	2	3	4	5	6
<i>Anonymous</i>	Хакерская группа	Глобально	Киберкампании	DDoS-атаки, взломы	Формирование цифрового измерения конфликтов
<i>Killnet</i>	Хакерская группа	Европа	Киберкампании 2022–2025 гг.	DDoS-операции	Рост роли негосударственных киберакторов
<i>DarkSide</i>	Киберпреступная группа	Глобально	<i>Colonial Pipeline</i>	<i>Ransomware</i>	Уязвимость критической инфраструктуры
<i>Conti</i>	Киберпреступная группа	Глобально	Атака на Коста-Рику	Шифровальщики	Возможность влияния на государственное управление
<i>Bellingcat</i>	Аналитическая сеть OSINT	Глобально	Расследования конфликтов	Анализ открытых данных	Новая роль гражданской разведки
<i>Conflict Intelligence Team</i>	Аналитическая группа	Глобально	Мониторинг конфликтов	OSINT-анализ	Расширение возможностей общественного контроля

Приложение В

Сравнительные показатели кибербезопасности и цифровой устойчивости ведущих государств мира

Таблица В.1 – Сравнительные показатели кибербезопасности и цифровой устойчивости ведущих государств мира

Государство	Индекс кибербезопасности GCI (0–100)	Место в группе GCI	Государственные расходы на кибербезопасность, млрд долл.	Национальный CERT/киберкомандование	Доля цифровой экономики в ВВП, %	Основные направления развития
США	100	Tier 1	13	Да	10,3	ИИ, защита критической инфраструктуры, кибероперации
Великобритания	100	Tier 1	3,2	Да	12,4	Национальная киберстратегия, защита госуслуг
Германия	97,9	Tier 1	2,4	Да	8,8	Промышленная кибербезопасность
Франция	98,4	Tier 1	2,1	Да	8,1	Суверенные цифровые технологии
Япония	97,5	Tier 1	1,9	Да	8	Защита критической инфраструктуры
Республика Корея	100	Tier 1	1,7	Да	10,8	Кибероборона и технологии ИИ
Китай	96,2	Tier 1	9,1	Да	9,6	Цифровой суверенитет и контроль сетей
Индия	98,5	Tier 1	1,3	Да	11,5	Развитие национальной цифровой инфраструктуры
Россия	95,6	Tier 1	1,5	Да	6,5	Защита критической информационной инфраструктуры