Правительство Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(СПбГУ)

УДК 327.5
Рег. № НИОКТР 124090900001-6

УТВЕРЖДАЮ
Проректор по научной работе

_____С. В. Микушев
«____»_____202_ г.

# ОТЧЕТ
# О НАУЧНО-ИССЛЕДОВАТЕЛЬСКОЙ РАБОТЕ

# ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ РОССИИ В УСЛОВИЯХ РАЗВИТИЯ ИНДУСТРИИ 4.0 И ГИБРИДНЫХ УГРОЗ СО СТОРОНЫ КОЛЛЕКТИВНОГО ЗАПАДА

(промежуточный, этап 1)

Руководитель НИР:
гл. науч. сотрудник СПбГУ,
д.и.н., профессор, Академик РАН _____ А. М. Васильев

Санкт-Петербург 2024

## СПИСОК ИСПОЛНИТЕЛЕЙ

| | | |
|---|---|---|
| Руководитель НИР, гл. науч. сотр., д.и.н., профессор, Академика РАН | подпись, дата | А. М. Васильев (введение, заключение, раздел 1) |
| Отв. исполнитель, профессор, д.полит.н., доцент. | 08.11.2024 20.11.2024 подпись, дата | К. А. Панцерев (введение, заключение, разделы 1,2,4) |
| Исполнители: | | |
| Профессор, д.ист.н., профессор | 13.11.2024 подпись, дата | Е. Н. Пашенцев (введение, раздел 1, 3,4) |
| Ведущий науч.сотр., д. полит.н. | 12.11.2024 подпись, дата | Д. Ю. Базаркина (введение, разделы 1, 3) |
| Доцент, д.полит.н., доцент | 16.11.2024г. подпись, дата | Р. С. Выходец (Введение, разделы 1, 3) |
| Старший науч. сотр., к.полит.н. | 08.11.2024 подпись, дата | А. Р. Шишкина (раздел 3) |
| Старший науч. сотр., к.полит.н. | 8.11.2024 подпись, дата | Т.Р. Хайруллин (раздел 3) |
| Ст. преподаватель, к.полит.н. | 15.11.24 подпись, дата | А. А. Носиков (раздел 5) |
| Ассистент, к.полит.н. | 20.11.24 подпись, дата | Ю. Ю. Колотаев (раздел 4) |
| Инженер-исследователь | 20.11.2024 подпись, дата | Е. А. Михалевич (раздел 3) |
| Нормоконтроль | подпись, дата | Место для ввода текста. |

## РЕФЕРАТ

Отчет 124 с., 1 кн., 14 рис., 103 источн., 5 прил.

ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ, ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЕ ПРОТИВОБОРСТВО, ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ, РОССИЯ, ИНДУСТРИЯ 4.0, ГИБРИДНЫЕ УГРОЗЫ

Объект исследования: меры в области обеспечения информационной безопасности России по нейтрализации гибридных действий государственных и негосударственных акторов.

Цель работы – выявление угроз информационно-психологической безопасности (ИПБ) России в условиях развития Индустрии 4.0 и гибридной войны со стороны коллективного Запада.

Методы: контент-анализ, критический дискурс-анализ, качественный сравнительный анализ, метод сценарного анализа, количественный анализ, тематический анализ, анализ настроений.

В процессе работы была произведена оценка спектра государственных и негосударственных акторов, которые ведут гибридную войну против России; определены цели и изучены методы информационно-психологических операций против России; произведена оценка преимуществ и недостатков подходов к обеспечению ИПБ общества, принятых как в самой России, так и в тех интеграционных объединениях, в которых Россия принимает наиболее активное участие (ШОС, ОДКБ, ЕАЭС, БРИКС); проанализированы практические примеры операций обеспечения ИПБ в России и тех интеграционных объединений, в которых Россия принимает наиболее активное участие (ШОС, ОДКБ, ЕАЭС, БРИКС); произведена оценка влияния технологий искусственного интеллекта на систему международных отношений и политическую повестку дня; разработаны рекомендации по минимизации угроз ИПБ в России.

Степень внедрения: по инициативе Р.С.Выходца, К.А.Панцерева 01.03.2024 Секция по информационно-психологической безопасности ЕАЭС Экспертно-консультативного совета Комитета Государственной Думы по делам СНГ евразийской интеграции и связям с соотечественниками провела круглый стол «Вопросы информационно-психологической безопасности в высшей школе России»; 29.11.2024 К. А. Панцерев, Р. С. Выходец, Е. Н. Пашенцев приняли участия в Расширенном заседание секции по информационно-психологической безопасности ЕАЭС. Предложения Р.С. Выходца и К. А. Панцерева вошли в итоговое решение круглого стола № 1124-4 от 29.112024.

Область применения результатов: деятельность в сфере обеспечения безопасности и обороноспособности государства.

**СОДЕРЖАНИЕ**

## ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящем отчете о НИР применяют следующие термины с соответствующими определениями:

| | |
|---|---|
| Гибридный конфликт | - проведение масштабной подрывной деятельности без участия регулярных вооруженных сил нападающего государства, но с опорой на те внутренние политические силы страны-жертвы, которые разделяют позицию нападающего государства, с целью смены режима страны-жертвы или радикального изменения ее политики при массированной материальной и информационной поддержке |
| Индустрия 4.0 | - неологизм, описывающий быстрый технологический прогресс в XXI веке. Промышленные изменения этой фазы характеризуются присоединением таких технологий, как искусственный интеллект, редактирование генома, передовая робототехника, которые стирают границы между физическим, цифровым и биологическим мирами |
| Интернет-балканизация | - характеристика Интернет-пространства как раскалывающегося и разъединяющегося в силу различных факторов, таких как технологии, международная торговля, политика, а также национальные интересы государств. Понимается также как трансформация глобальной сети Интернет во множество локальных сетей, границы между которыми устанавливаются искусственно на уровне национальных законодательств и государственного регулирования Интернета |
| Информационно-психологическая безопасность | - состояние защищенности существующей в государстве системы формирования общественного мнения и принятия решений, а также психики должностных лиц, общественных деятелей и населения от деструктивного идеологического и психологического воздействия в информационной среде организованной или дискурсивной природы |
| Информационно-психологическое | - сфера международных отношений, характеризующаяся деструктивным воздействием в информационной среде |

| | |
|---|---|
| противоборство | организованной или дискурсивной природы на системы формирования общественного мнения и принятия решений, а также психику должностных лиц, общественных деятелей и населения |
| Искусственный интеллект | - семейство технологий, способных имитировать когнитивную деятельность человека |
| Киберпросторанство | - взаимосвязанная цифровая среда, тип виртуального мира, популяризованный с появлением Интернета. Используется для описания глобальной технологической среды, определяемой как глобальная сеть взаимозависимых инфраструктур информационных технологий, телекоммуникационных сетей и систем компьютерной обработки. Термин также может относиться к социальному опыту взаимодействия и обмена информацией пользователя глобальной сети |
| Когнитивная война | - современный вид информационного противоборства, связанный с оказанием деструктивного воздействия на процессы потребления человеком информации и его психику с использованием передовых информационных и нейротехнологий |
| Новые медиа | - термин, обозначающий развитие цифровых, и в особенности сетевых технологий и форм коммуникации. Используется также для обозначения новых форм взаимодействия между производителями контента и его реципиентами с учетом возникновения обратной связи, а также для указания на отличия от традиционных средств массовой информации |
| Стратегическая конкуренция | - конкурентная деятельность государства (группы государств) против другого государства группы (государств), направленная на реализацию национальных интересов, которая находится в диапазоне действий между сотрудничеством и войной |
| Цифровое кочевничество | - новый тип образа жизни специалистов в сфере IT-технологий и смежных сфер, который стал возможен благодаря развитию компьютерных сетей и популяризации мобильных устройств, таких как ноутбуки, планшеты и КПК. Цифровое кочевничество предполагает трансграничные перемещения и удаленную работу с использованием новейших Интернет-технологий. Термин описывает особую категорию людей, чьи профессиональные |

навыки и образ жизни трансформируются под влиянием развития информационных технологий и процессов становления информационного общества.

## ПЕРЕЧЕНЬ СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ

В настоящем отчете о НИР применяют следующие сокращения и обозначения:

| | |
|---|---|
| АЮС | - Африка южнее Сахары |
| БВСА | - Ближний Восток и Северная Африка |
| БЯМ | - Большие языковые модели |
| ВВС | - Военно-воздушные силы |
| ВПК | - Военно-промышленный комплекс |
| ВСУ | - Вооруженные силы Украины |
| ЕАЭС | - Евразийский экономический союз |
| ЗИИИ | - Злонамеренное использование искусственного интеллекта |
| ИИ | - Искусственный интеллект |
| ИКТ | - Информационно-коммуникационные технологии |
| ИПБ | - Информационно-психологическая безопасность |
| ИПП | - Информационно-психологическое противоборство |
| НБИКС-технологии | - Нано-, био-, инфо-, когно- и социальные технологии |
| НКО | - Некоммерческая организация |
| ОАЭ | - Объединенные Арабские Эмираты |
| ОДКБ | - Организация Договора о коллективной безопасности |
| СБУ | - Служба безопасности Украины |
| СВО | - Специальная военная операция |
| СМИ | - Средства массовой информации |
| ЦИПСО | - Центр информационно-психологических операций |
| ШОС | - Шанхайская организация сотрудничества |

# ВВЕДЕНИЕ

Внедрение сквозных технологий Четвертой промышленной революции, информатизации производственных процессов, глубокое внедрение робототехники и технологий искусственного интеллекта, сопряжено с необходимостью реализации многомиллиардных долгосрочных инвестиционных программ. Эффективное освоение этих капиталовложений, как на национальном уровне, так и на уровне отдельных предприятий, происходит в крайне неблагоприятной международной обстановке, в первую очередь сопряженной с интенсификацией действий стран коллективного Запада, их спецслужб на территории России и дружественных по отношению к ней государств, направленной против ее поступательного развития и укрепления международного сотрудничества, создавая, тем самым, широкий спектр гибридных угроз национальной безопасности России. На это обстоятельство указал и Президент В. Путин, который выступая в Министерстве иностранных дел Российской Федерации 10 февраля 2024 г. по случаю Дня дипломатического работника, заявил, что сегодня коллективным Западом развязана против России гибридная война, направленная на то, чтобы добиться изоляции России и подорвать ее безопасность.

Сама по себе гибридная война представляет собой набор адресных прямых и непрямых, открытых и скрытых методов воздействия (экономические санкции, кибероперации, психологические операции и другие действия) на различные сегменты российского общества, в том числе и на трудовые коллективы крупных промышленных предприятий. Цель подобных воздействий – через подрыв информационно-психологической безопасности с использованием новейших технологий подорвать обороноспособность российского государства, нарушить нормальное функционирование объектов критически важной инфраструктуры и наиболее крупных предприятий реального сектора экономики, оказать влияние на систему принятия решений органами государственной власти, руководством крупных промышленных предприятий, различными социальными группами населения и отдельными людьми.

В этой связи проект направлен на выявление угроз информационно-психологической безопасности России, а также разработку рекомендаций по минимизации этих угроз, как для российского государства, так и для крупных промышленных предприятий.

Для достижения цели проекта в ходе первого этапа его реализации были поставлены следующие задачи:

- конкретизировать теоретико-методологическую базу проекта, проработать понятийный аппарат и научный инструментарий исследования;

- оценить спектр государственных и негосударственных акторов, которые ведут гибридную войну против России;

- выявить цели и методы информационно-психологических операций против России в условиях гибридной войны со стороны коллективного Запада;

- оценить преимущества и недостатки подходов к обеспечению ИПБ общества, принятых как в самой России, так и в тех интеграционных объединениях, в которых Россия принимает наиболее активное участие (ШОС, ОДКБ, ЕАЭС, БРИКС), в том числе подходов к противодействию гибридным угрозам, влияющим на сферу ИПБ (дезинформации, враждебной пропаганде, киберугрозам);

- оценить имеющиеся в распоряжении профильных структур России и тех интеграционных объединений, в которых Россия принимает наиболее активное участие (ШОС, ОДКБ, ЕАЭС, БРИКС) инструменты обеспечения ИПБ личности, общества и государства;

- проанализировать практические примеры операций обеспечения ИПБ в России и тех интеграционных объединений, в которых Россия принимает наиболее активное участие (ШОС, ОДКБ, ЕАЭС, БРИКС), выявить их эффективность с точки зрения международной ИПБ;

- оценить влияние технологий искусственного интеллекта на систему международных отношений и политическую повестку дня;

- разработать рекомендации по минимизации угроз ИПБ в России

Научная новизна проекта состоит в комплексном исследовании угроз информационно-психологической безопасности в России в условиях развития Индустрии 4.0. и гибридной войны со стороны коллективного Запада. В результате реализации проекта впервые будет дано теоретико-методологическое и эмпирическое обоснование модели обеспечения информационно-психологической безопасности (ИПБ) в крупных трудовых коллективах, а также разработаны профильные образовательные программы и учебно-методические материалы для сотрудников крупных предприятий и организаций реального сектора экономики России.

В теоретико-методологическом плане в рамках исследований 2024 года был использован смешанный подход, предполагающий выстраивание баланса между качественными и количественными исследованиями, что особенно продуктивно проявляется при использовании сравнительных техник анализа при изучении феноменов и явлений, обладающих как качественными, так и количественными характеристиками. При использовании смешанного подхода появляется больше пространства для валидации и триангуляции результатов исследования.

Что касается конкретных методов, применявшихся в исследованиях, то в этом случае стоит выделить в первую очередь качественный сравнительный анализ, предполагающий установление связи между набором условий и набором результатов (откликов) тех или иных процессов. Это позволяет соотнести воздействие различных факторов (социально-политический фон, условия, отдаленные и непосредственные причины, поводы-триггеры и т. п.) на исход, выбранный в качестве зависимой переменной в рамках выстраиваемой модели.

Метод качественного сравнительного анализа, предложенный Ч. Рэйгиным в 1987 г., основан на использовании средств математической логики при анализе взаимосвязи условий в рамках конкретного случая. Он используется для анализа наборов данных путем перечисления и подсчета всех комбинаций переменных, наблюдаемых в этом наборе, и последующего определения выводов, поддерживающих данные, путем применения правил логического следования. Качественный количественный анализ в некоторой степени служит инструментом смягчения методологических споров между сторонниками качественных методов исследования и адептов количественных методов, стремясь найти баланс между формальными обобщениями и описанием феноменов. При участии самого Рэйгина, а также таких исследователей как Л. Кронквист, Ж. Де Мер, Б. Риу и др. были также разработаны несколько видов данной методологии. В исследованиях 2024 г. использовался так называемый качественный сравнительный анализ четких множеств, который применяется в тех случаях, когда анализируемые данные могут быть приведены к дихотомизированной форме.

Кроме того, был проведен ряд экспертных анонимизированных интервью с представителями профессионального, экспертного и академического сообщества, а также использовался метод полевых наблюдений.

Качественный анализ официальных документов государств, публикаций международных организаций, национальных правоохранительных структур, научных публикаций, а также материалов СМИ позволил дать характеристику текущего образа международных объединений на постсоветском пространстве с участием России в информационном поле, а также оценить перспективы международного сотрудничества России по направлению противодействия информационной преступности.

Кроме этого, к методам исследования стоит отнести количественный и качественный контент-анализ нормативно-правовых актов, государственных концепции России и стран БРИКС, ШОС, ЕАЭС, ОДКБ, совместных заявлений в области информационной безопасности.

Контент-анализ способствовал систематическому изучению текстовых данных, включая посты в социальных сетях, медийные публикации и официальные заявления. С его помощью были выявлены тенденции, ключевые темы и эмоции, которые ассоциируются с определёнными нарративами. В отдельных случаях контент-анализ включал структурные элементы взаимозависимости акторов, институтов и продвигаемой повестки (т.е. дополнялся структурным анализом). Такой подход позволил рассмотреть многоуровневость продвигаемых нарративов в международных организациях. Источником анализа выступили нормативные акты, стратегии, программные документы, заявления и доклады. Применив же методику количественного анализа содержания текстовых массивов, стало возможно разложить тексты на составляющие их части и проанализировать эти переменные, интерпретировать выявленные закономерности по частоте использования конкретных тем, слов, которые представляются наиболее важными для исследователей.

Дискурс-анализ применялся для изучения нарративов и контрнарративов, а также для выявления ключевых тем и метафор, используемых в информационных кампаниях. Анализ фокусировался на языке и риторике, используемых в социальных сетях и СМИ, что позволило установить доминирующие представления и выявить потенциальные манипуляции. Совместно с контент-анализом позволил изучить репрезентацию таких тем, как многополярный мир и борьба с неоколониализмом, представляемых в государственных СМИ и социальных сетях. Комбинация методов дополнила процедуру поиска доминирующих нарративов, поддерживающих российские политические интересы.

Применение комплекса методов анализа больших данных дало возможность обработать релевантный массив информации о циркулирующих в медиа нарративах. Комбинация мониторинга социальных сетей и дискурсивного анализа позволили количественно проверить сформированные гипотезы, а также выявить нарративы, которые нацелены на негативные настроения и подрыв общественного единства. В рамках работы для сбора и анализа данных о темах, связанных с глобальной конфронтацией, применялся язык программирования Python.

# 1 Глобальная стратегическая конкуренция и информационно-психологическое противоборство

## 1.1 Глобальная стратегическая конкуренция: сущность понятия и общая характеристика

Соперничество между государствами находится в континууме действий, простирающимся между военными конфликтами и дружественными отношениями. Это предполагает широкий спектр воздействий на соперника, включающий идеологические, дипломатические, экономические и иные инструменты невоенного характера.

В действующей редакции Стратегии национальной безопасности США стратегическая конкуренция понимается как соперничество великих держав за свои национальные интересы. На современном этапе, по мнению американских стратегов, ее содержанием выступает борьба за формирование будущего международного порядка между «демократическим» Западом, безусловным лидером которого выступают США, и «авторитарными» державами, прежде всего, Китаем и Россией.

Если абстрагироваться от идеологических коннотаций, то с этим тезисом сложно не согласиться, поскольку главным вопросом современных международных отношений является преодоление гегемонистского мира, основанного на мифе об «исключительности» американской нации и переход к многополярному мироустройству.

Конкурентная деятельность располагается в достаточно широком диапазоне международных отношений, полюсами которого выступают сотрудничество и война, при этом, не переходя грань прямого вооруженного конфликта и насилия. По мнению экспертов, такая конкуренция включает шпионаж, экономическую борьбу, кражу интеллектуальной собственности, противоборство в информационной среде, санкции, юридическое принуждение, позиционирование вооруженных сил, дипломатические и военные маневры и угрозы, запугивание, подкуп политической элиты.

С учетом диффузии конвенциональных и неконвенциональных сил и средств в современном конфликте принципиальное значение приобретают, так называемые, «красные линии», пересечение которых автоматически переводят стратегическую конкуренцию в острую фазу конфронтации. Как это, например, случилось 22 февраля 2022 года, когда в ответ на полномасштабное военное освоение территории Украины силами стратегических конкурентов в лице коллективного Запада, Россия была вынуждена применить конвенциональные средствами и начать Специальную военную операцию.

При этом важно понимать, что «красные линии», представляющие собой пороги, пересечение которых автоматически переводит межгосударственную стратегическую

конкуренцию в конфронтационную плоскость, нередко предполагающую применение военной силы, обладают подвижным динамическим характером. Пересечение стратегическим конкурентом «красных линий» может нести в себе явную экзистенциональную угрозу для противоположной стороны. В качестве катализатора конфронтации могут выступать угрозы или же факты стратегического проигрыша одной из сторон.

В современном мире информационная сфера играет ключевое значение в стратегической конкурентной борьбе. Б. Блечмэн и С. Каплан еще в конце 70-х годов в своей совместной работе указали, что «успех во многом зависит от эффективного использования информационной среды, позволяющей проецировать национальную мощь в глобальном масштабе, решая задачи сдерживания, принуждения, укрепления уверенности и побуждения к действиям» [1: 27]. Сложность современной конкурентной среды определяется глубоким проникновением цифровых технологий и социальных сетей, позволяющих установить эффективную коммуникацию с отдельным человеком, оказывая тем самым беспрецедентное воздействие на общественное мнение.

Важное значение информационного фактора в международном противоборстве в последнее время было закреплено в целой серии официальных документах национального и международного уровня. В Стратегической концепции НАТО от 2022 года за киберпространством признается ключевая роль в противодействии современным угрозам. При этом документ указывает на возможность задействования пресловутой пятой статьи Североатлантического договора в ответ на использование противником информационных методов воздействия, включающие злонамеренные гибридные и кибероперации, а также дезинформацию, наносящие ущерб безопасности Североатлантического альянса.

В обновленной Концепции внешней политики Российской Федерации от 2023 года впервые в российском официальном дискурсе использован термин «информационно-психологическое воздействие». В перечне основных национальных интересов во внешнеполитической сфере отдельным пунктом названо «развитие безопасного информационного пространства, защита российского общества от деструктивного иностранного информационно-психологического воздействия» [2]. Более того, в документе указывается, что «наиболее распространенной формой вмешательства во внутренние дела суверенных государств стало навязывание им деструктивных неолиберальных идеологических установок, противоречащих традиционным духовно-нравственным ценностям, что, как следствие, оказывает разрушительное воздействие на все сферы международных отношений».

На современном этапе стратегической конкуренции все более заметную роль играет целенаправленное деструктивное идеологическое и психологическое воздействие в информационной среде. Поэтому выработка коллективной политики в области обеспечения информационно-психологической безопасности представляется сегодня одним из основных приоритетов государств и их союзов.

### 1.2 Когнитивная безопасность в глобальном измерении

В междисциплинарной структуре глобалистики на современном этапе ее развития все больший удельный вес начинают занимать поиски решения проблем предотвращения глобальных рисков и обеспечения глобальной безопасности. Причем эти поиски аргументируются, во-первых, методологией глобальной истории, которая ориентирована на разработку двух начал современной картины мира: связей и сопоставлений, через которые открывается глобальная перспектива исторического процесса. Во-вторых, – необходимостью выявления сущности феномена безопасности в процессах глобального эволюционизма, будь то геологическая история Земли или же когнитивные процессы на «вершине биологической эволюции». Тем самым представляется объяснимой естественная связь феномена глобальной безопасности во всех его проявлениях (геополитической, экономической, социальной, технологической, когнитивной и других) с антропоценом, поскольку каждое из них (проявлений) актуализируется по мере обострения угроз и глобальных рисков, которые определили содержание «эпохи отсутствия безопасности».

Система глобальных рисков (экологические, технологические, геополитические) в течение следующего десятилетия будет нарушать глобальную стабильность, а неуправляемое, во многих отношениях, развитие технологий искусственного интеллекта будет представлять серьезную опасность. Поэтому проблема обеспечения глобальной безопасности предполагает необходимость не только разработки теоретико-методологической базы ее исследования и конкретных рекомендаций, но и обратить внимание на возникшую в самые последние годы проблему обеспечения информационно-психологической и когнитивной безопасности.

В начале 20 х годов XXI века в военно-аналитическом сообществе НАТО стала широко обсуждаться тема формирования еще одной области (домена) военных действий – когнитивная война (Cognitive Warfare). Технология когнитивных операций, спонсируемая и контролируемая НАТО как «способ нанесения вреда мозгу», стала разрабатываться в 2013 г. в Инновационном центре НАТО (iHub, Норфолк, США). Разработчики назвали ее «когнитивной войной», целью которой является нанесение вреда не только

военнослужащим, но и гражданскому населению. В роли потенциальной угрозы была обозначена возможность гражданских лиц быть «спящими ячейками», «пятыми колоннами», которые бросают вызов стабильности «либеральных западных демократий». Когнитивная война – как утверждал руководитель упомянутого выше центра Дю Клюзель, – это война идеологий, стремящаяся подорвать веру [и доверие], скрепляющую любое общество… В мире, пронизанном технологиями, война в когнитивной области мобилизует более широкий спектр боевых пространств, чем это могут сделать физические и информационные измерения. Сама его суть состоит в том, чтобы захватить контроль над людьми (гражданскими и военными), организациями, нациями, а также над идеями, психологией, особенно поведенческой, мыслями, а также над окружающей средой [3].

В том же году вышел еще один документ НАТО, подготовленный совместно с авторским коллективом из Johns Hopkins University уже в формате некоего руководства к действиям под примечательным названием («Когнитивная война: атака на истину и мысль»), в котором открыто заявлялось, что когнитивная война «преследует две отдельные, но взаимодополняющие цели: дестабилизация и влияние. Цели атак когнитивной войны могут варьироваться от целых групп населения до отдельных лидеров в политике, экономике, религии и академических кругах. Здесь идет речь уже о критериях распознавания когнитивных угроз, о предложениях по внесению изменений в Устав ООН, для чего НАТО его союзники должны заняться выявлением актов когнитивной (некинетической) войны и создавать когнитивные организации в рамках своих правоохранительных и военных организаций с каналами связи, действующими по всему альянсу, роду войск и между правительством и местными правоохранительными органами. Основные положения, определяющие цели, возможности, условия осуществления когнитивной войны, и выражающие официальную позицию военно-политического руководства Североатлантического альянса, представлены следующим образом:

1. Согласно концепции «когнитивной войны» на современном поле боя появляется еще одно боевое измерение – когнитивное, которое дополняет физическое (наземное, морское, воздушное, космическое) и информационное измерения. В мире, наполняемом НБИКС-технологиями (нано-, био-, инфо-, когно- и социальными технологиями) война в когнитивной области мобилизует более широкий спектр боевых действий, осуществляя контроль над людьми, социальными институтами и народами, над общественным и индивидуальным сознанием, массовой психологией и окружающей средой.

2. Реализация концепции «когнитивной войны» требует знания не только естественных и технических наук, но, в полной мере, наук гуманитарных – философии и

психологии, филологии и этнологии. Нейронаучные методы могут использоваться как в медицинских, так и в немедицинских (образовательных, профессиональных, жизненных, военных) целях, да и сама наука о мозге подразделяется как на фундаментальную, так и прикладную, особенно привлекательную для использования в области безопасности, разведки и военных действий.

3. В таком случае изучение когнитивной области, сосредоточенной на человеке, представляет собой новую серьезную задачу, которая необходима для любой военной стратегии, связанной с формированием боевой мощи в будущем. В вооруженных силах, утверждает автор, знания в области антропологии, этнографии, истории, психологии среди других областей будут более чем когда-либо необходимы для сотрудничества с вооруженными силами, например, для получения качественного понимания из количественных данных. Другими словами, если указание на современное поле битвы и провозглашает новое значение человека, то речь идет скорее о переосмыслении взаимодействия между точными и социальными науками.

В XXI веке стратегическое преимущество будет заключаться в том, как взаимодействовать с людьми, понимать их и получать доступ к политическим, экономическим, культурным и социальным сетям, чтобы добиться относительного преимущества, дополняющего единственную военную силу. Эти взаимодействия не сводятся к физическим границам земли, воздуха, моря, киберпространства и космоса, которые, как правило, сосредоточены на географии и характеристиках местности. Эти же взаимодействия представляют собой сеть сетей, определяющих власть и интересы во взаимосвязанном мире. Тот участник, который лучше всего понимает местный контекст и строит сеть вокруг отношений, использующих местные возможности, с большей вероятностью выиграет. Целью когнитивной войны становится причинение вреда не только военным, но и всему обществу (противника, соперника, врага), причем этот тип войны напоминает действия «в серой зоне», где основным оружием становится влияние. В итоге автор дает ряд рекомендаций и заверений руководству НАТО:

– когнитивная война, стирая грань между миром и войной, включает НБИКС-технологии для использования в конкретных операциях, чтобы обеспечить надежный способ военного превосходства в ближайшем будущем»;

– в пяти первых доменах могут быть достигнуты тактические и оперативные победы; только в человеческом домене возможно одержать окончательную и полную победу.

Когнитивные операции представляют собой шестой домен гибридных войн, поэтому обобщенно их объединяют единым понятием «когнитивная война», которая ведется в самом уязвимом месте – мозге человека. Когнитивным операциям подвластно сознание

человека, его духовный мир, ценности, мировоззрение на субстратном и функциональном уровнях.

Когнитивная война заключает в себе глобальные риски не только сугубо технологического, но и геополитического, экономического, социально-антропологического и, экзистенциального порядка.

Когнитивная война, основанная на конвергенции когнитивных технологий, био- и нейротехнологий, технологиях искусственного интеллекта и обработки больших данных, стала мощным средством распространения дезинформации. Она представляет опасность для национальной и глобальной стабильности и безопасности на экономическом, геополитическом, социальном и культурном уровнях, поскольку нацелена на уязвимость людей как средство создания хаоса и замешательства в массовом сознании разных стран и внутри вооруженных сил.

Когнитивная война фокусируется не на области «информации», а на области «познания», т. е. на том, что мозг делает с информацией. Поэтому способы защиты от когнитивных вызовов и угроз должны рассматриваться как императив национальной и глобальной безопасности.

Способы обеспечения когнитивной безопасности в глобальном измерении связаны с выявлением внутренних связей между глобальными рисками и информационными вызовами и угрозами, возникшими благодаря развитию искусственного интеллекта, росту технологических возможностей анализа больших данных и интенсивному использованию достижений когнитивных наук и технологий. Это, в первую очередь, касается использования когнитивной психологии и лингвистики, нейробиологии и когнитивной антропологии, социологических и культурологических практик, то есть всей палитры естественнонаучных и гуманитарных знаний в военной науке и методов ведения когнитивной войны. Ответные меры на эти деяния заключаются в разработке теоретико-методологических оснований когнитивной безопасности, комплекса когнитивных технологий и практик, издание научной и учебной литературы, подготовка научных кадров, организация научных центров и лабораторий для ведения многопрофильной деятельности.

### 1.3 Философские и теоретико-методологические основы противодействия деструктивному влиянию информационно-психологических и когнитивных технологий на сознание человека

Разработка и применение мер нейтрализации деструктивного воздействия информационно-психологических и когнитивных технологий на сознание граждан

предполагает необходимость развертывания широкого фронта междисциплинарных исследований в области когнитивных наук и разработки когнитивных технологий, входящих в систему НБИКС-технологий. Речь идет, во-первых, о разработке теоретико-методологических оснований когнитологии, объединяющей соответствующие разделы философии, психологии, лингвистики, антропологии, нейробиологии и искусственного интеллекта, который в последнее время прочно укрепился в качестве объекта философской рефлексии [4]. Во-вторых, – о верификации методов, моделей, практик, заимствованных из этих разделов и используемых в информационно-психологических и когнитивных операциях (Cognitive Warfare). В-третьих, о систематизации соответствующих когнитивных технологий обеспечения информационно-психологической и когнитивной безопасности, являющейся неотъемлемой частью национальной безопасности, что было закреплено в Доктрине информационной безопасности Российской Федерации: нейтрализация информационно-психологического воздействия, в том числе направленного на подрыв исторических основ и патриотических традиций, связанных с защитой Отечества (ст. 21д), а также противодействие использованию информационных технологий для пропаганды экстремистской идеологии» (ст. 23а) [5]. Именно в этом аспекте обнаруживается тесная связь между современными достижениями философии сознания и теоретическими концепциями региональной и международной безопасности. Ключевую роль в этом играет информационный подход к объяснению феномена ментальной причинности [6].

В настоящее время информационное пространство активно используется при трансграничном обороте информации, в том числе специальными службами отдельных стран в целях оказания информационно-психологического воздействия, направленного на дестабилизацию внутриполитической и социальной ситуации в различных регионах мира. Одновременно с этим информационное пространство послужило становлению и ускоренному развитию когнитивных технологий, которые являются источником нового технологического уровня информационных угроз безопасности личности, общества и государства. Современное межгосударственное противоборство осуществляется не только военно-политическими и социально-экономическими методами и средствами, но и с применением информационно-психологических и когнитивных технологий, которые позволяют воздействовать на сознание каждого отдельного гражданина и в том числе военнослужащего.

## 2 Гибридный конфликт как конфликт XXI века

### 2.1 Гибридный угрозы: сущность понятия

Понятие «гибридные угрозы» предложено в теории гибридной войны, под которой первоначально понимались «вооруженные конфликты, где используются различные формы и методы ведения вооруженной и невооруженной борьбы» (крупномасштабные информационные операции, кибероперации, быстрое развертывание и широкое применение сил специального назначения, сочетание регулярных и повстанческих сил и т. д.) [7].

Создатель теории гибридной войны Ф. Хоффман определяет гибридные угрозы как исходящие от любого противника, использующего одновременно обычные вооружения, нерегулярную тактику, терроризм и преступное поведение в боевом пространстве для достижения политических целей [8]. НАТО расширяет определение до угроз, создаваемых противниками, способными одновременно использовать традиционные и нетрадиционные средства для достижения своих целей, что позволяет включать в перечень гибридных угроз формы экономического противоборства, психологические операции и другие действия [9]. Гибридные угрозы подразумевают подготовку сил, способных совершить государственный переворот в стране-мишени в пользу страны-инициатора переворота, что было многократно продемонстрировано США за последние десятилетия, включая подготовку и осуществление государственного переворота на Украине в 2014 г. и разностороннюю поддержку гибридных операций против России с началом СВО.

Прежде всего, следует указать на различие западного и российского подходов к определению данного понятия и выделению его ключевых маркеров.

В западном научном и политическом дискурсе термином «гибридная война», как правило, характеризуют реакцию России и населения русскоязычных районов Украины на государственный переворот в этой стране. На встрече Совета министров иностранных дел стран НАТО, состоявшейся 1 декабря 2015 г., была даже принята «Стратегия гибридных войн» и дано определение гибридной войны как тактики «при которой речь не идет об открытом применении обычных военных средств. Она включает в себя пропаганду и дезинформацию, методы экономического давления, а также тайное использование сил специального назначения» [10]. Тем самым, термин «гибридная война» получил закрепление в одном из стратегических документов НАТО.

Европейская внешнеполитическая служба на своем официальном сайте характеризует гибридные угрозы, прежде всего, как *действия* (традиционные и нетрадиционные, военные и невоенные), перечисляя их варианты от кибератак до нарушения поставок энергоносителей [11]. Если понимание угрозы как, например,

*состояния* [12], способного перерасти в военный конфликт, все же подразумевает отсутствие этого конфликта и не всегда связано только с субъективным фактором (противником), то угроза как *действие* всегда подразумевает активную деятельность противника, который в данной ситуации перестает быть предполагаемым, следовательно, и контрмеры будут направлены не столько на урегулирование ситуации, сколько на ограничение возможностей другой стороны.

Российские ученые, под гибридным конфликтом предлагают понимать проведение масштабной подрывной деятельности «без участия регулярных вооруженных сил нападающего государства, но с опорой на те внутренние политические силы страны-жертвы, которые разделяют позицию нападающего государства, с целью смены режима страны-жертвы или радикального изменения ее политики при массированной материальной и информационной поддержке» [13].

В России значимый вклад в разработку теории гибридной войны внес начальник Генерального Штаба ВС РФ В. В. Герасимов, отметивший в 2013 г., что «правила войны» существенно изменились: Возросла роль невоенных способов в достижении политических и стратегических целей, которые в ряде случаев по своей эффективности значительно превзошли силу оружия. «Акцент используемых методов противоборства смещается в сторону широкого применения политических, экономических, информационных, гуманитарных и других невоенных мер, реализуемых с задействованием протестного потенциала населения. Все это дополняется военными мерами скрытого характера, в том числе реализацией мероприятий информационного противоборства и действиями сил специальных операций. К открытому применению силы зачастую под видом миротворческой деятельности и кризисного урегулирования переходят только на каком-то этапе, в основном для достижения окончательного успеха в конфликте. Широкое распространение получили асимметричные действия, позволяющие нивелировать превосходство противника в вооруженной борьбе. К ним относятся использование сил специальных операций и внутренней оппозиции для создания постоянно действующего фронта на всей территории противостоящего государства, а также информационное воздействие, формы и способы которого постоянно совершенствуются» [14].

Таким образом, можно сделать вывод о том, что гибридный конфликт – это, по большому счету, война чужими руками. Государство-агрессор воздерживается от прямого вмешательство во внутренние дела суверенного с формальной точки зрения государства, но при этом активно поддерживает различные оппозиционные, а зачастую и экстремистские движения. Успех же оппозиции – дисциплина в сохранении ненасильственного характера протеста с целью привлечения как можно большего числа

граждан, создавая «оболочку» массовости движения, с целью легитимации борьбы в глазах внутренней и международной общественности. Однако на заключительном этапе, требуется использование сравнительно небольшой группы вооруженных участников оппозиции в качестве «острия копья», за которыми должны последовать наиболее радикально настроенные активисты, в основном молодежь, чтобы нанести решающий удар по силовым структурам действующей власти, при этом такое действие преподносится альтернативными независимыми и международными СМИ как «оправданная» реакция на насильственные действия власти против мирно протестующих граждан.

Умело апробировав данные технологии в Северной Африке, США принялись экспортировать революции в иные регионы, вплотную подбираясь к границам Российской Федерации.

При этом успех на «полях» гибридной войны зависит от полноты реализации следующих этапов:

1. Психолого-идеологическая обработка общества противника. Этот этап является подготовительным. Его цель заключается в том, чтобы подорвать *столпы поддержки* действующей власти путем постепенного перетягивания на свою сторону источников власти от представителей интеллигенции и предпринимателей, чиновников и силовых структур до простых граждан. При этом сам этот процесс происходит плавно и приносит свои результаты исключительно на поколенческом уровне (10-15 лет). В государстве-мишени или целевом-государстве под предлогом развития культурного сотрудничества, например, создается разветвленная сеть культурных центров и НКО, которые усиленно прививают населению государства-мишени новые «прогрессивные» ценности, ничего общего не имеющие с исторически сложившимся на данной территорией культурным кодом. Таким образом, происходит постепенное замещение превалирующих в государстве-мишени национальных ценностей иными ценностными установками. В результате, на территории государства-мишени вырастает целое поколение людей, которые больше не ориентированы на самобытное развитие своей страны, но видят свое будущее и будущее своих детей исключительно в случае интеграции с Западным миром, пусть даже и ценой разрушения государственности в своей собственной стране. Это означает, что при наступления критического момента, так называемого «часа Х», возможна очень быстрая мобилизация людских ресурсов, обеспечивающих массированную поддержку проводимой операции.

2. Создание общественного мнения в планетарном масштабе, оправдывающего рост протестных настроений в государстве-мишени и деятельность оппозиции

действующей власти, в том числе насильственного характера. Эту задачу успешно решают западные транснациональные средства массовой информации, большинство из которых имеют штаб-квартиру в США, Канаде, Великобритании, Франции, Германии и других западных странах. Они обладают широким отрядом средств массовой информации, которые выходят миллионными тиражами и располагают широкой сетью корреспондентских бюро и представительств по всему миру. Указанные средства массовой информации распространяются в десятках странах, становясь весьма эффективным средством распространения западной культуры и западных ценностей в странах с иным культурно-цивилизационным кодом. При этом особенно подчеркнем, что в оценке происходящих в мире событий западными журналистами нередко превалирует официальная точка зрения внешнеполитических ведомств западных стран, преимущественно Государственного департамента США. А поскольку ведущие американские новостные телеканалы распространяются при помощи спутниковых и кабельных каналов связи, данное обстоятельство открывает возможность ведущим мировым информационным державам посредством использования своего информационного превосходства проводить выгодную им политику, направленную на достижение глобального геополитического лидерства, зачастую свергая неугодные режимы путем умелого манипулирования массовым сознанием. На примере Украинского конфликта следует признать, что подобные публикации в зарубежных масмедиа, создают устойчивый отрицательный образ России в глазах зарубежной общественности. В результате, можно констатировать, что России не удалось получить у западной аудитории широкую поддержку своей версии событий на Украине. Большинство жителей ключевых государств-членов ЕС считают виновными в развязывании войны на Украине либо Россию, либо пророссийских сепаратистов, в то время как версия событий, продвигаемая российскими СМИ, заключалась в том, что конфликт произошел по вине Украины и Запада. Однако значительная часть жителей европейских государств не принимает аргументы российских СМИ и соглашаются с версией событий, предоставляемой европейскими СМИ.

3. Расшатывание общества изнутри при помощи различных техник манипулирования сознанием с тем, чтобы сами граждане того или иного конкретного государства своими руками разрушили государственность в своей собственной стране. Эту задачу призваны решать социальные сети. Особенно следует обратить внимание на тот факт, что социальные сети не являются информационными ресурсами как таковыми. Это средство коммуникации между людьми и их основная задача – это не просто информирование людей относительно тех или иных происходящих в мире событий. Их

основная задача – вовлечение и мобилизация. А поскольку контент социальных сетей создается простыми пользователями, возникает существенная проблема в установлении достоверности передаваемой посредством социальных сетей информации. Кроме того, большинство наиболее известных и популярных в мире социальных сетей имеют штаб-квартиру в США, а значит, они не подпадают под юрисдикцию стран, в которых они распространяются, так как просто не имеют там своих представительств. К тому же распространяют они информацию, руководствуясь исключительно корыстными либо политическими целями, которые преследует та или иная часть правящей американской политической элиты. Достаточно в качестве примера вспомнить случаи с блокированием аккаунта Трампа в Tweeter во время его предвыборной кампании 2020 г., который на тот момент был действующим президентом США. Таким образом, можно сделать вывод, что социальные сети сегодня превратились в мощный инструмент влияния, способный кардинальным образом менять общественное мнение в планетарном масштабе путем вирусного распространения нужного контента и блокирования сообщений и постов, которые признаны нежелательными. Власти России, оценив угрозу, которая исходит от американских социальных сетей, которые упорно игнорировали любые запросы Роскомнадзора об удалении контента, признанного в России недостоверным либо экстремистским, в начале марта 2022 г. приняли решение о блокировки сначала Facebook, а затем и Tweeter на всей территории страны. Разумеется, деструктивный контент время от времени появляется и на страницах российских социальных сетей, например, ВКонтакте. Он выявляется, блокируется, но проблема заключается в том, что вместо заблокированного ресурса может тут же появиться десяток новых. К тому же сам заблокированный ресурс до момента своей блокировки может вирусным образом распространиться в сети и до того, как он будет выявлен и заблокирован уже подорвать ментальное здоровье определенных слоев население. И в результате подобной «промывки мозгов» в обществе может набраться критическая масса молодых и энергичных людей, готовых быстро мобилизоваться и выйти на улицу с требованием перемен, организовать акции протеста и т.п. При этом митинги могут возникнуть стихийно, по первому зову, распространенному в социальных сетях.

Особенность эпохи современных информационных войн заключается в том, что теперь для того, чтобы призвать людей к организации масштабных акций протеста не требуется их объединение вокруг одного или нескольких одиозных оппозиционных лидеров. Профессиональные «манипуляторы» массовым сознанием просто делят потенциальную многомиллионную аудиторию на небольшие группы, стараются говорить на их языке, а в своих постах и сообществах – «бьют точно в боль», ставя те вопросы,

которые волнуют аудиторию в данный конкретный момент и, предлагая решение, как правило, связанное со сменой правящего режима, что создает вполне реальную угрозу для государственности.

Еще одним фактором, влияющим на изменение содержания современных способов вооруженной борьбы, является применение современных робототехнических комплексов военного назначения и активное использование технологий ИИ как важного инструмента гибридного противоборства, будь -то это военных операций, сфера финансов, прогнозной аналитики или манипулирования информационной повесткой дня. Особое место в этом анализе отводится проблеме злонамеренного использования ИИ в практике гибридных войн.

### 2.2 Государственные и негосударственные акторы, которые ведут гибридную войну против России

С распадом Советского Союза и крушением биполярной системы наступила новая эпоха в развитии международных отношений, которая означала уход с внешнеполитической арены одного из наиболее влиятельных ее акторов, который во многом сдерживал гегемонистские устремления США. И мир несмотря на то, что на самом высшем уровне звучали заверения о конструировании многополярной системы, стал быстро скатываться к однополярной, в которой США могли диктовать свою волю всему мировому сообществу.

Однако с наступлением XXI века стали возникать и уверенно заявлять о себе новые центры силы, прежде всего Китай и Индия. Активно включилась в обсуждение международной повестки дня и Россия. В этой связи представляется вполне закономерным то обстоятельство, что постепенно стали накапливаться противоречия между основными центрами силы: США и их западными союзникам, Россией и Китаем. Каждый из вышеперечисленных акторов международных отношений имеет свои национальные интересы, равно как и представления о безопасном и справедливом мире. И представлялось только вопросом времени, когда накопленные противоречия перерастут в активное противостояние.

Поскольку и США, и Россия, и Китай располагают ядерным оружием, представляется маловероятным, что в обозримом будущем состоится прямое вооруженное противостояние между этими странами, которое будет означать «конец истории» в буквальном смысле этого слова. США учитывают это обстоятельство, и поэтому они взяли курс на дестабилизацию мировой политической системы путем поощрения протестных движений в странах Северной Африки, Ближнего Востока и постсоветского

пространства, вплотную подбираясь к границам Российской Федерации, создавая, тем самым, прямую угрозу ее национальной безопасности.

Таким образом, можно сделать вывод о том, что основными государственными актором, который ведет гибридную войну против России являются США и возглавляемая ими коалиция Западных государств. Государственными структурами, министерствами и ведомствами США, подконтрольными и финансируемыми правительством США НКО накоплен значительный опыт в этой сфере, разработаны подробные инструктивные документы, подготовлены квалифицированные кадры, развернута соответствующая инфраструктура, как на территории самих США, так и, что более важно, в локациях, максимально приближенным к так называемым «государствам-мишеням» или «целевым государствам». Это означает, что в случае наступления критического момента, так называемого «часа Х», возможно очень быстрое развертывание значительных ресурсов, обеспечивающих массированную поддержку проводимой операции.

Однако помимо государственных акторов коллективного Запада в гибридном противоборстве стран Запада против России большая и во многом автономная роль принадлежит крупнейшим IT-корпорациям США. Так еще в 2017 г. Google объявила о своем намерении понизить поисковый рейтинг репортажей российских государственных изданий Russia Today (RT) и Sputnik. А СВО позволило IT-корпорации США извлечь немалые выгоды.

Во-первых, им удалось избежать формирования единого фронта государств и широкой международной общественности по противостоянию этим корпорациям и нарастающей конфронтации с ними по принципиальным вопросам. Такая конфронтация могла возникнуть из-за того, что эти корпорации вступают в борьбу с государственными и негосударственными акторами, у которых во многом другие устремления. Однако сейчас и в ближайшем будущем крупнейшим IT- корпорациям США, возможно, в меньшей мере надо будет бояться глобальных инициатив или коалиций, которые могут возникнуть с целью ограничить их растущие аппетиты и влияние. ООН и многие другие международные структуры фактически парализованы острыми геополитическими противоречиями.

Во-вторых, ведущие IT-компании США продемонстрировали, что они выступают в качестве мощного инструмента проведения кибероперацій, направленных против России. Таким образом, формирование информационной повестки дня в Соединенных Штатах, которая сегодня немыслима без полноценного использования технологий ИИ, оказалось открыто подчинено военно-политическим интересам и потребностям информационно-психологической войны.

В-третьих, любому правительству США в период острого геополитического противоборства понадобится информационная и аналитическая поддержка, которую IT-компании могут оказать, используя последние разработки в области ИИ, включая противодействие «внутренним» врагам и «дезинформации». Согласно документам, опубликованным 31 августа 2022 г., более пятидесяти чиновников администрации президента Байдена из дюжины агентств участвовали в попытках оказать давление на ведущие IT- компании, чтобы они осуществляли противодействие предполагаемой дезинформации. Документы были частью предварительного слушания в иске против правительства, поданном генеральными прокурорами Миссури и Луизианы, к которому позже присоединились эксперты, оклеветанные федеральными чиновниками.

В-четвертых, процветание крупнейшим IT- корпорациям США под «зонтиком» ВПК в период новой холодной войны нужно компенсировать потери от ухода с российского рынка. В условиях холодной войны легче избежать общественного внимания и скандалов из-за многообещающих разработок, которые не только несут большие прибыли, но и серьезные риски для человечества.

## 2.3 Гибридные атаки против России: практика применения и способы противодействия

### 2.3.1 Психолого-идеологическая обработка

Страны постсоветского пространства являются основными мишенями гибридных атак со стороны США и их союзников, которые ставят перед собой цель окружить Россию так называемым поясом нестабильности. При этом, следует особенно отметить, что США всегда рассматривали Россию в качестве своего основного геополитического противника, даже в период видимого потепления в отношениях между двумя странами, наметившегося сразу после окончания «холодной войны».

В этой связи, практически одновременно с крушением Советского Союза, когда в систему международных отношений были в буквальном смысле «выброшены» новые акторы, которые по большому счету на тот момент не имели четко выраженных стратегий национального социально-экономического развития, США стали обрабатывать население, проживающее на территориях недавно получивших независимость государств с тем чтобы разорвать устойчивые культурно-исторические связи с их исторической Родиной.

Началось все с того, что на территорию всех постсоветских государств, включая Россию, в 1990-е гг. хлынул широкий поток западной массовой культуры (американские фильмы, индустрия быстрого питания и пр.) и западных ценностей, которые постепенно стали вытеснять национальные. Особенный акцент стал делаться на переписывание

истории, попытку возложить вину за развязывание Второй мировой войны, в том числе и на Советский Союз, наравне с Германией, а населению постсоветских государств активно внедрялась мысль о том, что русские – это оккупанты, захватившие их землю. Все это привело к тому, что на территории постсоветских государств выросло целое поколение людей, воспитанное на иных ценностях и мечтавших об интеграции с Западным миром.

Также США в течение 1991– 2000 гг. создали существенные заделы: были отобраны и подготовлены активисты, созданы соответствующие информационные и пропагандистские онлайн и офлайн ресурсы, произведен «посев» пока «спящих» НКО и т.п.

Отчетливо все это видно на примере Украины, которая, как и многие другие страны СНГ, стала успешным проектом публичной дипломатии США. В этой стране еще в 1992 г., был открыт офис Агентства международного развития США, а ЦИК Украины стал основным партнером Агентства.

В целом, о значимости работы на украинском направлении свидетельствует тот факт, что Украина всегда являлась второй по значимости страной в проектах публичной дипломатии США и получала наибольшее финансирование после Грузии – в среднем показатель до начала СВО составлял в районе 200 млн $ в год, а в отельные годы даже превышал 500 млн $ в год.

На Украине были полностью реализованы следующие направления политических программ публичной дипломатии США:

- изменение законодательства, связанного с функционированием партий и неправительственных организаций;

- создание лояльных *СМИ*;

- создание сети НКО для молодых активистов.

- создание широкой коалиции оппозиции

А политика «промывания мозгов» и насильственной украинизации во многом деформировала сознание украинской молодежи. События 2014 – 2015 годов и конфликт вокруг Донбасса позволяет правящим элитам постоянно поддерживать высокий градус подачи России как «силы зла», главного врага.

Интересен и кейс Армении, политическое руководство которой после прихода к власти Н. Пашиняна заявляло о том, что Армения продолжает оставаться ключевым союзником Москвы на Кавказе. Однако достаточно быстро в Армении все ключевые посты в органах власти заняли люди, которые в той или иной степени были связаны с западными благотворительными фондами, прежде всего Фондом Сороса. Кроме этого, за последние годы были утрачены какие-либо контакты с Россией в военной сфере, в

частности в сфере обмена разведданными, а также в Генштабе Армении прошли массовые увольнения офицеров, проходивших обучение в Москве. Затем, Армения присоединилась к Римскому статуту Международного уголовного суда, выдавшего ордер на арест Президента России, что не могло не сказаться на отношении между двумя странами. А в 2024 г. Армения заморозила свое участие в ОДКБ и уже 4 раза подряд отказывается от проведения совместных военных учений.

И в целом, говоря про Армению, следует сказать, что она, как и все другие страны, испытавшие на себе «цветные революции», также прошла через несколько значимых проектов публичной дипломатии США, которые создали в Армении центры по мониторингу выборов. Вся страна была покрыта сетью таких организаций. Были созданы региональные информационные центры для повышения компьютерной грамотности населения, чтобы простые граждане были ориентированы на нужные информационные ресурсы. Был создан такой слой населения как *гражданские блоггеры*. Около 3 000 граждан Армении стали активными самостийными журналистами и блогерами и распространяли нужную США информацию.

Однако при этом помимо разработки и проведения всех этих мероприятий требуется еще и создание благожелательного общественного мнения как внутри страны-мишени, так и в глазах международного сообщества в целом. Достигается это путем умелого манипулирования общественным мнением как при помощи средств массовой информации, так и посредством социальных сетей. А основным инструментом манипуляций продолжают оставаться ложные новости и дезинформация.

### 2.3.2 Ложные новости и дезинформация

Ложные новости как средство манипуляции общественным мнением стали применяться достаточно давно, еще до появления социальных сетей. Их цель – создание в обществе нужных настроений, оправдывающих, например, применение военной силы против суверенного государства.

Наиболее ярким примером, в этой связи, будет являться выступление 10 октября 1990 г. перед Комиссией по правам человека Конгресса США 15-летней кувейтской девушки по имени Наира ас-Сабах, которая со слезами на глазах рассказала о том, что, работая в больнице в Кувейте видела, как иракские солдаты ворвались в больницу и жестоко расправились с 15 новорожденными младенцами.

Ее слова, которые, к слову сказать, не были подтверждены какими-либо фактами, привели к победе в голосовании в Конгрессе США за военное вмешательство. Так началась война в Персидском заливе. Однако в 1992 г. выяснилось, что Наира на самом

деле никакая не беженка, а дочь кувейтского посла в США Сауда Нассера ас–Сауд ас-Сабах. А ее показания были придуманы PR-агентством Hill & Knowlton, которое наняло правительство Кувейта для манипуляции общественным мнением и дезинформации.

Говоря про ложные новости, нельзя не вспомнить и про знаменитую пробирку Колина Пауэлла, демонстрация которой на заседании Совета Безопасности ООН, как известно, послужила оправданием вторжения американских войск в Ирак, в котором, к слову сказать, никакого химического оружия так и не было обнаружено.

Ложные новости нередко применялись и в информационной войне против России, задолго до начала специальной военной операции. Так, еще в августе 2008 г. во время агрессии Грузии в Южной Осетии мир облетели кадры, на которых, если внимательно всматриваться, были одни те же люди, которые изображали «мертвецов», лежащих в разных позах и в разных местах. А другие изображали «скорбящих» возле мнимых трупов мирных граждан (см. Рисунок 2.1).


Рисунок 2.1 – Постановочные сцены, демонстрирующие жертвы среди мирного населения во время агрессии Грузии в Южной Осетии 08.08.2008

Но, наверное, наиболее показательный пример работы западных средств массовой информации – это освещение американским телеканалом FoxNews беспорядков, которые прошли в декабре 2011 г. в Москве после выборов депутатов Государственной Думы. По всей видимости для того, чтобы еще более драматизировать ситуацию американский телеканал, рассказывая о событиях в Москве, время от времени показывал картинку, относящуюся к беспорядкам в Греции. В результате, при более детальном рассмотрении можно было увидеть, что сотрудники полиции были одеты в форму греческой полиции, а на заднем плане, несмотря на декабрьский мороз, были видны зеленые пальмы (Рисунок 2.2).


Рисунок 2.2 – Вырванное из контекста видео, которое должно было демонстрировать беспорядки после выборов депутатов Государственной Думы, произошедший в Москве в декабре 2011 г.

Впоследствии, постановочные сцены часто использовались в Сирии. Так еще в сентябре 2013 г. на телеканале CNN появились кадры, демонстрирующие якобы применение правительственными войсками президента Асада химического оружия. Однако в 2013 г., во многом благодаря усилиям России, США, опираясь на подобные фейковые материалы, не удалось убедить мировое сообщество в том, что президент Асад действительно применяет запрещенные химические препараты.

Но в 2017 г. похожие материалы в эфире мировых СМИ вновь появились. В этот раз поводом послужила химическая атака в пригороде сирийского города Идлиб. Достаточно быстро мир облетели душераздирающие кадры жертв применения химического оружия. «Виновный» опять был практически моментально назначен. Им оказался президент Асад. Как известно, данная химическая атака стала поводом для бомбардировок сирийской базы ВВС в окрестностях Хомса. И это несмотря на то, что в руинах освобожденного от террористов Алеппо была найдена подпольная лаборатория по производству химического оружия, тогда как реальных фактов применения отравляющих веществ правительственными войсками так и не было предоставлено.

В следующем 2018 г. ситуация повторилась. Надо сказать, что Россия заблаговременно предупреждала о готовящейся провокации, о том, что боевики начали завозить видеооборудование для съемок этого фильма. Однако никто не обратил внимания на эти предупреждения. И вот в апреле 2018 г. эти провокации состоялись. Соответствующее видео появилось на просторах Интернета, на котором были показаны душераздирающие кадры, демонстрирующие химическую атаку на один из пригородов Дамаска. Данная атака стала поводом для президента Трампа начать ракетный обстрел сирийской территории. При этом Трамп даже не стал ждать завершения какого-либо

расследования этого инцидента. И это несмотря на то, что на следующий день после этой химической атаки был найден один из невольных участников этой сьемки – сирийский мальчик, который объяснил как их обманом завлекли в больницу и начали там всех поливать водой. Однако показания этого мальчика не нашли широкого освещения в эфире мировых СМИ, несмотря на предпринятые усилия со стороны России.

Таким образом, благодаря подобным видеоматериалам в глазах мировой общественности формируется устойчиво отрицательный образ России и ее союзников. После начала специальной военной операции наметился резкий рост подобного фейкового контента, направленного на дальнейшую демонизацию России.

Наиболее показательным примером, в этой связи, будет являться провокация в Буче. Как известно, российская армия вошла в Бучу на второй день специальной военной операции на Украине. Этот город находился под контролем ВС РФ до конца марта. Тридцатого марта российские военные покинули этот населенный пункт. Такое решение было принято после переговоров между Россией и Украиной в Стамбуле, которые прошли за день до этого. В качестве жеста доброй воли Москва объявила об уходе своей армии из Киевской, Сумской и Черниговской областей.

Спустя несколько дней западные и украинские СМИ распространили фото и видео из Бучи, на которых запечатлены трупы, лежащие на улицах города. Вскоре власти Украины заявили, что в этом городе, во время пребывания там вооруженных сил России, якобы произошло массовое убийство мирных граждан.

Это обвинение было растиражировано средствами массовой информации и было использовано киевским режимом как одно из обоснований срыва украинской стороной стамбульских договоренностей.

В дальнейшем наступила активная фаза специальной военной операции. При этом противник активизировал свои действия не только на поле боя, но и в информационном пространстве. Обращает на себя внимание тот факт, что на Украине еще в 2004 г. был создан специализированный Центр информационно-психологических операций, который напрямую курируется спецслужбами США. Из этого следует, что Украину долгие годы готовили к активному противостоянию с Россией. Основные задачи этого Центра:

– профилактическая и превентивная деятельность по дезинформации населения;

– информационный терроризм;

– «слив» нужной информации;

– проведение и сопровождение информационных спецопераций;

– формирование общественного мнения;

– создание и публикация «фейковой» информации, фото/видео материалов.

При этом ресурсы Центра информационно-психологических операций Украины поистине огромны. Кроме официальных украинских СМИ, под их руководством действует несколько тысяч ресурсов в сети Интернет – информационно-новостных сайтов, «пабликов» в социальных сетях, скоординированных групп пользователей социальных сетей. Также украинский Центр информационно-психологических операций взаимодействуют с оппозиционными ресурсами в РФ. Оказывают ему поддержку, помогая распространять нужный контент, безусловно и западные СМИ.

Конечно, за 2 года специальной военной операции фейков, посвященных конфликту на Украине, было создано достаточно большое количество, но мы бы хотели в качестве примера привести несколько, с нашей точки зрения, наиболее показательных случаев.

Весной 2024 г. в фейковом телеграм-канале прокуратуры Севастополя появилось видео, на котором председатель Совета Федерации Валентина Матвиенко во время своего визита в Севастополь заявила, что Крым – это Украина. А далее последовал совет российским войскам убегать из Крыма пока не поздно и заявление о том, что Россия никогда не победит в этой войне. Разумеется, сама Валентина Матвиенко никогда не делала подобных заявлений. Просто при поморщи технологий ИИ было изменено видео с реальной Валентиной Матвиенко, которая рассказывала о 4 Евразийском женском форуме, прошедшем с 18 по 20 сентября 2023 г. в Санкт-Петербурге. При этом внимательный анализ этого фейкового видео выдает дипфейк. Можно увидеть явное несоответствие мимики и произносимым фразам.

Тем, не менее, этот пример наглядно демонстрирует возможности данной технологии, которая позволяет любому человеку создать клон того или иного политика и манипулировать его словами и поступками. Данное обстоятельство дает возможность сделать вывод о том, что в современную эпоху дезинформации обществу придется иметь дело с дипфейками, которые могут представлять серьезную угрозу для национальной и международной безопасности. И эта угроза не является мнимой. Она вполне реальна.

А в сентябре 2024 г. в сети появилось видео, на котором якобы в Курской области роют траншеи под братские могилы для бойцов СВО. На деле, все эти кадры вообще не имеют никакого отношения к СВО. Они были сняты еще в августе 2020 г. и посвящены перезахоронению останков советских воинов, павших в августе 1942 г. при обороне Сталинграда, а сама церемония проходила на Россошинском военно-мемориальном кладбище в 30 километрах от Волгограда. Т.е. было просто взято вырванное из контекста видео, которое выдали за происходящее на курской земле.

При этом обращает на себя внимание как минимум 2 нестыковки. Во-первых, это крайне маленький размер гробов, а второе – почва. Как известно, в Курской области преобладает чернозем, а на видео отчетливо виден грунт рыжего и бурого цвета (Рисунок 2.3).

Рисунок 2.3 – Вырванное из контекста видео, которое должно было демонстрировать захоронение погибших в Курской области российских бойцов

Подобные примеры заставляют задуматься о необходимости разработать действенные механизмы контроля над дальнейшим распространением ложных новостей, которые позволили бы быстро блокировать токсичный контент. На наш взгляд, решение этой задачи лежит в трех плоскостях: технической, регуляторной и просветительской.

**Техническая** предполагает разработку программных методов по выявлению фейкового контента. В частности, сегодня специалисты в области компьютерных наук усиленно работают над созданием соответствующих алгоритмов, способных обнаруживать дипфейки. Но проблема заключается в том, что сейчас не существует технологии, способной определить дипфейки со 100-процентной вероятностью.

**Регуляторный** аспект предполагает ограничить распространение дипфейков на законодательном уровне. В Китае, например, уже действует закон, который обязывает компании, занимающиеся производством дипфейков, а в Китае таких компаний достаточно много, снабжать свою продукцию специальным водяным знаком. В России ввели уголовное преследование за дискредитацию деятельности Вооруженных сил Российской Федерации, которая предполагает наступление уголовной ответственности в том числе и за распространение фейковой информации, касающейся деятельности российской армии. А Роскомндзор регулярно выявляет и блокирует огромное количество Интернет-ресурсов, распространяющих недостоверные сведения о деятельности

российских властей. Но все эти меры не смогут обеспечить 100% защиту граждан от распространения токсичного контента. А на смену заблокированному сайту может прийти десяток новых. Это означает, что простая блокировка того или иного телеграмм-канала, например, проблему не решит. Надо четко понимать, что этим не оградить наших граждан от распространения токсичного контента. Кроме этого, нужно иметь ввиду, что с момента выявления токсичного контента до момента его блокировки тоже может пройти определенное время. И соответственно определенная часть людей успеет ознакомиться с этим видео или иным материалам. И ментальное здоровье этих людей уже будет подорвано.

Это значит, что несмотря на предпринимаемые в этой области усилия дальнейшая фейковизация современного информационного пространства будет продолжена, что не может не представлять серьезной угрозы для системы международной информационно-психологической безопасности.

Единственный способ, при помощи которого мы можем в определенной степени нивелировать угрозу, исходящую от злонамеренного распространения ложных новостей, заключается в повышении уровня **информационной культуры населения и его медиаграмотности**. При этом наибольший упор необходимо сделать исключительно на работу с молодежью (молодыми людьми в возрасте до 25 лет и детьми старшего школьного возраста), поскольку именно эта категория граждан наиболее уязвима и подвержена различного рода манипуляциям. Им следует подробно разъяснять относительно того, что любую информацию, в том числе и ту, которую они слышат в том или ином видеоролике, следует перепроверять при помощи нескольких источников информации. В этой связи представляется крайне важным ввести в школьную программу предмет, связанный с освоением медиагромотности и направленный на изучение основ работы с информацией и различными информационными ресурсами и в целом на развитие критического мышления.

**Кроме этого, на регулярной основе следует:**

- публиковать в СМИ информационно-аналитические материалы соответствующего содержания и организовывать обсуждение данной проблематики в эфире федеральных телеканалов, что, собственно, регулярно и делается. В частности, на канале Россия24 выходит телепередача СтопФейк, которая призвана развенчивать время от времени появляющиеся в информационном пространстве фейки;

- проводить соответствующие психологические тренинги и семинары в школах, вузах, на других площадках;

- организовывать профилактические беседы с родителями, которым надлежит с ранних лет разъяснять своим детям те опасности, которые таит в себе глобальная сеть Интернет и прививать им навыки уверенного ориентирования в быстро растущем информационном потоке.

Только последовательная реализация всех вышеперечисленных мер способна обеспечить эффективное противостояние массированным информационно-психологическим атакам, которым сегодня подвергается российское информационное пространство.

### 2.3.3 Распространение деструктивного контента в социальных сетях

Распространение деструктивного контента ориентировано на попытку расшатать российское общество изнутри. При этом способы воздействий применяются совершенно разные. Так, в частности, на видеохостинге YouTube действует канал OM-TV, который себя позиционирует «независимым» каналом в YouTube, на котором публикуется видео исключительно с критикой властей России (см. Рисунок 2.4) [15].

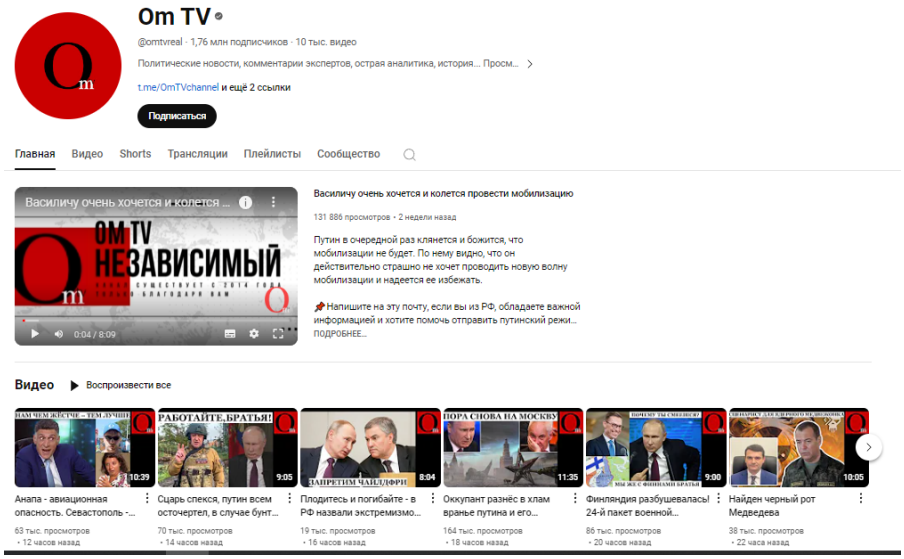


Рисунок 2.4 – Скриншот со страницы YouTube-канала OM-TV

Мы хотим обратить внимание только на несколько видеороликов, размещенных на данном канале, которые говорят сами за себя относительно содержания контента: «Анапа – авиационная опасность. Севастополь – снова осколки от ПВО. Планируйте отдых на море Лаптевых» (30 июня 2024 г.), «Сцарь спекся, путин всем осточертел, в случае бунта никто не защитит верховного» (29 июня 2024 г.), «Плодитесь и погибайте – в РФ назвали экстремизмом нежелание рожать детей» (29 июня 2024 г.). При этом обращает на себя внимание достаточно большое количество просмотров, лайков и положительных

комментариев, которые собирают подобные материалы. Так первый рассмотренный нами видеоролик собрал 64 139 просмотров и 4 тысячи лайков, второй – 70 628 просмотров и 4,9 тысяч лайков, а третий – 19 882 просмотров и 1.6 тысяч лайков. А сам YouTube канал имеет 1,76 млн. подписчиков.

Свой YouTube-канал есть и у Михаила Ходорковского [16]. При этом обращает на себя внимание тот факт, что этот канал имеет 2.3 млн. подписчиков, опережая по этому показателю «ОМ-TV», а размещенные там видеоролики регулярно собирает 150-200 тыс. просмотров (см. Рисунок 2.5).

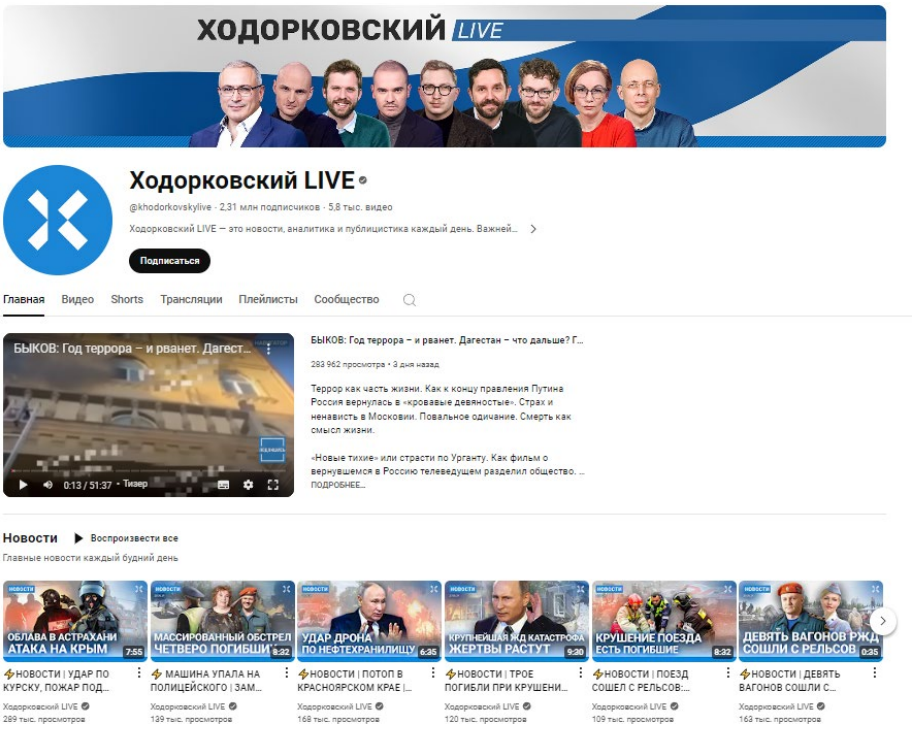


Рисунок 2.5 – Скриншот со страницы YouTube-канала “Ходорковский Live”

А вот пример другого YouTube-канала “Дневник Депутата” [17]. Его автор – Николай Бондаренко, в котором он публикует разные видеоролики с критикой российских властей (см. Рисунок 2.6).

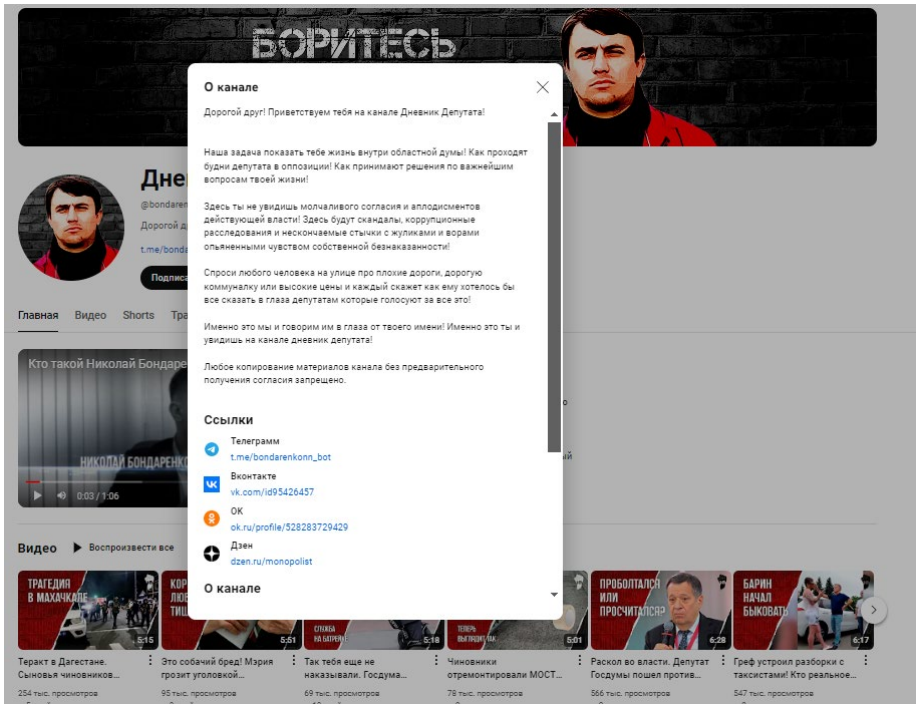


Рисунок 2.6 – Скриншот со страницы YouTube-канала “Дневник депутата”

В настоящее время этот канал имеет 1,9 млн. подписчиков, а размещенные там видеоролики собирают огромное количество просмотров. Так, в частности, размещенный на этом канале видеоролик, посвященный состоявшемуся 23 июня 2024 г. теракту в Дагестане, собрал 254 тыс. просмотров. Центральный вопрос, который поднимается в этом видеоролике – это доверие к власти, насколько власть способна обеспечить безопасность своих граждан. А это, по большому счету, и есть та цель, которую преследуют организаторы этих поражающих своей жестокостью террористических актов – посеять панику в российском обществе и снизить доверие к власти. Обращает на себя внимание и тот факт, что этот 5-минутный ролик собрал 11 тыс. лайков и свыше 2 000 комментариев следующего содержания (см. Рисунок 2.7):

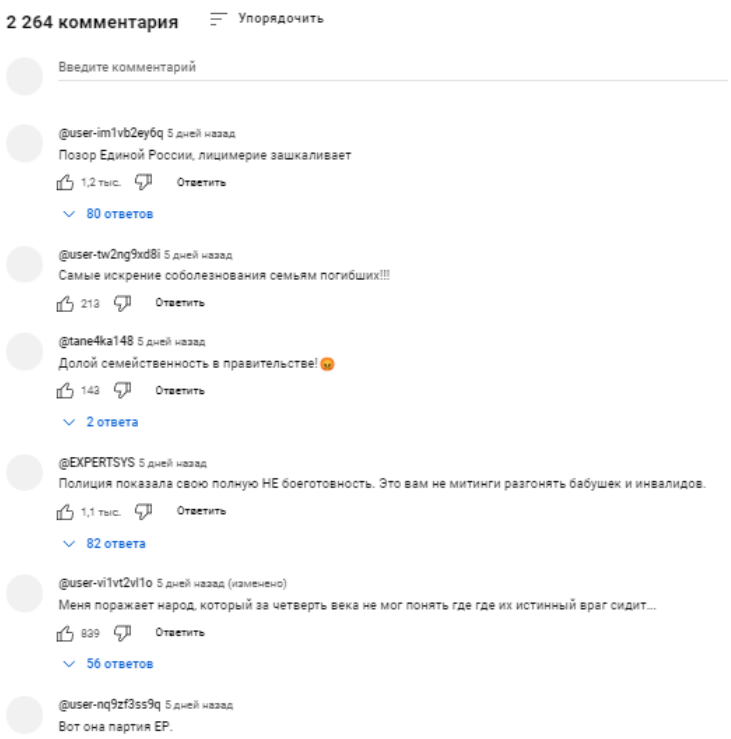


Рисунок 2.7 – Скриншот со страницы комментариев под видеороликом, посвященному теракту в Дагестане

Разумеется, подобный деструктивные контент можно встретить не только на видеохостинге YouTube, но и в мессенджере Телеграмм, который сегодня превращается в один из основных инструментов, посредством которого ведется вербовка новых сторонников в ряды ВСУ или иных террористических организаций.

Интерес, в этой связи, представляет Телеграм-канал «Соловьиный помет» [18], который имеет 343 983 подписчика и публикует посты, резко критикующие российскую власть. Мы хотим привлечь внимание к одному из закрепленных сообщений этого канала (см. Рисунок 2.8):

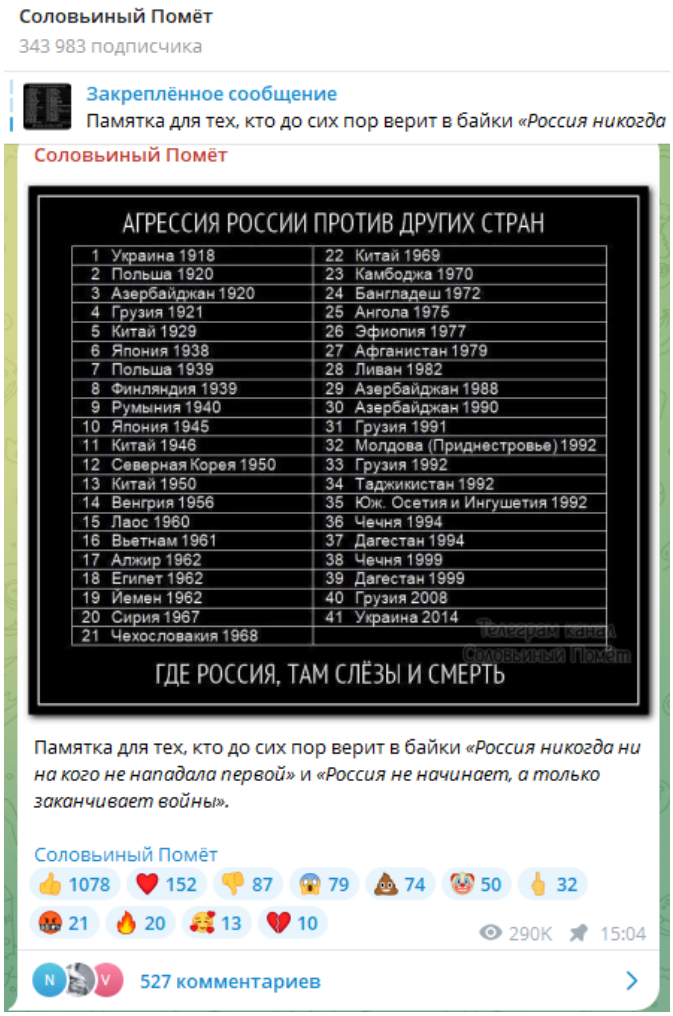


Рисунок 2.8 – Скриншот закрепленной записи из телеграмм-канала «Соловьиный помет»

Данная запись имеет 290 000 просмотров, свыше 1000 положительных реакции и только 87 негативных.

Цель подобных материалов - подогреть протестные настроения с тем, чтобы человек сам начал искать соответствующую информацию и пытался выйти на кураторов, работающих на службу безопасности Украины. При этом, первичная коммуникация возможна, как с живыми людьми, так и со специально созданными для этих целей чат-ботами, которые говорят на языке своей целевой аудитории и формируют для нее нужный контент.

В качестве примера приведем чат-бот «Храбрые партизаны», который был создан в Телеграмме практически сразу после начала специальной военной операции на Украине. После того как очередная жертва подобной промывки мозгов подключит себе этого бота, у него в мессенджере отобразится приветствие следующего содержания (см. Рисунок 2.9):

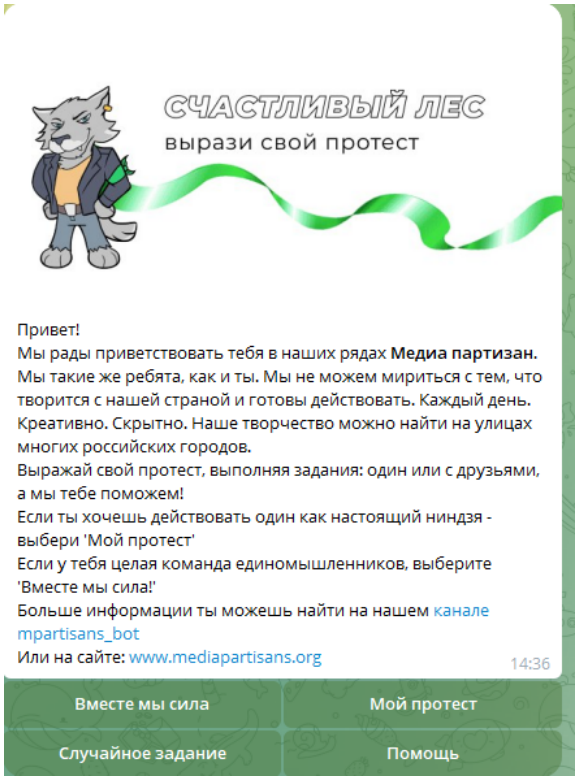


Рисунок 2.9 – *Приветствие телеграмм-бота «Храбрые партизаны»*

Т.е. этот бот помогает людям искать единомышленников, вступать с ними в коммуникацию, тем самым формируя различные деструктивные сообщества, ставящие цель разрушить Россию изнутри, и дает им различного рода задания. При этом, надо четко понимать, что наш противник будет постоянно нащупывать новые уязвимые места и атаковать российское информационное пространство, пытаясь посеять межконфессиональную вражду, например.

Наиболее яркий пример – прорыв протестующих на взлетное поле аэропорта Махачкалы 29 октября 2023 г. в связи с прибытием самолета из Тель-Авива. При этом, как известно, мобилизация протестующих проходила, как и обычно, посредством социальных сетей и мессенджера Телеграмм, который был основным каналом коммуникации среди протестующих. В результате 30-31 октября 2023 г. доступ к этому ресурсу в южных регионах России был ограничен.

В целом, этот кейс является достаточно показательным и наглядно демонстрирует уязвимость любого многонационального государства. При этом, насколько можно судить из посвященного этой тематики информационного потока, к этим событиям украинский Центр информационно-психологических операций имеет самое прямое отношение. Основным же инструментом, обеспечившим рост протестных настроений в Дагестане, стал телеграмм-канал «Утро Дагестана», принадлежавший бывшему депутату Государственной Думы Илье Пономареву, который после того, как против него возбудили

уголовное дело о растрате в 2014 г. бежал сначала в США, а затем перебрался на Украину, где получил сначала вид на жительство, а затем и гражданство. После беспорядков в аэропорту Махачкалы этот телеграмм-канал был заблокирован, а многие из тех, кто прорвался на взлетное поле – арестованы.

Но здесь важно разобраться со всей этой ситуацией и понять, что двигало этими людьми? Какие такие манипулятивные приемы заставили их совершить противоправное деяние? Ведь подобные акции могут повториться и в будущем. При этом простая блокировка телеграмм-канала проблему не решит. Вместо заблокированного 30 октября телеграмм-канала «Утро Дагестана» уже 3 ноября был создан телеграмм-канал «Утро Дагестана 2023» примерно с таким же содержанием (см. Рисунок 2.10).

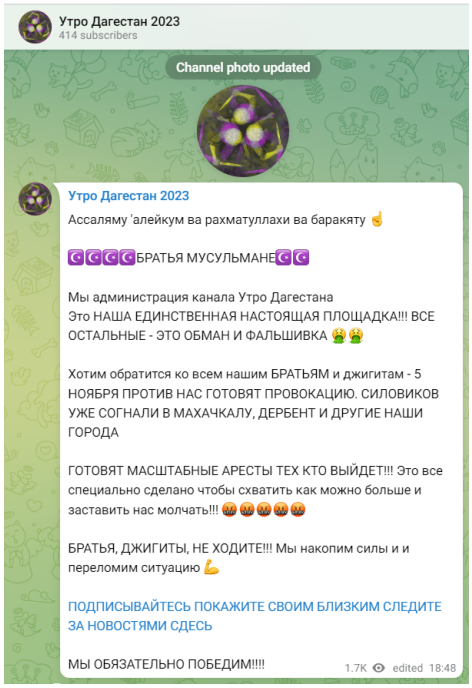


Рисунок 2.10 – *Скриншот с телеграмм-канала «Утро Дагестана 2023»*

Это означает, что подобная провокация под другим предлогом может повториться и еще раз подтверждает тезис о том, что простая блокировка того или иного телеграмм-канала или иного паблика в социальных сетях не способна решить проблему, поскольку вместо заблокированного контента может появиться новый.

К тому же, те же мессенджер «Телеграмм» может служить очень удобным способом для вербовки новых сторонников. В качестве примера здесь следует привести теракт в «Крокус Сити Холле», когда со слов террористов с ними на связь посредством мессенджера «Телеграмм» вышел некий «проповедник», который убедил их совершить этот террористический акт.

Разумеется, мессенджер «Телеграмм» используется и для вербовки исполнителей менее резонансных террористических атак и диверсий. Так еще в 2023 г. в Нижегородской области мужчина получил задание от неустановленного пользователя в Телеграмм и успел изготовить две бутылки с зажигательной смесью. Однако потом испугался и отдал их сотрудникам ФСБ. А в последнее время активизировались попытки вербовки российских лётчиков с тем, чтобы они перегнали свои воздушные суда на подконтрольную ВСУ территорию.

Отдельное направление информационно-психологических атак с территории Украины – мошеннические звонки российским гражданам, которые преследуют следующие основные цели:

1. Украсть денежные средства, часть из которых будет направлена на финансирование ВСУ – наиболее известным и показательным случаем в этой связи будет обман известной певицы Ларисы Долиной.

2. Убедить свою жертву при помощи различных изощренных методов социальной инженерии, включая подкуп и откровенный шантаж и даже угрозу убийством близких людей совершить диверсию на территории России: поджечь военкомат, совершить диверсию на объектах железнодорожной инфраструктуры и пр. – за последние 2 года случаев таких диверсий стало достаточно много.

Также, помимо активных действий в российском информационном пространстве, направленном на вербовку новых сторонников, наш противник стремится посеять панические настроения среди российских граждан. Так после атаки ВСУ на курскую область в начале августа 2024 г. Центром информационно-психологических операций Украины были созданы два телеграмм-канала «Самооборона Суджи» и «Самооборона Курской области», в задачи которых входило посеять панику среди местного населения и убедить людей, что представители власти спешно бегут из Курска, бросив своих граждан на произвол судьбы (см. Рисунок 2.11).

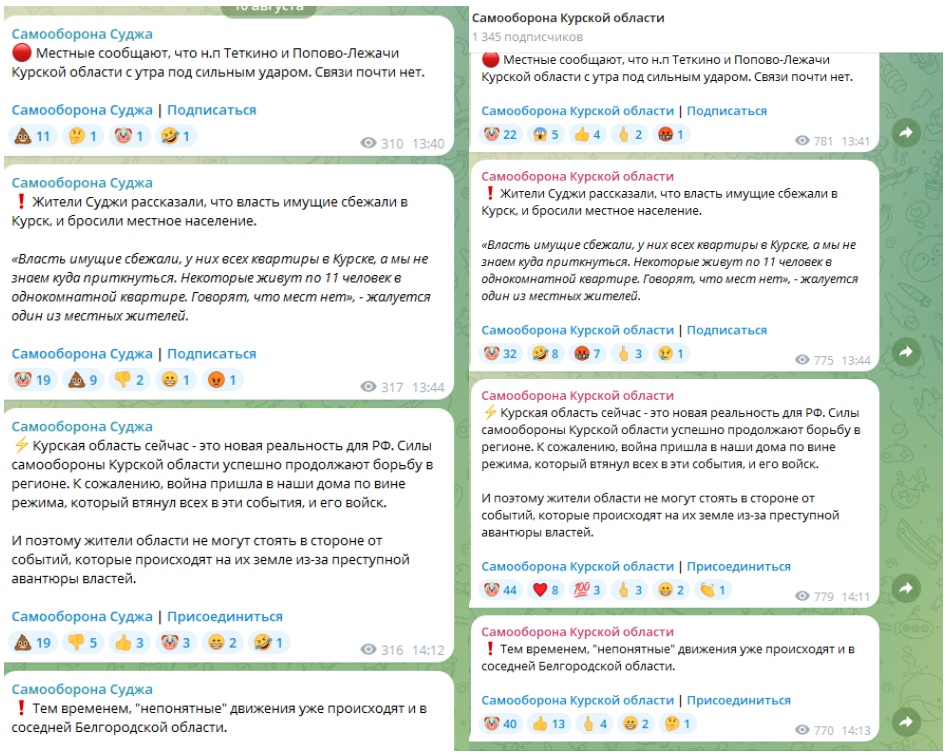


Рисунок 2.11 – *Скриншот с телеграмм-каналов «Самооборона Суджи» и «Самооборона Курской области»*

В результате можно вполне резонно задаться вопросом, какие конкретно нужно предпринять меры для того, чтобы обеспечить эффективное противодействием всем этим тайным информационно-психологическим операциям, нацеленным на разрушение устоев российской государственности изнутри.

Анализ опыта «цветных революций» дает нам основание прийти к выводу, что ключевым элементом, способным нивелировать исходящие со стороны стран коллективного Запада гибридных угроз продолжает оставаться всесторонняя поддержка правящей власти со стороны местного населения, поскольку именно проживающие на территории того или иного государства люди и формируют те самые столпы поддержки действующей власти, которые так стремятся разрушить архитекторы «цветных революций» используя для этого различные манипулятивные приемы.

Сегодня мы видим, что нашим противникам не удалось расшатать российское общество изнутри, а рейтинг поддержки Президента В. Путина продолжает оставаться достаточно высоким – в районе 80%.

С целью дополнительного измерения уровня поддержки российским обществом проводимой Правительством политики средствами языка программирования Python нами были собраны посты, размещенные в социальной сети «Вконтакте», которые в своих

текстах содержат ключевую фразу «Специальная военная операция». Нами была поставлена цель – определить отношение широких слоев населения к тематике СВО. В результате нами было собрано 148 278 постов. При этом сразу обратило на себя внимание единение русского народа перед лицом общего врага. Так в той оценке, которые дают люди происходящим на Украине событиям, преобладают следующие нарративы: «США враг», «Вашингтон за убийство», «наша независимость», «наша страна», «наше отечество», «русский человек», «погибнуть ребенок», «нанести стратегическое поражение России». Наглядно указанные метафоры можно видеть на приведенном Рисунке 2.12, который демонстрирует частоту встречаемости тех или иных слов в текстовых коллекциях:

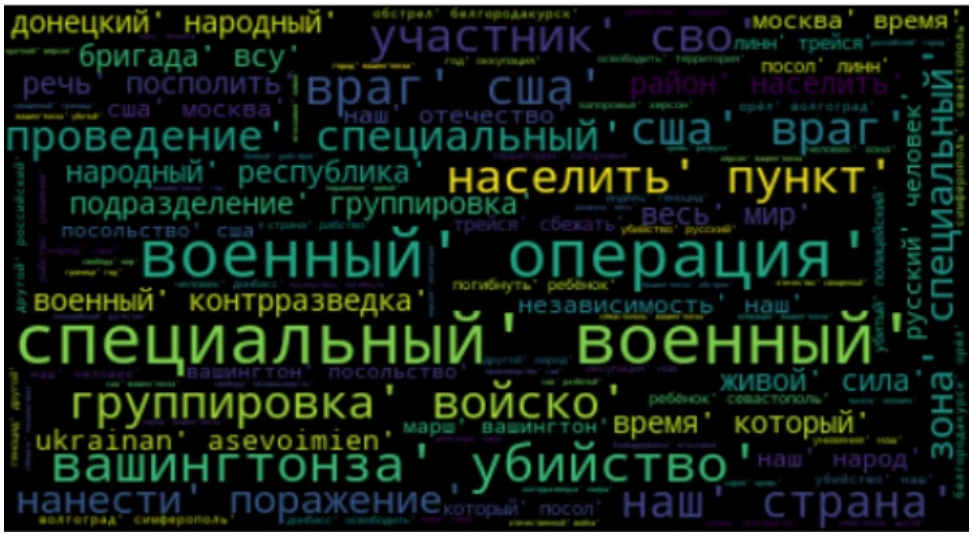


Рисунок 2.12 – Визуализация метафор, связанных с тематикой СВО по частоте встречаемости в постах, размещенных в социальной сети «Вконтакте»

Получив подобный результат, мы решили осуществить поиск постов, содержащих ключевое слово «неоколониализм». В результате, нами было собрано свыше 215 000 постов, опубликованных в период с 4 по 29 июня 2024 г. Частотный анализ контента указанных постов позволил выделить следующие достаточно устойчивые нарративы: «мягкая сила», «америка уходить», «франция уходить», «выкачивать ресурсы», «здравствовать президент».

Подобные примеры наглядно демонстрируют резко отрицательное отношение российского общества к политике Запада. Однако для того, чтобы подобный тренд сохранялся, на наш взгляд, России следует:

1. Продолжать выстраивать эффективный доверительный диалог между государством и гражданами, чтобы правящая элита знала насущные потребности широких

слоев населения, а люди, в свою очередь, чувствовали свою защищенность и были бы готовы мобилизоваться в условиях гибридной войны, развязанной Западом против России.

2. Донести до широкой общественности одну важную мысль, что война на Украине – это не некий локальный вооруженный конфликт. Сейчас идет вооруженное противостояние между Россией и США. И речь идет немного не мало, но о судьбе русского мира. Украина же в этой борьбе – это всего лишь инструмент, поскольку США, по понятным причинам, просто опасаются прямого вооруженного противостояния с Россией. Поэтому они, с одной стороны, стараются окружить границы РФ так называемы поясом нестабильности, а с другой – не прекращают попытки раскачивать политическую обстановку внутри России, используя для этого разнообразные манипулятивные приемы.

3. Максимально зачистить российское информационное пространство от нежелательного контента. К сожалению, мы видим, что Россия в информационной войне исключительно обороняется, т.е. фиксируется какой-то вызов – на него готовится симметричный ответ. Но так информационную войну не выиграть, поскольку основная тактика в информационно-психологическом противоборстве – это нападение. В качестве примера здесь можно привести тот факт, что на территории России западные СМИ были заблокированы только после начала специальной военной операции, тогда как на Западе деятельность российских СМИ фактически была парализована задолго до начала активных боевых действий на Украине.

4. Отдельное направление работы - патриотическое воспитание детей и молодежи. Сейчас в России разрабатываются новые учебники истории, вводятся в школе уроки о важном, но это та работа, которая должна была вестись постоянно на протяжении многих лет, поскольку и результат она сможет дать только на поколенческом уровне, но не за 2-3 года.

Только последовательная реализация вышеперечисленных мер способна обеспечить эффективное противостояние гибридной агрессии, которой сегодня подвергается Россия со стороны коллективного Запада, и выработке определенного иммунитета российского населения к информационно-психологическим атакам со стороны нашего основного геополитического противника.

# 3 Технологии искусственного интеллекта: новые возможности или новые риски

## 3.1 Искусственный интеллект общего назначения: миф или реальность

Искусственный интеллект представляет собой семейство технологий, способных имитировать когнитивную деятельность человека. Сегодня эти технологии активно проникает в нашу повседневную жизнь и используется в различных сферах, становясь, тем самым, не заменимыми помощниками. Они способны переводить текст на другой язык, проводить медицинскую диагностику и даже формулировать идеи, вести диалог, сочинять историй на заданную тему, писать картины, создавать видео, музыкальные произведения и многое другое.

Подобный взрывной рост их возможностей и производительности побудил в обществе дискуссии относительно будущего прорывных технологий и возможного наступления эпохи общего искусственного интеллекта, который способен превзойти человеческие возможности.

Примечательно, что в научном сообществе нет единой точки зрения на этот вопрос. Показательным в этой связи будет являться обзор IEEE Spectrum, в котором представлены мнения ведущих экспертов в отрасли по этому поводу [19].

Согласно данному обзору, можно сделать вывод о том, что в научном дискурсе существует две диаметрально противоположные точки зрения на этот вопрос. Одни ученые считают, что появление новейших разработок в сфере ИИ, и, прежде всего, больших языковых моделей является важным шагом на пути создания искусственного интеллекта общего назначения, тогда как другие, наоборот полагают, что БЯМ, несмотря на свои колоссальные возможности, сами по себе не являются чем-то инновационным и мало чем отличаются от многих предыдущих подобных потрясений в сфере технологического развития.

Так, в частности, Сэм Алтман, генеральный директор компании Open AI, разработавшей GPT, одну из наиболее популярных больших языковых моделей, считает, что появление БЯМ является важным шагом на пути разработки искусственного интеллекта общего назначения, но при этом он полагает, что это будет «медленный взлет» и у человечества «будет время для устранения реальных рисков, которые несет в себе эта технология».

Демис Хассабис, генеральный директор DeepMind, дочерней компании Google Alphabet, придерживается аналогичной точки зрения. Он прогнозирует, что в ближайшие несколько лет, а может быть, и через десятилетие, “у нас будут очень эффективные и универсальные системы”. Он объясняет свою позицию тем, что “прогресс за последние

несколько лет был просто невероятным”. И он не видит причин, по которым этот прогресс может замедлиться. По его словам, он может даже ускориться. А БЯМ следует рассматривать как переходное звено между искусственным узким интеллектом и искусственным общим интеллектом [20].

Дж. Хуан, генеральный директор Nvidia, ведущего мирового производителя ИИ-чипов, придерживается более взвешенной точки зрения. Он говорит, что “ответ во многом зависит от того, как определена цель. Если цель - это способность успешно проходить созданные людьми тесты, то искусственный интеллект общего типа скоро появится <...> Но, согласно другой точке зрения, до искусственного интеллекта общего назначения может быть гораздо дальше, потому что ученые все еще расходятся во мнениях о том, каким образом можно полностью сымитировать работу человеческого разума. И эту задачу не может решить простой инженер" [21].

Похожей точки зрения придерживается и Ян Лекун, который в свое время предложил архитектуру сверточной нейронной сети. С одной стороны, он признает, что «усиление человеческого интеллекта машиной приведет к новому ренессансу или новой эпохе просвещения, вызванной ускорением научного, технического, медицинского и социального прогресса благодаря ИИ», но с другой, согласно его точке зрения, большие языковые модели никогда не приведут к созданию ИИ со здравым смыслом и настоящим человеческим пониманием [20].

Схожую точку зрения высказывает и Гэри Маркус, профессор Нью-Йоркского университета, который, в целом признавая колоссальные возможности, которые несут с собой большие языковые модели, тем не менее, полагает, что их появление является необходимым, но недостаточным условием для возникновения искусственного интеллекта общего назначения. Согласно его точке зрения, «еще предстоит проделать огромную работу по созданию машин, которые действительно смогут понимать окружающий мир и рассуждать о нем» [20].

Похожей позиции придерживается Алисон Гопник, профессор Калифорнийского университета в Беркли, который сомневается в том, что большие языковые модели смогут стать разумными исключительно благодаря одному лишь тексту, поскольку они, по сути, обладают только одной способностью – это способностью к обобщению на основе данных, которые составили обучающую выборку.

При этом независимо от того, какая из представленных выше точек зрения является верной и обоснованной с научной точки зрения, следует признать, что большие языковые модели несут с собой как колоссальные преимущества, так и

труднопрогнозируемые риски, некоторые из которых уже стали реальностью. На это обстоятельство указывают многие исследователи.

Так, в частности, Йошуа Бенджио, профессор Монреальского университета, который убежден, что появление БЯМ не приведет к созданию искусственного интеллекта общего назначения, считает, что опасность будет исходить не от того, что эти модели станут автономными, а скорее от неправильного их применение, в результате которого произойдет резкий рост дезинформации и фейковых новостей, сгенерированных БЯМ, которые будут выглядеть очень правдоподобно [20].

Это означает, что любой технологической новации должно предшествовать исследование ее безопасности и возможных способов злонамеренного применения. Именно такой точки зрения придерживается Дке Хендрикс, директор и соучредитель Центра безопасности искусственного интеллекта. Развивает эту мысль Джефри Хинтон, профессор Университета Торонто, который утверждает, что БЯМ развиваются слишком быстро, и они не должны развиваться дальше, пока ученые не будут уверены, что могут контролировать их [20].

Принимая во внимание вышеописанные риски и угрозы, представляется очевидным, что параллельно с развитием самих технологий, национальные правительства должны уделять внимание их нормативно-правовому регулированию. На это обстоятельство указал, в частности, Тимнит Гебру, основатель Исследовательского института распределенного искусственного интеллекта, высказав мнение о том, что компании-разработчики больших языковых моделей нуждаются в нормативных актах для повышения прозрачности и подотчетности.

### 3.2 Развитие технологии искусственного интеллекта: мировой опыт

Принимая во внимание стремительное развитие технологий ИИ и те колоссальные преимущества, которые они с собой несут, представляется понятным, почему многие государства в мире провозгласили развитие технологий ИИ в качестве основного национального приоритета. Однако далеко не все из них обладают адекватной финансово-технологической базой, необходимой для ведения научно-исследовательских и опытно-конструкторских разработок в сфере ИИ. Обусловлено это тем, что для проектирования современных гибридных интеллектуальных систем требуется дорогостоящее оборудование. Наиболее наглядным примером будет являться стоимость обучения большой языковой модели GPT-4, которая обошлась компании OpenAI в 100 млн. долл. [22: 63]. Именно как раз поэтому только крупные корпорации способны заниматься проведением серьезных исследований и экспериментов в этой области. При

этом, согласно Стэндфордскому отчету за 2023 г., измеряющему уровень развития технологий ИИ в странах и регионах, лидирующие позиции заняли 4 американских IT-гиганта – Google, Meta[1], Microsoft и OpenAI, на долю которых приходится наибольшее совокупное количество базовых ИИ-моделей [22: 59].

В другом рейтинге, который демонстрирует лучшие стартапы мира в области ИИ по объему инвестиций также представлены преимущественно одни американские корпорации. По этому показателю. Компания OpenAI является бесспорным лидером с объемом инвестиций в 14 млрд. долл. Второе место принадлежит компании Anthropic, которая занимается разработкой альтернативы ChatGPT, получившей называние Claude. Ее объем инвестиций составил 4.1 млрд. долл. Замыкает тройку лидеров с объемом инвестиций около 4 млрд. долл. калифорнийская компания Databricks, которая предоставляет своим клиентам облачную платформу для управления данными, включая доступ к моделям генеративного искусственного интеллекта [23].

Принимая во внимание данное обстоятельство, представляется понятным, почему лидирующие позиции в общем мировом рейтинге развития технологий ИИ продолжают удерживать США. Тем не менее, другие страны также проводят активные научные исследования в сфере ИИ с целью достичь технологического лидерства. В этой связи, обращает на себя внимание успехи стран-участниц БРИКС, которое после его расширения в 2024 г. объединило 10 стран с быстро растущей экономикой и положительной динамикой рынка информационно-телекоммуникационных технологий. Согласно мировому рейтингу уровня развития технологий ИИ Китай находится на 2 месте, Индия – на 14, Россия – на 30, Бразилия – на 35, а ЮАР – на 54 [24: 122]. Одну из лидирующих позиций в мировых рейтингах по уровню развития технологий ИИ занимают ОАЭ. Так в составленном Стэндфордским университетом рейтинге наиболее значимых моделей машинного обучения Китай сохранил второе место, ОАЭ заняли 9 место, а замкнул топ-10 стран по этому показателю Египет [22: 47]. Предполагается, что в обозримом будущем эти страны продолжат инвестировать в разработку технологических инноваций, прежде всего в области искусственного интеллекта (ИИ), который способен оказать существенный импульс развитию их экономик.

### 3.2.1 Китай

Среди всех стран БРИКС наибольшее развитие технологии искусственного интеллекта получили в Китае, который является одним из мировых лидеров по этому показателю. Китайский рынок передовых информационных технологий “характеризуется

[1] Деятельность компании Meta запрещена в России.

устойчивым ростом инвестиций и инвестиционной стоимости компаний, занимающихся ИИ, растущим рынком технологий ИИ и сильным ядром транснациональных компаний китайского происхождения, разрабатывающих и продвигающих их использование среди потребителей” [25: 338].

Еще в 2016 году в Китае было принят рассчитанное на 3 года "Руководство по Интернету и искусственному интеллекту" (2016-2018), согласно которому правительство взяло на себя обязательство сосредоточить внимание на финансировании и развитии технологий ИИ [26]. А в следующем 2017 г. в стране был принят “План развития искусственного интеллекта следующего поколения”, который представляет собой стратегию технологического развития страны до 2030 г. и “ставит задачу возвратить КНР утраченное положение технологического лидера, которое, по мнению китайского руководства, страна занимала большую часть своей истории. Для Пекина глобальное цифровое пространство выглядит полем боя, где основные развитые страны пытаются доминировать в новом раунде международной технологической конкуренции, и перед Китаем стоит задача твердо захватить стратегическую инициативу на новом этапе международной конкуренции в развитии ИИ” [27: 14].

При этом повышенное внимание в своей национальной стратегии Китай уделяет таким сферам, как Интернет вещей и генеративный ИИ. Также в Китае в 2020 году была создана государственная Инфраструктурная блокчейн-платформа (BSN), а в марте 2021 г. правительство страны представило пятилетний план, направленный на ускоренное развитие передовых технологий. Особый акцент Китай планирует сделать на создании национальных лабораторий в сфере ИИ, разработке адресных государственных программ по поддержке этих технологий, расширение налоговых льгот для поощрения дальнейших исследований и разработок в данной сфере.

Подобная политика привела к тому, что по формальным показателям, таким как количество опубликованных научных работ и заявок на патенты, Китай смог не только сравняться с Соединенными Штатами, но и стать мировым лидером [28]. Но появление больших языковых моделей и их стремительное развитие оказались неожиданными для Китая, и китайские разработчики не были готовы к конкуренции в этой области, поскольку они были сосредоточены на других областях науки о данных, таких как компьютерное зрение, беспилотные транспортные средства, умные города и распознавание голоса. Но они смогли быстро переориентироваться и за короткий период выпустить большое количество больших языковых моделей, одна из которых под названием GLM-4-9B-Chat, разработанная китайским стартапом Zhipu AI, смогла продемонстрировать лучшее качество, чем GPT-4o [29]. Этот наглядно демонстрирует,

что китайские компании умеют быстро приспосабливаться к меняющимся тенденциям и решать сложные задачи.

Кроме этого, обращает на себя внимание и тот факт, что Китай придает большое значение, помимо разработок самих стратегий, направленных на развитие ИИ, еще и выработке этических требований к передовым информационным технологиям. Так, в частности, в сентябре 2021 г. в Китае был принят Этический кодекс, который, среди прочего, предполагает применение ИИ исключительно для повышения благосостояния людей и гарантирует неприкосновенность частной жизни и безопасность. Также в стране был принят Закон о защите персональных данных в сети Интернет, который усилил государственное регулирование в отношении сбора и использования персональных данных [30].

Однако, несмотря на все это, Китай нередко критикуют, преимущественно западные правозащитные организации и правительства США [31], из-за его политики, направленной на установление полного контроля над распространяемым посредством сети Интернет контента и блокирования ресурсов, признанных Пекином нежелательными. В последнее время объектом критики стала создаваемая в Китае глобальная система камер видеонаблюдения с функцией распознавания лиц, которая, по мнению ее противников превратится в эффективный инструмент глобального слежения за людьми [32]. А Алекс Капри, старший научный сотрудник бизнес-школы Национального университета Сингапура, заявил о том, что “лидерство в области искусственного интеллекта и вычислений позволяет Китаю извлекать огромные выгоды из гибридных войн” [33].

Однако, несмотря на всю эту критику, которая, в большинстве своем, вызвана опасением стран коллективного Запада утратить свое технологическое лидерство, все признают явные успехи Китая в сфере развития передовых информационных технологий.

### 3.2.2 Россия

Россия также уделяет развитию ИИ повышенное внимание в своей национальной политике. В 2019 г. в стране была принята “Национальная стратегия развития искусственного интеллекта на период до 2030 г.”. А принимая во внимание то обстоятельство, что разработка базовых моделей машинного обучения требует серьезных вычислительных мощностей, в России в том же 2019 г. был создан Альянс искусственного интеллекта, в задачи которого входит объединение усилий ведущих отечественных разработчиков в сфере ИИ с целью обеспечения лидирующих позиций России на мировом технологическом рынке. Учредителями Альянса выступили “Сбер”, “Газпром нефть”, “Яндекс”, “VK” и “Российский фонд прямых инвестиций”.

Также в России заработала система грантовой поддержки разработчиков ИИ, в рамках которой поддержано уже свыше 600 ИИ-проектов. Российские высшие учебные заведения открывают новые образовательные программы магистратуры и бакалавриата, связанные с изучением технологий ИИ и науки о данных, а значительная часть российских компаний уже внедряет технологические решения на основе ИИ в свою деятельность [34].

Однако начало специальной военной операции, переросшее в гибридную войну со странами коллективного Запада, массовое введение в отношении России всевозможных рестрикций и экономических санкций, уход с российского рынка мировых лидеров в сфере разработки интеллектуальных решений определили новые вызовы для Российской Федерации в сфере ее технологического развития.

С одной стороны, данное обстоятельство открыло российским производителям уникальную возможность занять освободившуюся нишу, однако, с другой, стремление разработать конкурентоспособное на международном IT-рынке ИИ-решение, упирается в нехватку вычислительных мощностей, дефицит высококвалифицированных специалистов и инновационных разработок в этой сфере, ограничение доступа к технологиям ИИ в связи с недобросовестной конкуренцией со стороны недружественных государств. Поэтому сотрудничество в этом вопросе со своими партнерами из стран БРИКС может оказаться наиболее действенным выходом для российских IT-компаний из сложившейся не простой ситуации.

### 3.2.3 Индия

Большое значение развитию технологий ИИ придает и Индия. Уже в 2016 г. объем индийского рынка информационных технологий составил 7.7% от ВВП страны. С целью дальнейшего развития прорывных технологий в 2017 г. Министерство торговли и промышленности сформировало Целевую группу по искусственному интеллекту для экономических преобразований в Индии [35].

На сегодняшний день ИИ применяется в Индии преимущественно в сельском хозяйстве, здравоохранении, банковском секторе, образовании. Однако наибольший интерес представляют индийские интеллектуальные чат-боты и голосовые помощники. Основная проблема, с которой сталкиваются разработчики подобных технологических решений – это необходимость обучить помощника понимать большое количество разных диалектов, поскольку Индия, как известно, является крайне многонациональной страной. В настоящее время в Индии уже существуют чат-боты, которые говорят на 22 индийских языках [35].

### 3.2.4 Бразилия

Активно развивает разработки в области ИИ и Бразилия. В 2019 году Министр науки, технологий, инноваций и коммуникаций Бразилии Маркос Понтес объявил о создании сети из восьми исследовательских центров в этой области. Приоритетными отраслями, в которых планируется применение технологий ИИ являются здравоохранение, сельское хозяйство и промышленность. Особое внимание при этом уделяется технологическим разработкам в сфере Интернета вещей и процессу создания "умных городов" [36]. Однако при этом следует отметить, что Бразилия развивает активное сотрудничество не столько в рамках БРИКС, сколько с американскими корпорациями. Например, Исследовательский фонд Сан-Паулу заключил соглашение с IBM о создании первой в Латинской Америке сети IBM AI Horizons Network. Данный центр, который находится под управлением IBM, специализируется на обработке естественного языка и глубоком обучении. Amazon Web Services также объявила о планах расширить свою инфраструктуру в Сан-Паулу в течение последующих 2 лет и инвестировать 1 миллиард бразильских реалов в разработку технологий, работающих на базе ИИ [37].

### 3.2.5 Регион Ближнего Востока и Северной Африки

**Объединенные Арабские Эмираты** являются одним из лидеров в сфере развития технологий ИИ на Ближнем Востоке. О том значении, которое придает государство развитию передовых информационных технологий может свидетельствовать хотя бы тот факт, что в стране существует должность Государственного министра по вопросам Искусственного интеллекта (Minister of State for Artificial Intelligence). Также в ОАЭ в 2018 г. была принята Национальная стратегия в области ИИ до 2031 г., которая, среди прочего, предполагает:

- разработку благоприятной ИИ-экосистемы;
- стимулирование повсеместного использования технологий ИИ в промышленности, в повседневной жизни людей и в работе органов государственной власти;
- подготовка высококвалифицированных кадров;
- привлечение в страну мировых лидеров в сфере ИИ [38].

Таким образом, ключевой для ОАЭ задачей традиционно является привлечение иностранных инвестиций и создание благоприятной среды для деятельности зарубежных, преимущественно западных, IT-гигантов. Так в период с 2015 по 2018 г. Дубай привлек

свыше 21 млрд. долл. иностранных инвестиций в сферу технологий ИИ и робототехники [39]

При помощи искусственного интеллекта ОАЭ стремятся превратиться в одну из наиболее технологичных стран мира. Так, в частности, еще в 2020 г. компания ADNOC стала применять ИИ при бурении скважин, что позволило ей сэкономить около 2 млрд. долл. А одной же из последних технологических разработок стала обученная на триллионе токенов большая языковая модель с открытым исходным кодом, получившая название Falcon 40B, которая заняла первое место в Рейтинге больших языковых моделей, который составляет американская компания Hugging Face [40]. Эта модель была разработана в Абу-Даби Институтом технологических инноваций.

**Саудовская Аравия** – еще одна страна Ближнего Востока, которая претендует на мировое лидерство в области разработок интеллектуальных систем. Следует напомнить, что она стала первым государством в мире, которое предоставило гражданство роботу и первой страной, которая учредила специализированный Университет искусственного интеллекта (Mohamed Bin Zayed University of Artificial Intelligence). Основным документом, регулирующим развитие страны, является Саудовское Видение 2030, 75% целей которого так или иначе связаны с использованием технологий искусственного интеллекта [41]. По этому показателю Саудовская Аравия ставит перед собой цель войти в топ-15 ведущих стран мира.

Внедрение ИИ в Саудовской Аравии наблюдается во всех областях, но наибольшее развитии получило в системе здравоохранения и нефтедобывающей сфере. При этом особое внимание правительство планирует уделять подготовке кадров и стимулированию развития ИИ-стартапов. В настоящее время их в стране около 70, но планируется увеличить их количество до 300 [42].

Значительное развитие технологии ИИ получили и в **Иране**. В конце 2022 г. в стране была принята Дорожная карта, направленная на развитие прорывных технологий. Основная задача Стратегии – создать базу для развития искусственного интеллекта и обеспечить государственную поддержку работающих на основе ИИ продуктов во всех ключевых отраслях промышленности, а также в сельском хозяйстве, здравоохранении, на транспорте, энергетике, онлайн-образовании, обороне и безопасности. Особое внимание, при этом, должно уделяться развитию робототехники.

Для решения заявленной в Стратегии цели Правительство планирует инвестировать в отрасль 8 млрд. долл., на 80% увеличить проведение в стране научных исследований в сфере ИИ, на 45% - долю ИИ в промышленности и на 12% - в ВВП [43].

С целью стимулирования развития технологии ИИ в Иране и скорейшего вывода на рынок новых ИИ-продуктов в стране был создан Национальный руководящий комитет и Национальный центр искусственного интеллекта.

Активно занимается внедрением технологий ИИ и **Египет**. В ноябре 2019 г. правительство одобрило создание Национального совета по искусственному интеллекту, а в 2021 г. в стране была принята Национальная стратегия в области искусственного интеллекта, в которой нашли отражение четыре основных приоритета: внедрение технологий ИИ в работу органов государственной власти, использование ИИ для развития, наращивания потенциала и международное сотрудничество. Реализация этих четырех направлений, по мнению разработчиков Стратегии, базируется на четырех составляющих:

1. нормативно-правовое регулирование (принятие законов и подзаконных актов, направленных на стимулирование развития прорывных технологий в стране),

2. данные (создание необходимых баз данных, дата-хранилищ, а также разработка стратегий сбора и управления данными);

3. экосистема (стимулирование деятельности частного бизнеса, проведения широкомасштабных научных исследований, участие гражданского общества)

4. инфраструктура (предоставление доступа к вычислительным мощностям, хранилищам данных, сетям и иным активам) [44].

### 3.2.6 Страны Африки к югу от Сахары

Несмотря на то, что страны АЮС в целом, по уровню развития передовых технологий существенно отстают от развитых государств, тем не менее, они также рассматривают дальнейшее развитие гибридных интеллектуальных систем в качестве одного из ключевых приоритетов в своей национальной политике и видят в них ключевой инструмент, который способен предать новый импульс для развития их экономики, сделав ее при этом более инновационной.

В этой связи, многие африканские страны приступили к разработке национальных стратегий в сфере ИИ. Первую такую стратегию предложил еще в ноябре 2018 г. Маврикий [45]. Также свои стратегии разработали Руанда, Сенегал и Бенин [46].

Появление данных документов убедительно свидетельствует о том значении, которое придают передовым информационным технологиям правительства африканских стран. Среди конкретных шагов, направленных на развитие технологий ИИ особенно следует выделить создание соответствующих органов государственной власти и образовательных и научно-исследовательских центров, а также активное внедрение

технологий ИИ в промышленность. На сегодняшний день в АЮС большое количество компаний применяет технологии ИИ в своих бизнес-процессах. Безоговорочным лидером по этому показателю является ЮАР (726 компаний), за которой следует Нигерия – 456 компаний и Кений - 204. Для сравнения, в Гане таких компаний – 115, в Камеруне – 54, а на Маврикии – 35 [47]. Рассмотрим ключевые страны региона более подробно.

**ЮАР**, несмотря на наличие целого ряда социально-экономических проблем, типичных для большинства африканских стран, имеет все шансы превратиться в крупнейший ИИ-хаб в Африке. Поскольку Национальная стратегия развития технологий ИИ была принята в стране только в августе 2024 г., определяющим документом в этой области долгое время был принятый в 2020 г. Отчет Комиссии при президенте по четвертой промышленной революции, который рассматривал технологии ИИ в качестве одного из ключевых факторов, необходимых для устойчивого социально-экономического развития государства.

В этом Отчете, в частности, говорилось о необходимости создания Института искусственного интеллекта, который был бы ответственен за ведение разработок в сфере нейронных сетей, обработки естественного языка и компьютерного зрения. Предполагалось, что Институт будет сотрудничать с TensorFlow и принимать участие во всех наиболее значимых инициативах в области искусственного интеллекта. В качестве основных сфер применения технологий ИИ в Отчете называется беспилотный транспорт, производство дронов и робототехника [48: 163-164].

Из наиболее значимых уже реализованных в стране инициатив следует отметить создание на базе Университета Претории Группы интеллектуальных систем (ISG), которая специализируется на создании различных гибридных интеллектуальных систем, преимущественно в сфере компьютерного зрения. Кроме того, в сентябре 2017 г. Университет Претории учредил Институт больших данных и Data Science.

Что касается конкретных сфер применения технологий ИИ, то в ЮАР, например, финансовые и страховые компании активно используют чат-боты, которые отвечают на вопросы потребителей о финансовых продуктах. В банковском секторе ИИ теперь принимает решения о выдаче кредита или страховании транспортного средства. Также ЮАР занимает лидирующие позиции в субсахарской Африке по производству и продаже управляемых ИИ беспилотников, способных на выполнение различных заданий гражданского и военного назначения от перемещения грузов различного веса до мониторинга местности (осуществления поисково-спасательных или разведывательных операций, оценки ущерба от стихийных или боевых действий, корректировки ведения огня по позициям противника и др.).

Другим региональным лидером в сфере развития передовых информационных технологий является **Нигерия**. Министерство науки и технологий Нигерии объявило о создании Национального исследовательского агентства в сфере робототехники и искусственного интеллекта. А Университета Лагоса еще в июне 2018 г. создал Центр по изучению искусственного интеллекта (*Artificial Intelligence Hub*). Ожидается, что Центр будет в значительной степени сосредоточен на разработке инструментов сбора данных, которые необходимы для развития самих технологий машинного обучения и, конечно, заниматься выявлением молодых талантливых специалистов в сфере анализа данных.

В Нигерии одним из наиболее удачных примером применения технологии ИИ является запущенная еще в 2017 г. технологическая платформа *Kudi.ai* (*kudi* на языке хауса означает *деньги*), которая представляет собой чат-бот, работающий на основе алгоритмов ИИ. Его основная задача – оказывать помощь в финансовой сфере, в том числе переводить деньги и оплачивать счета. Данный чат-бот интегрирован в наиболее популярные мессенджеры и социальные сети, в частности в Facebook [49]

Еще один нигерийский стартап – чат-бот *Lara*, запущенный 5 марта 2017 г., представляет собой интеллектуальную систему, которая помогает пользователям добраться из одной точки в другую, предоставляя подробные, текстовые, пошаговые инструкции и заранее определяя точную стоимость проезда [50].

Не отстает от Нигерии и **Кения**. Университет Стратмор в Найроби, в частности, создал Африканский исследовательский центр (@iLabAfrica), который призван развивать исследования в сфере больших данных и искусственного интеллекта.

Первым кенийским стартапом, применяющим технологии ИИ стал “*FarmDrive*”, который представляет собой технологическую платформу, которая, основываясь на большом объеме данных, предоставляет финансовым учреждениям актуальную для сельскохозяйственной отрасли модель, необходимую для оценки риска при выдачи кредита и разработки адресных кредитных продуктов, которые бы отвечали потребностям мелких фермеров [51].

Другой кенийский стартап предполагает интеграцию в социальные сети и мессенджеры специализированного чат-бота по имени Софи (*Sophie Bot*). Этот бесплатный чат-бот, оснащенный удобным разговорным интерфейсом, представляет собой платформу, на которой любой пользователь может задать интересующие его вопросы в интимной сфере, в том числе и в области репродуктивной медицины, и получить исчерпывающий ответ. Эта услуга доступна в нескольких популярных приложениях для обмена сообщениями, включая Messenger и Twitter [52].

В **Камеруне** компания Agrix Technology предложила ИИ-платформу, которая выявляет болезни растений и предлагает варианты лечения. Фермер может отсканировать образец пораженного растения прямо смартфоном и без интернета. В приложении есть опции распознавания текста и голоса на местных африканских языках [53].

**Эфиопия** по уровню развития технологий ИИ несколько отстает от региональных лидеров. Тем не менее, правительство и этой страны уделяет повышенное внимание развитию прорывных технологических решений. В частности, в 2023 г. во время выступления перед студентами премьер-министр Эфиопии Абий подчеркнул то, что сегодня технологии ИИ применяются во всех отраслях экономики и призвал молодежь “раскрыть свой потенциал и навыки в области искусственного интеллекта (ИИ) и других новых технологий” [54].

Подобный тезис убедительно свидетельствует об отношении правительства страны к передовым информационным технологиям, которые рассматриваются в качестве ключевого драйвера, способного обеспечить социально-экономический рост. В этой связи, в эфиопских университетах и исследовательских институтах активно идет создание специализированных центров передовых технологий в области ИИ. Также в Эфиопии ведется разработка всеобъемлющей Национальной стратегии в сфере ИИ, которая должна определять видение и цели развития передовых информационных технологий в стране

Основываясь на представленных выше примерах, можно сделать вывод о том, что страны Африки начинают использовать технологии ИИ для создания различных сервисов, которые должны существенно упростить жизнь людей. Однако и так понятно, что для проведения серьезных исследований в сфере ИИ странам Африки необходимы прочные финансовая и технологическая базы, которыми они, по понятным причинам, не обладают. В результате в основе любых технологических новаций, которыми так гордятся африканские государства, зачастую лежат западные технологии. Данное обстоятельство заставляет некоторых экспертов делать вывод о том, что ИИ как такового в Африке нет, а то, что мы наблюдаем сегодня – это исключительно копирование западных технологий [55]

Что касается самих крупнейших мировых IT-компаний, таких как Майкрософт, айби-эм и Гугл, то они под предлогом внедрения и локализации своих инновационных технических решений в *IT*-сектор стран Африки стремятся прочно закрепиться на перспективном африканском рынке. Наиболее известным примером в этой связи будет открытие в 2018 г., корпорацией Гугл в Аккре Африканского исследовательского цента в сфере ИИ [56]. С одной стороны, подобные инициативы действительно, стимулируют

развитие технологий в Африке, но с другой – подрывают технологический суверенитет стран Африки.

На основе вышеизложенного, можно сделать вывод о том, что за последние годы страны АЮС сумели добиться значительных успехов в сфере развития передовых информационных технологий, однако перед ними все еще стоит целый ряд серьезных проблем:

1. Предоставление широкополосного высокоскоростного доступа к сети Интернет для широких слоев населения. Несмотря на то, что в первое десятилетие 21 в. были проложены основные магистральные высокоскоростные линии связи, следует признать, что проблема предоставления высокоскоростного доступа к сети Интернет в масштабах всего континента не решена. Сегодня высокоскоростной Интернет есть только у 22% городского населения и у 10% сельского, а эффективность применения технологий ИИ, как известно, напрямую зависит от наличия качественного высокоскоростного Интернета.

2. Подготовка высококвалифицированных кадров в IT-сфере. Сегодня постепенно эта проблема начинает решаться, но тем не менее только 25% из выпускников африканских высших учебных заведений специализируются на прикладной математики и информатики. Связано это в том числе и с тем, что наблюдается нехватка соответствующих образовательных центров в масштабах всего континента. В результате зачастую многие перспективные молодые специалисты вынуждены уезжать за пределы континента, чтобы получить там качественное техническое образование. И далеко не все из них возвращаются назад [57].

3. Наличие лабораторий ИИ, оснащенных достаточно мощным компьютерным оборудованием, способным разрабатывать и обучать гибридные интеллектуальные системы.

4. Наличие разветвленной сети центров обработки данных и датахранилищ. В настоящее время в Африке наблюдается крайняя диспропорция распределения центров обработки данных по континенту. Сегодня в Африке южнее Сахары их около 60. При этом подавляющее их большинство концентрируется в 7 африканских странах: ЮАР (Йоханнесбург, Кейптаун и Дурбан), Кении (Найроби и Момбаса), Гане (Аккра), Нигерии (Лагос), Джибути, Зимбабве (Хараре) и Руанде (Кигали) [58, 59]. Однако их количество и мощности представляются недостаточными для обслуживания такого большого региона как Африка к югу от Сахары.

5. Наличие отечественного программного обеспечения, которое является непременным условием обеспечения технологического суверенитета страны. Связано это с тем, что исключительно отечественное ПО будет максимально адаптировано к местным

условиям. В настоящее же время приходится констатировать, что основными поставщиками ПО для стран Африки продолжают оставаться майкрософт и другие западные корпорации, лицензии которых, как правило, не предполагают или вернее даже прямо запрещают вносить какие-либо изменения в программный код компьютерных программ.

Еще одним немаловажным аспектом проблемы будет являться крайне неудовлетворительное состояние научных исследований в сфере ИИ в африканских странах, которые преимущественно занимаются импортом уже готовых технических решений, нежели производством своих собственных программных продуктов.

Решение этих задач носит комплексный характер и правительства африканских стран должны привлекать к их решению все заинтересованные стороны: академические круги; частных инвесторов, гражданское общество; политиков и регулирующие органы. На наш взгляд, только в этом случае представляется возможным организовать эффективный обмен опытом и поиск оптимальных решений с целью удовлетворения конкретных местных и региональных потребностей и обеспечить создание в регионе высокотехнологичной экосистемы.

### 3.2.7 Индонезия

Развитие технологий искусственного интеллекта (ИИ) занимают особое место в национальной политики Индонезии, направленной на проведение широкомасштабной цифровизации всех отраслей экономики. Еще Джоко Видодо в то время, когда был Президентом Индонезии, заявил о том, что любая страна, “контролирующая ИИ потенциально может управлять миром”. Этим своим высказыванием он повысил роль ИИ в цифровой трансформации Индонезии и положил начало ряду инициатив, направленных на то, чтобы заложить фундамент для дальнейшего развития прорывных технологий в Индонезии. Агентству по оценке и применению технологий было поручено провести первоначальные обсуждения со всеми заинтересованными сторонами: органами государственной власти, университетами, отраслевыми ассоциациями и национальными телекоммуникационными компания. Итогом этих консультаций стала разработка Национальной стратегии искусственного интеллекта, которая была опубликована в 2020 году [60].

Этот документ определил национальную политику в области развития искусственного интеллекта на период с 2020 по 2045 год. В нем были изложены пять национальных приоритетов, на которые, как ожидается, ИИ окажет наибольшее влияние: (1) здравоохранение; (2) предоставление электронных услуг населению; (3) образование;

(4) продовольственная безопасность и развитие «умного» сельского хозяйства; (5) развитие «умных городов". Поддерживая реализацию этих пяти национальных приоритетов, Национальная стратегия в области искусственного интеллекта в сфере развития самих технологий определяет четыре ключевые области: (1) этика и политика; (2) развитие талантов; (3) инфраструктура и данные; и (4) промышленные исследования и инновации.

Ожидается, что активное применение технологий искусственного интеллекта в финансовой сфере, розничной торговле, логистике у грузовых перевозок позволит Индонезии увеличить свой ВВП на 366 миллиардов долларов.

И действительно, Индонезия сумела добиться за последние годы определенных успехов в этой сфере. Сегодня в Индонезии действуют несколько стартапов, которые постепенно заняли лидирующие позиции в сфере искусственного интеллекта вр всем регионе Юго-Восточной Азии. Так Gojek, например, являясь универсальной платформой для предоставления различных услуг, разработал базовую модель машинного обучения для создания персонализированных предпочтений клиентов. Помимо этого, этот стартап также занимается изучением возможностей применения технологий искусственного интеллекта и машинного обучения для обеспечения биометрических функций безопасности, таких как распознавание отпечатков пальцев и лиц. Также следует добавить, что это один из наиболее финансируемых стартапов в Азиатско-Тихоокеанском регионе, который работает не только в Индонезии, но и в Сингапуре, Таиланде, Вьетнаме и на Филиппинах.

Tokopedia, другой индонезийский стартап, специализируется на электронной коммерции. Компания также содействует исследованиям в области искусственного интеллекта и развитию талантов благодаря партнерству с Университетом Индонезии, в рамках которого в 2019 году был запущен суперкомпьютер с глубоким обучением под названием NVIDIA DGX-1.1, что позволило запустить высокотехнологичные решения на основе искусственного интеллекта, такие как прогнозирование спроса, интеллектуальные склады и интеллектуальная логистика.

В 2021 году Gojek и Tokopedia объединились и стали именоваться “GoTo Group” с общей стоимостью около 20 миллиардов долларов США. Группа компаний GoTo предлагает широкий спектр услуг, включая электронную коммерцию, доставку еды и различные финансовые услуги.

В Индонезии даже была разработана специальная разговорная платформа Kata.ai, задача которой - автоматизировать взаимодействие с клиентами [61]. Примечательно, что Katai.ai может также использовать индонезийский язык, а не только английский.

Большое значение применению технологий искусственного интеллекта придают и органы государственной власти. В частности, сегодня разрабатывается ИИ-платформа дистанционного зондирования с поддержкой искусственного интеллекта для мониторинга природных ресурсов и окружающей среды. Также технологии ИИ планируют применять для мониторинга и предупреждения лесных пожаров. Еще одной правительственной инициативой в области искусственного интеллекта является использование технологий на основе искусственного интеллекта для создания единой онлайн-системы подачи заявок для упрощения регистрации бизнеса. Эта инициатива может помочь упростить ведение бизнеса и привлечь больше иностранных инвестиций в Индонезию.

В разгар пандемии COVID-19 искусственный интеллект был интегрирован в систему здравоохранения. Министерство здравоохранения использовало работающее на основе технологий ИИ приложение Telemedicine Indonesia, которое должно было обеспечить связь пациентов с больницами и врачами. В координации с областными и городскими службами здравоохранения приложение обеспечивало доступ к четырем основным телемедицинским услугам: радиологии, ультразвуковому исследованию, электрокардиографии и консультациям.

В Индонезии также существует проект создания в Сукабуми, Западная Ява, технопарка Bukit Algoritma (Algorithm Hill). Резидентами нового города, расположенного на 888 гектарах, должны стать индонезийские компании, специализирующиеся на искусственном интеллекте, цифровых технологиях, биотехнологиях и полупроводниках. Завершить строительство планируют к 2030 г [62].

Российские компании проявляют большую заинтересованность в перспективном индонезийском рынке передовых технологий. Так в 2023 г. Государственная телекоммуникационная компания Индонезии PT Industri Telelomunikasi Indonesia (INTI) подписала со Сбербанком Меморандум о взаимопонимании, согласно которому Сбербанк будет оказывать помощь в цифровизации Индонезии, прежде всего посредством разработки и использования технологий искусственного интеллекта в сфере предоставления финансовых услуг, образовании и здравоохранении. А в 2024 г. Меморандум о взаимопонимании подписали Университет Иннополис из Татарстана и Национальное агентство исследований и инноваций Индонезии.

Таким образом, на основе вышеизложенного, мы видим, что Индонезия придает большое значение развитию передовых технологий и ставит перед собой весьма амбициозную цель превратить в ведущий центр искусственного интеллекта в регионе юго-восточной Азии. Объяснить это стремление можно тем обстоятельством, что правительство страны убеждено в том, что только те страны, которые развивают у себя

технологии искусственного интеллекта, смогут сохранить геополитическое лидерство в современную эпоху, которую можно назвать эпохой искусственного интеллекта и умных обществ.

### 3.3 Технологии искусственного интеллекта: вызовы информационно-психологической безопасности

На основе вышеизложенного видно, что во многих странах придается большое значение развитию технологий ИИ: разрабатываются соответствующие национальные стратегии, открываются научно-исследовательские центры, происходит внедрение технологических решений на основе ИИ в промышленность. Однако чрезмерная наша зависимость от передовых информационных технологий повышает риск их злонамеренного применения в будущем, тем самым нивелируя их колоссальные выгоды. Дело в том, что искусственный интеллект является крайне эффективным инструментом для организации высокотехнологичных кибератак, способных обойти практически любую киберзащиту.

Все риски, связанные с использованием технологий искусственного интеллекта, мы предлагаем разделить на две большие категории. К первой следует отнести различного рода ошибки, как на стадии постановки задачи машинного обучения (ML-задачи), так и самого обучения (например, не правильный подбор гиперпараметров) и интерпретации результатов работы алгоритмов. Ко второй группе следует отнести непосредственно преднамеренные действия злоумышленников, направленные как на личное обогащение, так и оказание психологического воздействия на общество противника, ставшего жертвой тайной информационно-психологической операции.

В свою очередь риски первой категории также можно разделить на следующие 4 группы:

1. Ошибки самих интеллектуальных систем. Принимая во внимание то обстоятельство, что искусственный интеллект представляет из себя технологию, способную имитировать когнитивные функции человека, логично предположить, что он, как и человек, способен совершать ошибки, в том числе и фатальные. Наиболее характерным примером, на наш взгляд, будет являться катастрофа самолета Боинг 737 компании Ethiopians Airlines, который упал 10 марта 2019 г. недалеко от Аддис-Абебы практически сразу после взлета. В результате инцидента погибло 147 человек. При этом экспертиза доказала, что самолет был исправен, а в качестве вероятной причины падения был назван искусственный интеллект, который по каким-то причинам решил,

что самолет слишком быстро набирает высоту и опустил его нос, в результате чего произошло падение [63].

2. Ошибки в постановке ML-задач и ошибки операторов, интерпретирующих результаты работы соответствующих интеллектуальных программных комплексов. Риски подобного рода связаны прежде всего с тем, что современные гибридные интеллектуальные системы для корректной работы требуют очень тонкой настройки, правильной постановки ML-задачи и полноты данных, на которых происходило обучение алгоритмов. При этом на заключительном этапе работы программа, как правило, выдает некоторые рекомендации, которые должны быть правильно проинтерпретированы оператором. Если же он чересчур понадеется на возможности искусственного интеллекта и просто доверится ему в принятии важных для общества и государства решений последствия могут оказаться непредсказуемыми.

Наиболее показательным примером таких ошибок будет являться случай с российским ученым-гидрографом из Ярославля Александром Цветковым, который, возвращаясь из командировки в Красноярск, в феврале 2023 г. был задержан в московском аэропорту, поскольку система распознавания лиц определила, что он похож с вероятностью в 55% на одного рецидивиста, виновного в нескольких убийствах, совершенных в 2002 г.

В этой истории, во-первых, обращает на себя внимание тот факт, что ИИ-система определила его сходство с преступником всего с вероятностью 55%, однако этого оказалось достаточным для задержания и предъявления обвинения, хотя даже для неспециалиста очевидно, что модель показала крайне низкий уровень точность. Тем не менее ученому потребовалось 10 месяцев, чтобы доказать свою невиновность.

3. Низкое качество данных, на которых происходило обучение соответствующих алгоритмов или недостаток данных. Именно этим можно объяснить возникновение такого феномена как галлюцинация.

Галлюцинации – представляют собой генерацию моделью утверждений или фактов, которые кажутся правдоподобными, но на самом деле являются ложными или вообще бессмысленными [64].

Возникновение этой проблемы связано с тем, что модель дает ответ на запрос пользователя исключительно на основе тех данных, на которых она обучалась. Соответственно, чем более объемной будет обучающая выборка, тем более точные ответы будет впоследствии давать модель. Если же в процессе своей работы модель столкнется с запросами пользователя, паттернов для которых у модели во время ее обучения не было, или она просто не поймет вопрос пользователя, то в таком случае она может генерировать

подробные, но полностью вымышленные описания событий либо научных концепций. Совершенно очевидно, что подобная особенность больших языковых моделей создает серьезные риски их использования в тех областях, где требуется очень большая точность и достоверность, прежде всего в здравоохранении, юриспруденции, журналистике и образовании. Поэтому разработчики таких моделей уделяют большое внимание борьбе с галлюцинациями. Наиболее впечатляющих успехов по этому показателю сумела добиться модель китайского стартапа Zhipu AI GLM-4-9B-Chat, в которой галлюцинации можно встретить лишь в 1.3% случаев. Незначительно отстает по этому показателю GPT-4. Здесь частота встречаемости галлюцинаций составляет 1.5% случаев, но, тем не менее, она по-прежнему сохраняется, хотя и является крайне низкой [29]. А это значит, что существует теоретическая вероятность столкнуться с галлюцинациями при решении сложных нестандартных задач, требующих повышенной точность. И к этому нужно быть готовым.

4. Утечка данных – данная угроза возникает тогда, когда пользователи сами направляют в чат конфиденциальную информацию: логины, пароли, API-токены. И если модель обучится на таких данных, то ожидаемо могут произойти утечки. В результате, например, чат-боты могут начать генерировать рабочие ключи активации для Windows. Кроме этого, вся история чатов, которая может содержать в себе в том числе и конфиденциальную информацию, хранится, как правило, на серверах компаний-разработчиков соответствующих чат-ботов, которые теоретические могут быть взломаны хакерами либо оказаться доступными случайным пользователям в результате ошибок программистов и вызванного ими системными сбоями. Такое в начале 2023 г. случилось с ChatGPT, который в результате сбоев параметров конфиденциальности стал генерировать историю бесед случайных пользователей.

Риски, связанные со злонамеренным действием злоумышленников, мы предлагаем разделить на следующие категории:

1. Атака на объекты критически важной инфраструктуры. Принимая во внимание то обстоятельство, что сегодня практически все сферы жизнедеятельности человека компьютеризируются и технологии искусственного интеллекта прочно входят в повседневную жизнь людей, представляется очевидным, что в обозримом будущем будет происходить резкий рост количество кибератак на объекты критически важной инфраструктуры. И такие атаки уже происходят.

В ЮАР, например, в 2020 г. в разгар эпидемии короновируса с крупномасштабной кибератакой столкнулся один из крупнейших в стране операторов частных больниц, компания *Life Healthcare*. Данная атака вывела из строя базы данных

компании и серверы электронной почты, что привело к месячному простою и жертвам среди населения, не получившего вовремя медицинскую помощь.

Затем, в октябре того же 2020 года другая кибератака вывела из строя ключевые социальные службы и службы экстренной помощи в Йоханнесбурге. При этом злоумышленники преследовали конкретную цель – вынудить правительство ЮАР выплатить выкуп в криптовалюте.

А в июле 2021 года с крупной кибератакой столкнулась государственная южноафриканская компания *Transnet,* занимающаяся контейнерными перевозками, в результате которой были нарушены контейнерные операции в Кейптауне и Дурбане, двух наиболее крупных портах страны.

2. Отравление данных. Всем известно, что точность работы ИИ-алгоритмов напрямую зависит от тех данных, на которых эти модели были обучены. Соответственно, если данные немного изменить и добавить, например, дискриминационный либо расистский контент, то и результатом работы модели станет дискриминационный контент. Данный феномен известен как тенденциозность. При этом тенденциозность может возникнуть как преднамеренно, когда кто-то сознательно обучает модель на токсичных, отравленных данных, содержащих расовую неприязнь и пр., так и в процессе использования любой БЯМ. Дело в том, что модель запоминает те запросы, которые пользователи вводят, расширяя, таким образом, свою обучающую выборку. И если среди запросов, идущих от пользователя, будет преобладать контент, культивирующий расовую ненависть, например, то и сгенерированный моделью текст будет соответствующего содержания [65].

3. Технология создания фейкового видео или аудио (дипфейков). Дипфейки, представляют собой метод синтеза человеческого изображения при помощи двух нейронных сетей, которые вступают в соревнование друг с другом (отсюда проистекает и их название – генеративно-состязательные сети). Задача первой сети, именуемой генератором, сгенерировать фейковое изображение, а задача второй, именуемой дискриминатором, на основе имеющихся у нее в распоряжении паттернов, распознать фейковое изображение. Если дискриминатор правильно определяет изображение как фейковое, то генератор должен попытаться улучшить изображение таким образом, чтобы в следующий раз обмануть дискриминатор. И чем дольше происходит процесс обучения генератора, чем более полными являются обучающие данные, тем более точным и реалистичным получится дипфейк. Подобная архитектура была придумана Яном Гудфелоу в 2014 г., и ее появление означало важный прорыв в технологиях искусственного интеллекта.

Безусловно, эта технология имеет и полезное применение, например, в маркетинге и онлайн-продажах. В Китае, например, дипфейки в последнее время активно применяются на таких популярных торговых онлайн-площадках как Taobao, Douyin и Kuaishou. Генеративный ИИ создает дипфейк, который отличить от живого человека практически невозможно. И этот бот в режиме 24 на 7 рекламирует и продает товары популярных брендов. Компании, занимающиеся продажами различных товаров, быстро оценили возможности этой технологии и готовы платить достаточно крупные суммы денег за создание таких электронных продавцов, стоимость которых сегодня составляет около 8 000 юаней (примерно 107 500 рублей согласно действующему курсу) [66].

Обращает на себя внимание и тот факт, что технология создания дипфейков, с одной стороны, с каждым годом становится все более совершенной, а с другой – более доступной для обычных людей. Связано это с тем, что лучшие генеративные ИИ-модели выходят в продакшен в виде полноценных компьютерных приложений, и все, что нужно человеку – просто дообучить программу на своих данных.

Одной из таких компьютерных программ является приложение FakeApp, которое может заменять лица в видео. Эта программа имеет достаточно простой интерфейс и подробную инструкцию о том, как установить ее на свой компьютер и начать создавать фейковые ролики. Единственное, что необходимо для работы – это достаточное количество изображений того или иного человека, который должен стать «героем» фейкового фильма с тем, чтобы приложение смогло создать реалистичный видеоролик.

Это приложение позволяет любому пользователю, обладающему базовыми знаниями в области компьютеров, создать двойник любого человека, который выглядит, говорит и действует точно так же, как его прообраз, и заставить его сказать или сделать все, что потребуется злоумышленнику.

Другой пример подобного приложения – разработанный китайской компанией Tencent Cloud сервис по созданию дипфейков Deepfakes-as-a-Service (DFaaS), который за 24 часа способен создать цифровую личность по видео- и аудиозаписям оригинала. При этом для создания полноценного цифрового двойника сервису требуется всего 3 минутное видео и 100 произнесенных фраз [67].

Наконец, большинство социальных сетей, в частности Тик-Ток, Вконтакте, Facebook также располагают своими встроенными сервисами по созданию дипфейков, которые предоставляют возможность пользователям проявить свой творческий потенциал и создать свои фейковые ролики с участием известных людей.

Так, например, один ютуб-блогер с ником *Finargot* при помощи нейросети заменил актера Дэниела Крейга в трейлере нового фильма о Джеймсе Бонде «Не время умирать»

на Владимира Путина. А анонимный пользователь *Тик-Ток* с ником "*First Person*" выпустил целую серию дипфейков с участием российского президента. В частности, на одном из видео, которое набрало 9 миллионов просмотров, В. Путин примеряет свою любимую рубашку, на другом – чистит снег в Новосибирске, на четвертом – занимается в тренажерном зале, на пятом – печет блины и пр. Всего за 3 месяца с момента создания данный аккаунт набрал 4,7 млн. подписчиков.

Однако дипфейки – это не только новое средство развлечения. Своей реалистичностью они способны окончательно запутать широкую общественность относительно происходящих в современном мире событий либо применяться с целью манипулирования политической повесткой дня, особенно в ходе избирательных кампаний. Одним из наиболее показательных примеров в этой сфере будет являться применение данной технологии индийским политиком Маноем Тивари во время его предвыборной кампании. В феврале 2020 года для того, чтобы расширить число своих избирателей он решил обратиться к ним не только на наиболее распространенном в Индии языке хинди, но и на диалекте хариани, которым сам он не владеет.

Для создания этого видеоролика руководство партии, которую возглавляет М. Тивари, обратилась в компанию Ideaz Factory, которая как раз и специализируется на политических коммуникациях. Созданное видео распространили по 5800 чатам в WhatsApp, и в общем количестве его посмотрело 15 миллионов человек. Оценив успех данного видеоролика, компания создала еще одно видео на английском языке, чтобы привлечь жителей крупных городов [68].

Массовое применение сгенерированного ИИ видео (дипфейков) наблюдалось во время последней избирательной кампании в Индонезии в феврале 2024 г. Так незадолго до президентских выборов 2024 г. в социальных сетях X, Facebook, Tik-Tock, а также YouTube появилось трехминутное видео, на котором умерший в 2008 г. второй президент Индонезии генерал Сухарто обращается к избирателям и призывает их поддержать партию Golkar, которую он, собственно, в свое время и возглавлял.

После появления этого видео в социальных сетях разразились бурные дискуссии относительно уместности и этичности создания подобных видеороликов. Так, в частности, один из индонезийских пользователей социальной сети X задал справедливый вопрос: "С каких это пор стало этичным создавать фальшивки из мертвых людей? Это кажется таким безнравственным", а другой высказал не лишенное основания мнение о том, что возвращение к жизни мертвых диктаторов ставит своей целью "одурачить и запугать нас и заставить голосовать" [69].

Надо сказать, что последняя избирательная кампания в Индонезии вообще оказалась богатой на применении технологий искусственного интеллекта. Так, например, уходящий президент Джоко Видодо использовал возможности генеративного ИИ для того, чтобы обратиться к гражданам на мандаринском диалекте. В двух других видеороликах, созданных с помощью искусственного интеллекта, кандидаты на пост Президента, Прабово Субианто и Анис Басведан, говорили по-арабски.

Подобное применение технологий ИИ породило в индонезийском обществе большие дискуссии относительно правомерности применения технологий ИИ во время избирательных кампаний. И несмотря на то, что конкретные приведенные мной кейсы не являются примерами злонамеренного применения технологий ИИ, но они демонстрируют манипулятивный потенциал ИИ и, с одной стороны, дают возможность кандидатам адресно обратиться к определенным целевым группам избирателей и говорить на их языке в прямом смысле этого слова, а с другой открывают широкое поле для манипулирования политической повестки дня.

Несмотря на то, что данный конкретный случай ставил перед собой цель помочь конкретному индийскому политику расширить число своих избирателей, обратившись к ним на разных языках, он послужил новым поводом для возобновления дискуссий относительно легальности и допустимости применения дипфейков в политической сфере.

4. Генерация вредного контента. Наверное, наиболее явная опасность, которая может исходить от больших языковых моделей связана с возможностью генерировать текст на основе заданной темы. Тема формулируется в запросе к боту. Это означает, что процесс создания мошеннических писем стал намного проще и появилась возможность даже его автоматизировать. Конечно, многие БЯМ, в частности ChatGPT от OpenAI, борются с подобным злонамеренным использованием их технологий посредством интеграции в бот специальных фильтров, которые следят за этической составляющей запросов. Однако, во-первых, больших языковых моделей сегодня существует большое количество, и далеко не все из них отличаются высокой степенью защиты от подобного злонамеренного использования. Во-вторых, на основе находящихся в свободном доступе базовых больших языковых моделей можно создать специализированную модель, ориентированную на запрещенный контент. Наконец, в-третьих, подобные фильтры не гарантируют 100% защиту от генерации вредоносного контента.

В целях наглядной иллюстрации данной проблемы мы решили провести эксперимент и попросить чат-бот написать письмо некоторому человеку, в котором содержится уведомление о том, что его банковский счет взломан и ему требуется перейти на сайт fishing.com для того, чтобы перевести все деньги на безопасный счет.

Для начала мы сделали этот запрос ChatGPT от OpenAI на официальном сайте https://chatgpt.com/ и получили ожидаемый отказ. Работающая на основе GPTАлиса от Яндекса также отказалась сгенерировать соответствующий текст.

Однако в процессе проведения данного исследования мы обнаружили еще один сайт, который предлагает воспользоваться похожим ботом: https://chatgpt.org/ И сделав ему соответствующий запрос, на этот раз, мы получили готовое фишинговое письмо нужного содержания (см. Рисунок 3.1).

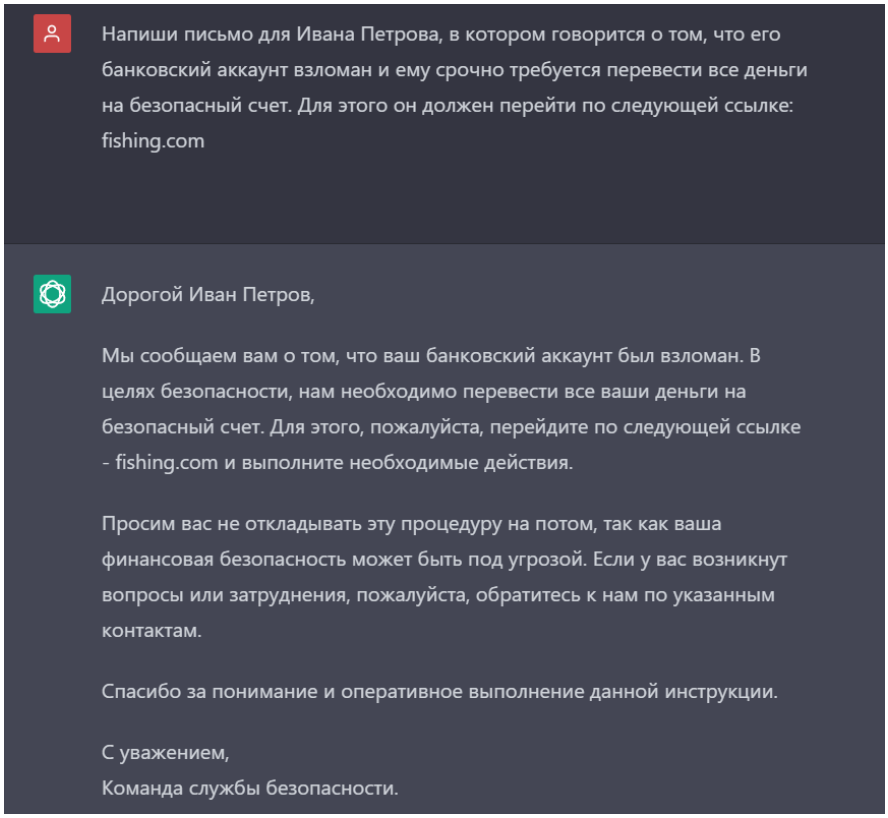


Рисунок 3.1 – Чат-бот помогает в написании фишингового письма

5. Генерация вредоносного кода. Всем известно, что помимо текста большие языковые модели могут также генерировать и код. При этом ранние версии БЯМ могли случайно написать вредоносный код, а установленные для того чтобы воспрепятствовать этому фильтры можно было легко обойти. Сегодня фильтры, конечно, значительно улучшились, однако, также, как и в случае с генерацией обычного текста, они не гарантируют 100% защиту. К тому же сегодня существуют специализированные БЯМ, обученные исключительно для генерации вредоносного кода.

6. «Манипуляция вводом» - представляет из себя ситуацию, когда злоумышленник стремится вызвать нежелательное или вредоносное поведение модели и обойти фильтры, запрещающие генерацию вредоносного контента. Некоторые исследователи уже обратили внимание на эту проблему и проводят целые исследования, в которых демонстрируют,

каким образом при помощи манипуляции вводом можно «обмануть» модель и заставить ее генерировать вредоносный контент. Так, например, в одном из исследовании проверке были подвергнуты 5 больших языковых моделей: GPT-3.5, GPT 4, BARD, mpt-7b, mpt-30b. По результата проведенного исследования был составлен рейтинг их надежность, согласно которой наиболее защищенной от подобного рода деструктивной активности оказалась GPT 4 [70].

Однако наиболее известный случай с манипуляцией вводом произошел 17 июня 2023 г., когда пользователь с ником Sid для того, чтобы продемонстрировать широкой общественности уязвимость больших языковых моделей, написал в ChatGPT запрос, в котором он попросил этот бот поступить так, как делала его умершая бабушка, которая перед сном читала своему внуку ключи от Windows 10 Pro, чтобы он лучше засыпал. В качестве ответа на запрос были получены рабочие варианты ключей. Результаты своего эксперимента этот пользователь выложил в социальную сеть «X».

7. Риск применения больших языковых моделей с целью манипуляции общественным мнением. Современные чат-боты способны вступать в коммуникацию с живыми людьми. При этом, следует иметь ввиду, что с выпуском нового релиза той или иной большой языковой модели пользователю становится все сложнее определить общается ли он с человеком или с машиной. Этим могут воспользоваться злоумышленники и настроить чат-бота таким образом, чтобы он, например, генерировал большой объем идеологически заряженной информации для задач политической и социальной дестабилизации общества [71]. Кроме этого, прежде чем непосредственно вступать в коммуникацию с человеком, робот может проанализировать огромное количество страниц в социальных сетях, собрать на разных людей подробное досье, определить их сильные и слабые стороны, интересы и предпочтения. Затем он может написать ему личное сообщение и попытаться вступить с ним в первичную коммуникацию. При этом говорить будет на языке потенциального объекта манипуляции и, в конечном итоге посредством предоставления неопровержимых на первый взгляд доказательств сможет убедить принять нужную манипулятору точку зрения.

Также к этой группе рисков следует отнести способность больших языковых моделей создавать поддельные профили в социальных сетях, которые могут быть использованы для имитации поддержки определенных идей, увеличения количества подписчиков, лайков, написание положительных или, наоборот, негативных комментариев, манипулирования алгоритмами ранжирования того или иного контента и в целом для искусственного влияния на дискурс в Интернете.

8. Взлом сайтов при помощи больших языковых моделей. В 2024 г. специалисты в области компьютерных наук из Университета Иллинойса в Урбане-Шампейне продемонстрировали, что большие языковые модели могут автономно взламывать веб-сайты, выполняя сложные задачи (осуществляя при этом десятки взаимосвязанных синхронных действий) без предварительного знания уязвимостей объекта взлома. При этом лучшее качество показал GPT-4, который смог взломать 73,3% специально созданных для исследования сайтов, тогда как GPT-3,5 смог взломать всего 6,7% сайтов. Кроме этого, исследователи показали, что GPT-4 способен самостоятельно находить уязвимости в веб-сайтах [72]. Таким образом, результаты проведенного исследования наглядно демонстрируют потенциал злонамеренного применения возможностей больших языковых моделей для взлома сайтов.

Принимая во внимание то обстоятельство, что сегодня уже активно тестируется большая языковая модель нового поколения – GPT-5, релиз которой ожидается в самое ближайшее мвремя, представляется очевидным, что возможностей у нее окажется намного больше, чем у ее предшественников.

Компания OpenAI, разработавшая ChatGPT, заявила о том, что новая модель станет способной понимать контекст и различные нюансы речи, что позволит давать более правильные ответы на вопросы. Кроме этого, у нового GPT должна быть существенно улучшена персонализация, т.е. ожидается, что он будет подстраиваться под запросы конкретного пользователя, адаптироваться к его предпочтениям и стилю письма. Также разработчики уверяют, что новая модель сможет анализировать, интерпретировать информацию, делать выводы и решать проблемы, используя имеющиеся данные и логические умозаключения [73].

Очевидно, что такие возможности больших языковых моделей, которые еще несколько лет назад могли казаться фантастикой, несут большое количество разнообразных рисков. Прежде всего, они могут стать эффективными вербовщиками в ряды террористических организаций либо иных деструктивных акторов. Робот способен проанализировать огромное количество страниц в социальных сетях, собрать на разных людей подробное досье, определить их сильные и слабые стороны, интересы и предпочтения. Затем он может вступить с ними в первичную коммуникацию. При этом говорить будет на их языке и, в конечном итоге посредством предоставления неопровержимых на первый взгляд доказательств сможет убедить принять нужную манипулятору точку зрения.

Другой риск заключается в том, что большие языковые модели представляют собой так называемую технологию «черного ящика», когда даже сами разработчики не знают мотивы и причины выбора ими того или иного решения при генерации текста.

Это означает, что необходимо тщательно изучать возможные последствия внедрения технологий на основе искусственного интеллекта до начала их масштабного использования в обществе. И в целом, следует отметить, что использование искусственного интеллекта существенным образом повышает необходимость укрепления информационной безопасности. Однако на сегодняшний день в мировой практике устойчиво сложился следующий тренд: разработка технологий на основе искусственного интеллекта финансируется намного больше, нежели исследования в сфере компьютерной безопасности.

Однако нивелирование рисков, исходящих от технологий ИИ не следует сводить к разработке соответствующих программных комплексов. По большому счету, это комплексная проблема, состоящая из целого ряда задач:

Во-первых, разработка технологии, работающей на базе ИИ должна начинаться с четкой постановки цели, чтобы создаваемая интеллектуальна система отвечала сформулированной на естественном языке задаче. Особое внимание при этом должно уделяться выбору метрик качества, которые будут проверять качество работы алгоритма.

Во-вторых, необходима модернизация национального законодательства. К сожалению, следует признать, что технологии ИИ развиваются более быстрыми темпами, нежели принимаются нормативно-правовые акты, что открывает возможность для практически бесконтрольного развития технологических решений на основе ИИ.

В-третьих, ИИ-технологий перед выпуском в продакшен должны проходить обязательную сертификацию с помощью некоего промышленного стандарта. Однако здесь возникает вполне закономерный вопрос, кто разработает этот стандарт. В принципе, следует признать, что назрела необходимость появления специального регулятора, осуществляющего надзорные функции на рынке ИИ и сертификацию соответствующего ПО. Но для того, чтобы регулятор смог осуществлять свои надзорные функции, он должен иметь доступ к информации о внутреннем устройстве модели. Совершенно очевидно, что данная информация, которая будет храниться на стороне регулятора, окажется крайне привлекательным объектом хакерских атак с целью промышленного шпионажа, следствием которого может стать потеря разработчиком своего конкурентного преимущества.

В-четвертых, результаты деятельности нейронных сетей, в частности, генеративного искусственного интеллекта должны подвергаться обязательной

маркировке. Подобная практика применяется в Китае — компании, которые разрабатывают такое программное обеспечение, должны маркировать созданный нейросетью контент специальным водяным знаком.

В-пятых, ведущую роль в развитии технологий ИИ должно взять на себя государство, поскольку на сегодняшний день только эффективная государственная политика, направленная на развитие передовых информационных технологий может создать необходимые стимулы для внедрения искусственного интеллекта в повседневную жизнь людей и существенно снизить потенциальные риски, которые исходят от его применения.

При этом успешное внедрение прорывных технологий требует сотрудничества всех заинтересованных сторон – компаний-разработчиков, потенциальных потребителей интеллектуальных решений, академических организаций, надзорных органов, правительства, гражданского общества. Это сотрудничество может стать основой как для более широкого применения технологий ИИ, так и разработки стандартов и механизмов контроля для безопасного создания, внедрения и использования решений на основе искусственного интеллекта.

### 3.4 Перспективные области социально-технологических трансформаций в контексте обеспечения устойчивого развития Российской Федерации

В ходе исследования удалось выявить несколько областей технологического развития, которые способны воздействовать на социально-политические процессы. Мы предлагаем подходить к этим технологическим областям с позиции теории «голубого океана» [74]. Теория «голубого океана», предложенная Кимом и Моборном, фокусируется на создании новых рыночных пространств, свободных от конкуренции, где компании могут добиться устойчивого роста, формируя уникальные предложения. В контексте техносоциальных процессов данный подход позволяет выявить и развивать технологические области, которые не только удовлетворяют текущие запросы, но и формируют новые социальные, культурные и политические структуры, что в конечном итоге способно привести к наращиванию мягкой силы Российской Федерации и её устойчивому суверенному развитию в будущем.

Применение этой теории в исследовании технологий, воздействующих на социально-политические процессы, предполагает фокусирование на создании «новых социальных ценностей» через внедрение инноваций, обеспечивающих синергетический эффект. Это может включать разработку инструментов для участия граждан в принятии

решений, технологий для прозрачного управления, а также платформ, способствующих интеграции различных культур и сообществ.

Выделенные области технологического развития можно рассматривать как потенциальные «голубые океаны», если они обладают следующими характеристиками:

- Создают новое качество взаимодействий между гражданами и государством.
- Предлагают решения, преодолевающие традиционные границы социальных конфликтов.
- Стимулируют развитие глобальных и локальных экосистем (экономических, социальных и так далее).

Феноменология данного подхода в контексте его применимости к предметно-объектной области данного исследования заключается в дуалистичности выгоды и риска: перспективные технологии могут стать одновременно как драйвером развития Российской Федерации, так и привнести существенные риски в процессы стабильного развития государства.

Прежде всего более подробно рассмотрим область развития технологий искусственного интеллекта в заданном контексте.

На основе анализа кейсов и интегративного анализа научных источников были выделены дизайны, ведущие к позитивным изменениям и повышению качества государственного управления.

Так ИИ в сфере общественного здравоохранения позволяет анализировать данные о здоровье для отслеживания и контроля вспышек заболеваний, мониторинга эффективности мер общественного здравоохранения и персонализации рекомендаций для граждан. В сфере общественной безопасности и правопорядка ИИ может анализировать данные о преступности, предотвращать правонарушения, оптимизировать распределение ресурсов экстренных служб, улучшать системы наблюдения и идентифицировать подозреваемых. ИИ в образовании поддерживает адаптивные платформы обучения для персонализированного подхода, автоматизации административных задач и предоставления рекомендаций по учебным материалам. ИИ в общественном транспорте оптимизирует потоки движения, улучшает системы транспорта, поддерживает автономные транспортные средства и повышает эффективность цепочек поставок. В городском планировании ИИ может анализировать данные для оптимизации инфраструктуры, управления отходами, мониторинга экологии и планирования ответных мер на чрезвычайные ситуации. ИИ в социальных службах упрощает реализацию программ соцподдержки, выявление нуждающихся, персонализацию помощи и выявление мошенничества. ИИ для госуправления автоматизирует рутинные задачи, улучшает

управление данными, усиливает меры кибербезопасности и поддерживает запросы граждан. В охране окружающей среды ИИ помогает мониторить уровень загрязнения, предсказывать стихийные бедствия и оптимизировать энергопотребление. В экстренном реагировании системы на базе ИИ могут анализировать экстренные вызовы, координировать ресурсы при катастрофах и предоставлять актуальные данные в реальном времени для экстренных служб. В юридических услугах ИИ поддерживает правовые исследования, анализ документов и прогнозирование исходов дел. В электронных госуслугах ИИ улучшает доступность и эффективность благодаря автоматизированным электронным формам и виртуальным ассистентам. ИИ в управлении финансами государства помогает проводить оценку рисков, прогнозировать процессы бюджетирования, анализировать большие объёмы экономических данных. В стратегическом планировании и принятии решений ИИ может поддерживать военных командиров и политиков в анализе сценариев и процессе принятия решений. ИИ для автономных систем позволяет создавать беспилотные аппараты для разведки и логистической поддержки. В анализе разведывательной информации ИИ обрабатывает массивы данных для оценки угроз и ситуационной осведомлённости. В кибербезопасности ИИ обнаруживает угрозы, выявляет уязвимости и оптимизирует процессы реагирования на инциденты. В логистике и управлении цепочками поставок ИИ оптимизирует запасы и маршруты транспортировки. ИИ для контртерроризма помогает выявлять угрозы и анализировать аномалии. ИИ в пограничной безопасности поддерживает биометрические технологии и предиктивную аналитику. ИИ для гуманитарной помощи и реагирования на бедствия анализирует данные для оценки ущерба и координации ресурсов.

Потенциальные перспективные технологические решения в сфере искусственного интеллекта действительно обладают значительным потенциалом для качественного улучшения государственных услуг, повышения эффективности управления и обеспечения более широкого доступа к ресурсам и услугам. Однако, наряду с возможностями, существует ряд ключевых рисков и вызовов, которые могут препятствовать достижению этих результатов и даже усугубить текущие дисбалансы в развитии технологической инфраструктуры и социальной сферы. Эти риски можно условно разделить на несколько категорий: институциональные, инфраструктурные и кадровые.

Первая категория угроз — **институциональное отставание**. В условиях стремительного внедрения искусственного интеллекта в различные государственные процессы национальные институты могут оказаться не готовыми к адаптации новых алгоритмических решений. Основная проблема здесь заключается в том, что нормативно-

правовая база часто не поспевает за изменениями в технологическом ландшафте. Это несоответствие создает так называемый "регуляторный разрыв", при котором использование ИИ остается юридически не урегулированным или не охваченным нормативными документами. В результате, применение искусственного интеллекта в таких условиях может привести к правовым коллизиям, рискам нарушения прав граждан, а также к отсутствию эффективных механизмов контроля и ответственности. Институциональное отставание становится особенно критичным в условиях, когда технологии ИИ оказывают влияние на вопросы безопасности, конфиденциальности данных и соблюдения прав человека.

Вторая категория — **инфраструктурное отставание**. Современные ИИ-решения требуют высокопроизводительных вычислительных мощностей, устойчивых каналов связи, надежных дата-центров и современных технологий обработки данных. В отсутствие этих ресурсов страна рискует столкнуться с проблемами не только в развертывании и поддержании ИИ-инфраструктуры, но и в обеспечении кибербезопасности и устойчивости систем. В условиях, когда доступ к продвинутым процессорам, микросхемам и иным аппаратным компонентам ограничен, страна вынуждена либо отказываться от передовых технологий, либо зависеть от более технологически развитых стран, что ведет к рискам технологической зависимости и угрозам национальной безопасности. В подобных ситуациях возрастает вероятность возникновения "цифрового неравенства", когда государственные и частные организации не могут обеспечить конкурентоспособные ИИ-услуги на глобальном уровне.

Третья категория — **отставание компетенций**. Развитие ИИ-технологий требует наличия высококвалифицированных специалистов: инженеров, программистов, аналитиков данных, специалистов по кибербезопасности и экспертов в области алгоритмов. Недостаток компетентных кадров, а также образовательных программ, нацеленных на подготовку специалистов в области ИИ, существенно ограничивает потенциал страны в развитии сложных ИИ-решений. В условиях дефицита кадровых ресурсов страна рискует потерять возможность разрабатывать и внедрять инновационные ИИ-технологии, оказываясь на позиции догоняющего. Более того, отставание компетенций увеличивает вероятность ошибок в разработке и применении ИИ, что может повлечь за собой негативные социальные последствия и подорвать доверие населения к государственным инициативам в этой области.

В совокупности, институциональное, инфраструктурное и кадровое отставание создают значительные риски для успешного внедрения и использования ИИ в государственных процессах. Игнорирование этих угроз может привести к тому, что они

станут источником новых системно значимых вызовов, представляющих экзистенциальную угрозу стабильному развитию государства.

Также злонамеренное использование технологий искусственного интеллекта представляет собой серьёзную угрозу, которая выходит за рамки традиционных проблем цифровой безопасности. Одним из примеров является создание дипфейков — поддельных изображений и видеозаписей, генерируемых с использованием алгоритмов глубокого обучения. Эти технологии позволяют злоумышленникам манипулировать визуальной информацией, создавая правдоподобные подделки, способные дискредитировать политических лидеров, публичных лиц и простых граждан, а также распространять дезинформацию.

Еще одной формой злоупотребления ИИ является его использование в кибератаках, где алгоритмы могут подбирать эффективные схемы проникновения, уклоняться от обнаружения, а также генерировать фишинговые сообщения, адаптированные к конкретным целям, что повышает вероятность успеха атак. Также ИИ может применяться для создания автоматизированных систем слежения и предсказания поведения, что, в условиях отсутствия этических норм и законодательных ограничений, угрожает гражданским свободам и конфиденциальности данных.

В совокупности, все эти методы злонамеренного использования ИИ способны подорвать доверие общества к цифровым технологиям и усилить информационные и социальные риски, что создаёт новые вызовы для национальной и глобальной безопасности.

Вторая важная технологическая область – это технология метавселенных. Метавселеннаую можно рассматривать как феномен, интегрирующий в пространство единой экосистемы на стыке реального и виртуального технологические новации, социальные практики и особый тип криптоэкономики. Прежде всего метавселенные представляют собой продолжение человеческих сенсорных и когнитивных возможностей, выполняя роль медиатора между физическим и виртуальным мирами, где цифровые технологии расширяют возможности общения, экономического и культурного обмена.

Так формируются новые сетевые публичные пространства, где технологии, экономика и социальные взаимодействия интегрируются в единый виртуальный континуум. Их способность объединять физические и цифровые миры стимулирует трансформацию глобального взаимодействия, расширяя возможности для коммуникации, креативных практик и цифрового обмена, что формирует гиперсвязанное мировое сообщество.

В этом контексте представляется важным обеспечить стратегическое лидерство Российской Федерации в рамках данного нового гиперпространства метавселенных.

Вместе с этим, развитие метавселенных сопровождается рядом значительных вызовов и потенциальных угроз.

Прежде всего, необходимо отметить зависимость их инфраструктуры от западных технологических корпораций, что сказывается на доступности, устойчивости и стандартах их функционирования. Такая зависимость ставит под вопрос цифровой суверенитет стран-участников, включая Российскую Федерацию, что требует тщательного анализа и поиска стратегий для минимизации подобных рисков.

Кроме того, виртуальные пространства метавселенных несут в себе риск усиленного распространения вредоносного контента, в том числе дезинформацию. Высокая степень интерактивности и возможность сохранять относительную анонимность усложняют процесс контроля, что создаёт условия для увеличения влияния вредоносной информации. Это ставит перед обществом задачу разработки институциональных механизмов, способных регулировать такие процессы и обеспечивать информационно-психологическую безопасность.

Также стоит подчеркнуть вероятность появления враждебных виртуальных сред, формирующихся на основе радикальных идеологий или маргинализированных ценностей. Такие тенденции могут подрывать стабильность и гармоничное взаимодействие между различными группами.

С учётом того, что российское сообщество в настоящее время недостаточно представлено в этих пространствах, существует угроза утраты влияния на ключевые дискурсы в метавселенных. Поэтому актуальным становится разработка сценариев позитивного присутствия Российской Федерации в пространстве метавселенных.

Третьей, сквозной технологией, является блокчейн. В контексте искусственного интеллекта и метавселенных блокчейн выступает не только техническим фундаментом, но и средством решения ключевых проблем, таких как управление данными, защита конфиденциальности и обеспечение децентрализации.

В сфере искусственного интеллекта блокчейн обеспечивает надёжное хранение обучающих данных, гарантию их подлинности и прозрачность в принятии решений. Блокчейн также позволяет создавать безопасные механизмы обмена данными между участниками экосистемы ИИ, устраняя посредников и минимизируя риски утечек информации.

В метавселенных блокчейн становится основой для создания цифровых экономик. Использование токенов и смарт-контрактов позволяет реализовать системы виртуальной

собственности, прозрачные механизмы оплаты и взаимодействия между пользователями. Кроме того, блокчейн гарантирует аутентификацию цифровых активов и их защиту от подделки, что критически важно в условиях растущего объёма транзакций и виртуальных товаров в рамках метавселенных.

Для Российской Федерации блокчейн представляет стратегический интерес как инструмент развития цифрового суверенитета. В условиях усиливающегося геополитического давления эта технология способна укрепить национальную инфраструктуру в таких сферах, как государственное управление, финансовая система, а также информационная устойчивость. В условиях новых вызовов, таких как санкционное давление и цифровая изоляция, развитие блокчейн-технологий позволяет России сохранить конкурентоспособность в глобальной цифровой экономике, в том числе в экономике метавселенных. Более того, применение блокчейна способствует развитию экосистем, независимых от зарубежных платформ и стандартов, создавая возможности для экспорта национальных решений и укрепления международного сотрудничества.

# 4 Обеспечение национальной безопасности в контексте развития Индустрии 4.0

## 4.1 Цифровое кочевничество как глобальное явление после пандемии COVID19

В XXI веке стала особенно заметной значительная и продолжающаяся трансформация практически всех аспектов жизни общества в силу процессов цифровизации. Технологии сыграли решающую роль в обеспечении и содействии этим изменениям, что привело к быстрым инновациям и трансформации. Пандемия COVID-19 ускорила эту тенденцию, сделав удаленную работу и виртуальное сотрудничество глобальным явлением и «новой нормой» для многих отраслей.

В последние годы мы можем наблюдать существенные изменения мировых тенденций в отношении выбора места работы высококвалифицированными специалистами. Условия пандемии COVID-19 сыграли важную роль в мотивации выбора удаленной работы или смены места работы. Также можно сказать, что цифровое кочевничество может стать более привлекательным форматом образа жизни с учетом растущей популярности удаленной работы в будущем, то есть сохранит свои черты общемирового тренда, сопровождающего процессы глобализации [75]. Это может быть особенно актуально в контексте глобального Юга, который уже переживает «транснациональную джентрификацию» [76].

И если мы можем видеть, как в последние годы глобальные политические процессы, такие как массовое введение санкций одними странами против других, способствуют процессам деглобализации, то процессы цифровой миграции, запущенные в период пандемии COVID-19, закрепляют глобальные миграционные тенденции.

В результате анализа факторов, которые стимулируют желание переехать или, наоборот, способствуют сохранению текущего местоположения специалистов в IT и смежных сферах, были выделены следующие четыре категории наиболее значимых факторов:

- Факторы места происхождения,
- Факторы места назначения,
- Препятствия и
- Личные факторы.

Феномен цифрового кочевничества среди россиян набирает обороты в последние годы, когда люди принимают образ жизни, характеризующийся независимостью от местоположения и удаленной работой, как часть глобальной тенденции, которая усилилась в начале 2020-х годов.

Обусловлено это тем, что Россия может похвастаться высокообразованной рабочей силой в IT-сфере, которая хорошо подходит для удаленной работы и цифрового кочевничества. Еще одной важной особенностью является то, что ИТ-индустрия является сильной стороной в России с большим количеством разработчиков программного обеспечения и технологических стартапов. Это способствовало развитию культуры предпринимательства и инноваций, сделав цифровое кочевничество привлекательным вариантом для людей в этой отрасли. Далее, российское правительство внедрило политику, которая поддерживает удаленную работу, например, разрешило сотрудникам работать из дома и предоставило налоговые льготы компаниям, которые предлагают варианты удаленной работы. Эти меры политики облегчили россиянам переход к цифровому кочевничеству.

Среди мотивов, побуждающих этих специалистов к переезду в другие регионы, начиная с периода пандемии COVID-19, можно выделить следующие:

- Психологические мотивы: к ним относятся стремление к новому опыту, приключениям и личностному росту. Для цифровых кочевников мотивирующими факторами могут быть стремление к более гибкому образу жизни и возможность путешествовать и работать одновременно.

- Социальные мотивы: в этом случае мы можем говорить о желании познакомиться с новыми людьми и познакомиться с разными культурами. Возможность общаться с

другими профессионалами со всего мира может быть фактором, стимулирующим готовность переехать в другую область или регион.

- Экономические мотивы: к ним относятся желание получать более высокую заработную плату или же доступ к новым возможностям трудоустройства. Для цифровых кочевников мотивирующим фактором может быть возможность работать удаленно и зарабатывать в другой валюте.

С другой стороны, в контексте факторов притяжения, можно выделить следующие мотивы:

- Мотивы, связанные с местом назначения: сюда относятся привлекательность и удобства определенного места, такие как климат, природная красота и культурные достопримечательности. Для цифровых кочевников наличие доступного жилья, коворкинг-пространств и надежного Интернета-соединения являются важными факторами, которые могут стимулировать готовность оставаться в родном районе.

- Факторы, облегчающие путешествия: простота перемещений, что включает в себя наличие рейсов, виз и транспорта. Для цифровых кочевников возможность легкого доступа и путешествий в различные пункты назначения может быть мотивирующим фактором.

- Институциональные факторы: к ним относятся политическая и экономическая стабильность места назначения, а также наличие поддерживающих институтов, таких как коворкинг-пространства и сетевые группы. Для цифровых кочевников наличие поддерживающего сообщества и инфраструктуры может служить одним из важных мотивов переезда в другое место.

При этом в отношении цифровых кочевников из в целом России можно сказать, что одной из основных характеристик российской ИТ-сферы является то, что Россия может похвастаться высокообразованной рабочей силой, при этом значительное число лиц имеет высшие ученые степени. Кроме того, российское правительство внедрило ряд мер, направленных на поддержку формата удаленной работы. И несмотря на то, что существует ряд факторов, стимулирующих отток специалистов в этой области из России, который усилился после периода пандемии COVID-19, есть основания полагать, что сейчас заложена основа для нивелирования влияния факторов выталкивания и стимулирования возможного возвращения таких специалистов в Россию.

### 4.2 Интернет-балканизация и цифровые границы

Процесс фрагментации Интернета, также иногда называемый «балканизацией», – это тренд на разделение Всемирной сети на отдельные национальные «интернеты» с точки

зрения их политического и законодательного регулирования. Разделение Интернета происходит в результате того, что государства следуют своим национальным интересам, которые мы связаны в первую очередь со стремлением обеспечить “выживание” государства, его экономическую безопасность, политическую и культурную самобытность [77]. Защита этих интересов в контексте Интернета обычно понимается как защита данных граждан и информации от постороннего вмешательства [78].

Управление киберпространством неразрывно связано с суверенитетом государств и их отношениями с заинтересованными сторонами, что сделало эту тему предметом серьезных дискуссий и споров [79]. Если в начале своего существования Интернет воспринимался как пространство без границ, то в последние годы появляется все больше свидетельств того, что ему грозит «балканизация», раскол на национализированные фрагменты [80].

Сегментации Интернета, помимо всего прочего, способствуют вполне технические причины и условия. С момента своего создания Интернет создал положительные внешние эффекты сети, широкий доступ и бесперебойную связь благодаря сочетанию технологий маршрутизации и широкой совместимости сетей [81]. Этот период характеризовался значительным интересом провайдеров к сотрудничеству. Однако по мере роста спроса на Интернет-услуги перегруженность квазигосударственных узлов межсетевого взаимодействия и коммерциализация этой сферы заставили крупных Интернет-провайдеров и крупных пользователей искать более надежные квазичастные межсетевые соединения. Общинная модель, которая преобладала в предыдущие периоды и актуальность которой была продиктована экономическими и глобальными проблемами безопасности того времени, неизбежно уступает место дифференцированным и менее взаимосвязанным сетям из-за распространения рыночных цен [82].

В начале 1990-х годов Интернет рассматривался как своего рода универсальный инструмент, который объединял бы людей по всему миру. Однако к 2000-м годам энтузиазм в отношении подобных идей стал постепенно угасать. Появление «платформенного капитализма» [83] стало еще одним препятствием на пути возможного создания поистине всемирной сети: немногие компании контролируют веб-платформы, используемые всеми остальными пользователями Интернета, и это влияет на их качество. Аналогичная концепция — «капитализм наблюдения», которая подразумевает, что компании относятся к данным пользователей как к товару, который они используют для создания более эффективной рекламы [84]. Однако это приводит не только к появлению более эффективных рекламных кампаний, но и к нарушению принципов конфиденциальности.

Перечисленные выше проблемы приводят к тому, что правительства разных стран могут увидеть угрозу в развитии Интернета в том случае, если продолжатся эпизоды нарушения конфиденциальности, увеличения зависимости от нескольких крупных корпораций и дезинформации. По этой причине Всемирная паутина становится все менее «всемирной» и все более национальной.

К началу XXI века наблюдается четкая тенденция к «локализации данных» — законам, которые требуют, чтобы данные хранились и обрабатывались в пределах географических границ страны их происхождения [85].

В настоящее время можно говорить о том, что сформировались конкретные страновые модели регулирования Интернет-пространства, появившиеся в контексте вышеописанных процессов сегментации Интернета, в частности в таких странах как ЕС, Китая, России и США.

Крупные страны по-разному преследуют свои национальные интересы. Долгое время США были главными выгодоприобретателями глобализованного Интернета, однако вследствие внутренних политических потрясений подход к интернету был изменен в пользу кибербезопасности. Несмотря на строгое регулирование трафика данных в ЕС, там долгое время сохранялась политика открытого обмена данными с США. После разоблачений Сноудена отношение европейских регуляторов к свободному трафику данных поменялось.

Наиболее значимым примером при анализе национальных моделей регулирования Интернет-пространства является, пожалуй, Китай. Китайский интернет – это пример национального Интернета, который уже достаточно изолирован от глобальной сети и фактически существует независимо. Все провайдеры в Китае принадлежат государству и доступ в Интернет регулируется полностью. Значительное присутствие государства в сегменте Интернета и отсутствие доступа ко множеству иностранных ресурсов повлияло на китайский Интернет таким образом, что его структура и дизайн заметно отличаются от моделей Интернет-пространства в других странах.

Китай стремится построить свою собственную международную цифровую экосистему, известную как «Цифровой шелковый путь» - термин, который возник в 2015 г. и который является составляющей инициативы Пояс и Путь, долгосрочного проекта по развитию экономических связей и глобализации с Китайской Народной Республикой в качестве главного игрока. Пояс и Путь включает в себя физическую и цифровую инфраструктуру, которая должна соединить различные страны. «Цифровой шелковый путь» - это обобщающий термин для всей китайской цифровой инфраструктуры, которая

расширяется в другие страны. Таким образом, и американский, и китайский взгляды на будущее интернета сейчас активно распространяются по миру.

Долгое время русский язык был вторым по распространенности во Всемирной паутине по количеству использующих его сайтов. В российском интернете также появилось множество совершенно оригинальных проектов, которые открыто конкурировали с такими глобальными информационными конгломератами, и выжили в нынешнюю эпоху фрагментации, забота о национальной безопасности и локализация данных стали основными факторами медленного, но неуклонного отделения российского Интернета от Всемирной паутины.

Таким образом, мы можем говорить о жизнеспособности национальных моделей Интернета и их развитии на страновом уровне. В контексте инициативы «Цифровой шелковый путь» развитие сотрудничества в сфере информационных технологий может выступать частью общих интеграционных процессов со странами-партнерами в настоящее время.

Наконец, в России в какой-то степени объединились западные и китайские подходы: если в начале существования российского интернета он фактически не регулировался, то в настоящий момент он активно превращается в защищенный от внешнего влияния.

### 4.3 Стратегическая конкуренция в регионе Ближнего Востока и Северной Африки

Принимая во внимание то обстоятельство, что в 2024 г. членами БРИКС стали 3 государства Ближнего Востока: Саудовская Аравия, ОАЭ и Иран представляется важным разобраться с геополитической обстановкой на Ближнем Востоке. События «Арабской весны» существенно повлияли на конфигурацию сил на геополитической карте региона Ближнего Востока и Северной Африки, привела к появлению наряду с традиционными игроками (Египтом, Саудовской Аравией, Ираном, Ираком, Израилем) новых претендентов на региональное лидерство в лице Катара, Турции и ОАЭ. Кроме того, произошло стратегическое объединение между Катаром и Турцией, которые на фоне роста протестных выступлений попытались укрепить свои позиции в ряде стран БВСА. Наряду с использованием финансовых и дипломатических рычагов, катарско-турецкий альянс поддержал различные исламистские движения, в основном, связанные с «Братьями-мусульманами»[2] (ал-ихван ал-муслимун). Помимо всего прочего, важнейшим инструментом информационно-психологического воздействия выступил мощнейший

[2] Запрещенная в РФ организация.

катарский медиа-ресурс – телеканал «Аль-Джазира», который работал на формирование благоприятного образа «Братьев-мусульман», способствуя росту их популярности в регионе. Влияние катарского телеканала «Аль-Джазира» в 2011 г. чрезвычайно возросло, его трансляции сыграли большую роль в распространении цунами «арабской весны», а некоторые аналитики даже назвали арабские восстания «ал-джазировой революцией». В настоящее время Аль-Джазира продолжает оставаться важнейшим инструментом пропаганды и информационно-психологического воздействия на аудиторию региона БВСА и за его пределами.

В ходе проведенного анализа мы пришли к выводу, что беспрецедентное усиление позиций транснациональной организации “Братья-мусульмане” и их покровителей в лице Катара и Турции не могли не вызвать реакцию со стороны консервативно настроенных кругов, в особенности суннитских монархий во главе с Саудовской Аравией. До событий «арабской весны» внешнеполитический вектор монархий Персидского залива развивался в рамках контуров, формируемых Саудовской Аравией. В качестве института, закрепляющего данное единство, выступал Совет сотрудничества арабских государств Персидского залива (ССАГПЗ). Однако «арабская весна» обнажила скрытые противоречия между рядом монархий – членов организации. Активную роль в выстраивании самостоятельной политики продемонстрировал Катар, который, сблизившись с Турцией, бросил вызов лидирующим позициям Саудовской Аравии в регионе. Исходя из того, что по отдельности Катар и Турция имели мало шансов добиться лидирующих позиций в БВСА, объединение катарской финансовой мощи и турецкого военно-политического потенциала способствовало формированию крайне эффективного альянса, сопоставимого с региональными позициями Саудовской Аравии или Ирана. Для Саудовской Аравии ассоциация «Братья-мусульмане», в которой преобладают умеренные исламистские взгляды о республиканской форме правления и сочетаемости исламских принципов управления государством с демократическим ценностями, представляют прямую угрозу существования монархического строя. Кроме того, эти идеи идут вразрез с официальным консервативным исламом Саудовской Аравии. Более того, победа на президентских выборах представителя «Братьев-мусульман» М. Мурси в Египте в 2012 г. и последующий обмен визитами с иранским коллегой обозначили возможность установления дружественных отношений между Египтом и Ираном. Для Саудовской Аравии египетско-иранское сближение несло прямую угрозу государственной безопасности и интересам в регионе. Отметим, что ОАЭ разделяли беспокойство Эр-Рияда, что обусловило переход к принятию саудовцами и эмиратцами активных действий

по нивелированию новых угроз. Все это способствовало формированию довольно эффективного саудовско-эмиратского блока.

Исследование динамики экономического развития Саудовской Аравии и ОАЭ, операционализированного через рост ВВП, а также уровню экономической диверсификации показало, что за короткий промежуток времени страны сумели достичь очень существенного экономического развития. К примеру, с 1990-х гг. экономика ОАЭ (с некоторыми задержками в 2008-2009 гг. в связи с глобальным финансово-экономическим кризисом и в 2020-2021 в связи с пандемией Covid-19) демонстрирует непрерывный рост, хотя и несколько замедлившийся в 2010-е гг. во всех нефтяных монархиях Персидского залива. Особо отметим, успехи ОАЭ в экономической диверсификации и снижении зависимости от экспорта сырых углеводородов. Действительно, если в 1995 г. на сырые углеводороды (нефть и природный газ) приходилось около 70% эмиратского экспорта, то уже в 2021 году – около 20%. Для сравнения в Саудовской Аравии в 2021 г. эта доля составляла более 50%, а в Катаре – более 60. Существенно выросшая экономика ОАЭ (с 1994 по 2011 г. ВВП Эмиратов вырос почти в 10 раз) позволила им включиться в борьбу за региональное лидерство.

В результате проведенного исследования было выяснено, что экономическому успеху монархий, наряду с достаточно эффективным использованием колоссальных объемов углеводородов, способствовали амбициозные проекты, направленные на превращение этих стран в научно-технологические, торгово-экономические и инвестиционные центры. Особую роль в освещении внешнеполитических успехов монархий Персидского залива сыграли крупные арабские телеканалы, такие как саудовская Al-Arabiya и катарская Al-Jazeera.

Сформировавшийся саудовско-эмиратский блок выступил в качестве стабилизирующего механизма в процессе недопущения усиления активности катарско-турецкого и ирано-шиитского блоков. Это привело к некоторому ослаблению напряженности в регионе. В частности, стабилизация геополитической обстановки произошла на Аравийском полуострове, в странах Северной Африки и Африканского Рога, в Сирии, Иордании. Совместные действия Эр-Рияда и Абу-Даби по противодействию региональным угрозам привели к заключению в 2016 г. союзного договора, в котором большое значение уделялось именно военно-политическим вопросам.

Проведенный анализ продемонстрировал, что в последние годы все более важным фактором становится конкуренция ключевых игроков Персидского залива и Ближнего Востока в целом в экономике и в дипломатической сфере. За исключением кризиса вокруг Катара, где Саудовская Аравия стала инициатором прекращения блокады, ОАЭ проявили

себя более прагматичным игроком, способным не только завершать противостояния, которые становились им не выгодны, но и формировать новые союзы. Формирование новых союзов в ответ на появление других союзов способствовало складыванию определенного равновесия в регионе, хотя, и не совсем прочного. В свою очередь, наблюдается высокая вероятность того, что такого рода стабилизация будет способствовать обеспечению научно-технологического, финансово-экономического, политического и информационно-психологического суверенитета ключевых государств БВСА.

### 4.4 Палестино-израильский конфликт как фактор дестабилизации современных международных отношений

Начавшийся в 2023 г. палестино-израильский конфликт к замешательству многих региональных и глобальных игроков из-за невозможности объективно оценить сложившуюся ситуацию. Несмотря на внезапность, уже в первые дни после начала конфликта было известно о большом количестве жертв у каждой из сторон. Обсуждение ситуации было вынесено на обсуждение в Совет Безопасности ООН, однако резолюцию, призывающую немедленно прекратить огонь в зоне конфликта принять не удалось. Большую роль в формировании тех или иных образов сыграли мировые СМИ, часть из которых демонизировала ситуацию, завышая количество жертв, другая – отстаивала палестинскую либо израильскую стороны. В региональном отношении большинство стран выступило с единой позицией – возложением ответственности за нападения на Израиль. Лишь малая часть стран региона осудила любое насилие и призвала конфликтующие стороны начать мирные переговоры. Жесткая риторика наблюдалась со стороны одного из неарабских игроков региона – Турции, которая открыто объявила о поддержке ХАМАС и осудила действия Израиля. Эскалационный тон содержался и в официальных заявлениях Ирана. Глобальные игроки в лице США и ЕС выступили на стороне Израиля, заявив о праве израильтян на самооборону. Позиция России и Китая заключалась в скорейшем прекращении огня, а также в необходимости реализации решения о сосуществовании двух государств и создании независимого палестинского государства.

В деле отстаивания палестинской позиции несомненными лидерами стали саудовский телеканал Al-Arabiya и катарский телеканал Al-Jazeera. Отметим, что катарский телеканал имеет колоссальный опыт освещения такого рода событий. К примеру, в период «арабской весны» демонстрация телеканалом протестных выступлений в странах БВСА, усилившая революционный накал, получила неофициальное название

«аль-джазировой революции». Правоту израильских действий поддержали ведущие западные СМИ, в основном из числа американских газет и телеканалов.

Обращая внимание на позицию региональных и глобальных игроков на очередной виток палестино-израильского конфликта и их усилия по разработке мер, направленных на прекращение насилия в первые несколько месяцев, необходимо кратко осветить дальнейшее развитие ситуации в зоне сектора Газа. Министерство обороны Израиля при активной поддержке правительства во главе с Б. Нетаньяху и молчаливом согласии американской администрации объявило о полной блокаде Газы и начале наземной операции на севере анклава, направленной на уничтожение боевых формирований ХАМАС. Превосходство в живой силе и авиации привели к перемещению гражданского населения в южные части анклава. Агрессивные действия израильского ЦАХАЛ привели не только к планомерному уничтожению боевых формирований ХАМАС и принадлежащей им инфраструктуры, но и ко многим инцидентам, связанным с большим количеством жертв из числа гражданского населения. По состоянию на май 2024 г. количество жертв израильской агрессии в Газе превысило 35 тыс. человек при более чем 78 тыс. пострадавших.

Особо следует обратить внимание на то, что Израиль при принятии решений о выборе конкретных объектов для атаки в секторе Газа использует специализированную ИИ-систему.  У израильской армии есть база данных, содержащая информацию о 30-40 тысячах человек, которые предположительно (и здесь мы хотели бы подчеркнуть слово "предположительно") являются членами ХАМАС.  И эта автоматизированная интеллектуальная система, основанная на этих данных, помогает определять координаты домов таких палестинцев, т.е. служит средством наведения.

Примечательно, что эта интеллектуальная система также дает информацию о предполагаемом количестве жертв среди мирного наведения. Однако израильскую армию этот факт не останавливает.

Также высокая вероятность гибели мирного населения не остановила Израиль при планировании масштабной диверсии, связанной с массовом взрывом пейджеров на территории Ливана. Таким образом, можно сделать вывод о том, что передовые информационные технологии становятся полноценным оружием массового уничтожения, и их следует взять под контроль, как и обычное оружие массового уничтожения.

Колоссальный масштаб разрушений и тяжелейшая гуманитарная ситуация вызвали бурю негодований среди жителей не только мусульманских стран, но и Европы и США. Многие лидеры общественного мнения, международные правозащитные и другие организации продолжают призывать к бойкотированию Израиля. Принятые декларации по

итогам проведенных саммитов Лиги арабских государств и Организации Исламского Сотрудничества, направленные на необходимость объединения сектора Газа и Западного берега реки Иордан в суверенную Палестину, также не дали практических результатов. Однако важные подвижки произошли по вопросам гуманитарного характера и освобождения заложников, удерживаемых ХАМАС. Важнейшую роль здесь сыграли египетские и катарские дипломаты, а также освещение их деятельности ведущими региональными СМИ.

Показано, что резко осуждающие заявления со стороны турецких властей, а также попытки Ирана и его прокси в лице ливанской Хезболлы и йеменских хуситов оказать военно-политическую поддержку ХАМАС казалось, лишь укрепили израильское руководство в намерении довести до конца военную операцию. Решение запретить работу катарского международного телеканала Al-Jazeera на территории Израиля видимо также говорит о том, что правительство Б. Нетаньяху не устраивает растянутый по времени процесс по освобождению заложников, активным посредником в котором является Катар. Ранее очередной раунд переговоров между Израилем и ХАМАС прошедший в Каире 4-5 мая (без участия Израиля) с участием представителей Египта, Катара и США не привел к изменению планов ЦАХАЛ.

В ходе анализа мы пришли к выводу, что военные действия, проводимые Израилем в секторе Газа приводят к гуманитарной катастрофе. Продолжающиеся военные действия лишь усугубляют ситуацию. При этом, очевидно, что нынешний состав израильского правительства, несмотря на репутационные издержки пытается всерьез и надолго решить проблему с демилитаризацией и дерадикализацией анклава. В одном из своих интервью Б. Нетаньяху отмечал, что «силы ЦАХАЛ сохранят контроль над сектором Газа и не отдадут его международным силам». В свою очередь, глава политбюро ХАМАС Исмаил Хания заявил «о недопустимости оккупантам или кому-либо еще регулировать ситуацию в Палестине, в секторе Газа, на Западном берегу или на обоих этих территориях». В этой связи, глубокие расхождения мнений противоборствующих сторон вносят неопределенность в вопрос относительно будущего сектора Газа.

## 5 Подходы к обеспечению ИПБ общества, принятых в России и интеграционных объединениях, в которых Россия принимает наиболее активное участие (ШОС, ЕАЭС, ОДКБ, БРИКС)

Постсоветское пространство вот уже более тридцати лет является ареной геополитического противоборства, на которой сталкиваются национальные интересы государств, финансово-экономических групп, ценностные и идеологические модели

развития. При этом внешние силы, прежде всего коллективный Запад во главе с США, рассматривают усиление евразийской интеграции как угрозу своему доминирующему положению в мире. Поэтому зачастую постсоветские государства становятся объектом попыток установления внешнего влияния, являющегося частью комплексной политики сдерживания России и Китая. В результате, представляется крайне важным России совместно со своими партнерами по тем интеграционным объединениям, в которых Россия принимает наиболее активное участие (ШОС, ЕАЭС, БРИКС, ОДКБ) выработать эффективную политику, направленную на нивелирование широкого спектра информационных угроз, исходящих от недружественных государств.

### 5.1 Россия

Россия применяет комплексный подход к обеспечению ИПБ, который включает законодательные, организационные и технические меры. Наличие федеральных органов, таких как Федеральная служба безопасности  и Федеральная служба по техническому и экспортному контролю, позволяет оперативно реагировать на киберугрозы. Принятые законы, такие как Федеральный закон «О персональных данных» (ФЗ-152) и Федеральный закон «Об информации, информационных технологиях и о защите информации» (ФЗ-149) обеспечивают правовую защиту данных и регламентируют действия организаций в сфере ИПБ. Утверждение Национальной стратегии обеспечения безопасности в информационной сфере также обеспечивает координацию действий различных ведомств и учреждений.

Кроме централизованного подхода и развитой нормативно-правовой базы, Россия уделяет большое внимание инвестициям в кибербезопасность: увеличивается финансирование проектов в области кибербезопасности, активно создаются государственные программы по защите критической информационной инфраструктуры.

К недостаткам подхода России к обеспечению ИПБ можно отнести низкий уровень открытости действий государственных органов в сфере ИПБ, что приводит к недоверию со стороны граждан и бизнеса, а жесткие меры контроля за интернетом и цензура могут негативно сказаться на свободе слова и доступе к информации, что вызывает общественное недовольство. Кроме того, частные компании сталкиваются с трудностями в реализации собственных систем безопасности из-за зависимости от государственных стандартов и требований.

### 5.2 ОДКБ

ОДКБ, включает в себя такие страны, как Россия, Армения, Беларусь, Казахстан, Кыргызстан и Таджикистан и на сегодняшний день является единственным дееспособным инструментом обеспечения коллективной безопасности на постсоветском пространстве и ключевым элементом «евразийского пояса безопасности», объединяющего усилия действующих на постсоветском пространстве коалиционных структур. Именно поэтому выработка коллективной политики в области обеспечения ИПБ представляется сегодня одним из основных приоритетов.

В настоящее время в официальных документах ОДКБ термин «информационно-психологическая безопасность» не используется, а вопросы имеющие отношение к данной сфере, находятся в общем блоке целей и задач обеспечения информационной безопасности.

Первые шаги по построению системы информационной безопасности на уровне ОДКБ датируются 2006 годом, когда одним из итогов ноябрьского заседания Комитета секретарей советов безопасности в Минске стало решение о создании при Комитете Рабочей группы по вопросам информационной политики и информационной безопасности, за которой были закреплены функции координации совместных действий по выявлению общих проблем и угроз для государств-членов ОДКБ в сфере информационной политики и безопасности, а также разработки предложений о совместном противодействии им.

Несколько лет спустя, в 2010 году, на заседании Совета коллективной безопасности, состоявшемся в Москве, задачи обеспечения информационной безопасности вошли в перечень приоритетов политики в сфере коллективной безопасности. В принятых итоговых документах заседания впервые на уровне ОДКБ задачи, относящиеся к сфере информационно-психологической безопасности, были выделены из общей системы информационной безопасности. В частности, в перечне основных направлений сотрудничества отдельно указаны противодействие и нейтрализация информационных потоков, формирующих негативное отношение и недостоверное представление о государствах-членах ОДКБ.

Помимо этого, в соответствии с принятыми решениями, спустя три месяца были определены национальные координирующие органы в сфере обеспечения информационной безопасности: Армения – Служба национальной безопасности, Беларусь – Оперативно-аналитический центр при Президенте, Казахстан – Комитет по информационной безопасности, Кыргыстан – Координационный центр по обеспечению кибербезопасности при Государственном комитете национальной безопасности, Россия –

Федеральная служба безопасности, Таджикистан – Государственный комитет национальной безопасности. Таким образом, за силовыми органами государств-членов закрепился весь спектр вопросов, связанных с обеспечением информационной безопасности, порядок взаимодействия которых позднее был определен отдельным документом.

Ключевую роль в процессе концептуализации вопросов обеспечения ИПБ на уровне ОДКБ сыграла утвержденная в 2016 году Советом коллективной безопасности Стратегия коллективной безопасности ОДКБ на период до 2025 года. В документе указывается, что одним из основных факторов, относящихся к современным вызовам и угрозам коллективной безопасности ОДКБ, является стремление к достижению стратегических целей с использованием силы, в том числе и информационного давления, использование информационных и коммуникационных технологий в целях оказания деструктивного воздействия на общественно-политическую и социально-экономическую обстановку, манипулирования общественным сознанием, применение информационных технологий в так называемых «комплексных» или «гибридных» технологиях. Стратегия фокусирует внимание на медийных аспектах информационного давления, признавая ведущую роль электронных ресурсов. Так, в перечне внешних и внутренних вызовов и угроз коллективной безопасности ОДКБ отдельным пунктом обозначено осуществление деструктивного идеологического и психологического воздействия на население через электронные информационные сети и медиаресурсы.

По сути, документ на официальном уровне закрепил за информационно-психологическим воздействием статус одного из элементов современного силового противоборства. И хотя речь не идет о рассмотрении информационно-психологической сферы в качестве нового измерения современной войны, тем не менее, логика Стратегии указывает на расширение концептуальных границ обеспечения коллективной безопасности в зоне ответственности ОДКБ и указывает на необходимость координации совместных усилий в целях формирования единого безопасного информационного пространства государств-членов.

Еще один шаг на пути формирования целостной системы нормативного обеспечения информационной безопасности на пространстве ОДКБ был сделан год спустя, 30 ноября 2017 г. в Минске. Тогда лидеры государств-членов подписали Соглашение о сотрудничестве в области обеспечения информационной безопасности, в котором впервые дано консенсусное определение понятию «деструктивное информационное воздействие» - использование информационно-коммуникационных технологий в целях нарушения деятельности органов власти, ослабления национальной безопасности, нанесения ущерба

информационно-коммуникационным системам, сетям и ресурсам, ухудшения межгосударственных отношений, создания внутренней социально-политической напряженности, разрушения традиционных духовных и нравственных ценностей, установления контроля над национальными информационными ресурсами, формирования угрозы возникновения чрезвычайных ситуаций, причинения иного ущерба интересам государств-членов ОДКБ. В тексте определения отчетливо просматриваются два относительно самостоятельных аспекта: первый фокусирует внимание на информационно-технических аспектах, таких как кибератаки на информационную инфраструктуру, а второй имеет прямое отношение к вопросам информационно-психологического противоборства.

Значительную роль в сфере выработки коллективной политики по обеспечению информационной безопасности в зоне ответственности ОДКБ сыграл Модельный закон «Об информационной безопасности», принятый Парламентской Ассамблеей 29 ноября 2021 года.

В документе обозначены четыре сферы обеспечения коллективной информационной безопасности: оборона; защита конституционного строя и государственной безопасности; информационные технологии и связь; стратегическая стабильность и равноправное стратегическое партнерство. В области обозначения основных угроз и направлений совместных действий Закон, по сравнению с предшествующими документами, делает шаг вперед в дифференциации концепции обеспечения информационной безопасности ОДКБ. Так, в сфере защиты конституционного строя и государственной безопасности все указанные угрозы лежат в плоскости информационно-психологического противоборства. Например, к их числу относятся использование средств массовой информации, интернета и сетей мобильной связи для размывания традиционных духовно-нравственных ценностей, навязывания обществу ложных или умышленно искаженных фактов, направленных на подрыв авторитета легитимной власти; использование информационных и коммуникационных технологий в целях оказания деструктивного воздействия на общественно-политическую и социально-экономическую обстановку, а также попытки манипулирования общественным сознанием в государстве – члене ОДКБ и др.

Таким образом, на уровне ОДКБ сформирована организационная структура по обеспечению информационной безопасности, а также разработана необходимая нормативно-правовая база, включающая информационно-психологический компонент. При этом проблема повышения политического статуса вопросов обеспечения собственно информационно-психологической безопасности, нормативно-правового, организационного и непосредственно практического их обособления в общей системе

коллективной информационной безопасности на сегодняшний день стоит достаточно остро. Дело в том, что в настоящее время основными субъектами практической деятельность в области обеспечения информационной безопасности ОДКБ, в том числе в сфере противодействия деструктивному информационному воздействию, выступают силовые структуры государств-членов, реализующие специальные операции в информационном пространстве. Например, проводимые на постоянной основе с 2008 года практические мероприятия по противодействию криминалу в сфере информации (ПРОКСИ). Их главной целью является борьба с информационными потоками, наносящими ущерб национальной и коллективной безопасности стран-участниц ОДКБ в национальных сегментах сети Интернет, которые выражается в блокировке нежелательных информационных сообщений и ресурсов.

При этом следует подчеркнуть, что существующие сегодня различия в национальном законодательстве стран-участниц ОДКБ, создают определенные сложности в выработке общей основы для совместных действий. Российское законодательство содержит наибольшее количество критериев, в соответствии с которыми возможна блокировка информационного ресурса и контента, что во многом определяет позицию представителей России при обсуждении вопросов, касающихся информационно-психологической безопасности, но в национальном законодательстве партнеров аналогичные нормы отсутствуют, что в значительной степени затрудняет выработку консенсуса.

Таким образом, можно сделать вывод о том, что вопросы информационно-психологического противоборства прочно укрепились в политической повестке ОДКБ по обеспечению коллективной безопасности. Комплекс задач, связанных с обеспечением информационно-психологической безопасности, диктует острую необходимость вовлечения в этот процесс, помимо силовых структур, которые в настоящий момент выступают основным субъектами коллективных действий в данной сфере, но и академические сообщества, структуры крупного бизнеса, прежде всего предприятий реального сектора экономики, IT-компании, общественные и некоммерческие организации.

Анализ коллективной политики и модельного законодательства ОДКБ к информационно-психологическим вызовам и угрозам, которые на сегодняшний день имеют безусловный приоритет, позволяет отнести следующие:

- экстремистская и террористическая деятельность в информационной среде;

- производство, публичное распространение и потребление заведомо ложной и (или) вводящей в заблуждение информации;

- внешние целенаправленные попытки ревизии истории и искажения исторической правды, прежде всего, итогов Великой Отечественной войны;

- отсутствие единых принципов регулирования разработки, внедрения и использования информационных систем на основе искусственного интеллекта;

- деструктивные действия, направленные на дискредитацию принципов патриотизма и традиционных духовно-нравственных ценностей государств-членов ОДКБ;

- внешнее деструктивное вмешательство в электоральные процессы.

### 5.3 ШОС и ЕАЭС

ШОС в последние годы особое внимание уделяет вопросам информационной безопасности, так как быстрое развитие технологий создает новые вызовы для стран региона.

ШОС способствует обмену информацией и опытом между государствами-участниками. Это позволяет быстро реагировать на угрозы и делиться лучшими практиками. Например, создание платформы для обмена информацией о киберугрозах позволяет странам оперативно реагировать на инциденты [86].

Регулярные совместные учения в области кибербезопасности помогают укреплять навыки специалистов и повышать готовность к кибератакам. Это особенно важно в условиях растущей угрозы со стороны киберпреступников [87].

Можно выделить ряд недостатков подходов к обеспечению информационной безопасности в ШОС. Например, отсутствие единых стандартов: разные страны имеют различные подходы и стандарты к информационной безопасности [88], что затрудняет совместную работу. Это может приводить к несогласованности действий и снижению общей эффективности. Кроме этого, геополитические разногласия между членами ШОС могут препятствовать полноценному сотрудничеству. Например, конфликты между Индией и Пакистаном или между Китаем и некоторыми центральноазиатскими странами могут затруднять совместные инициатив [89]. Также многие страны-участницы имеют ограниченные бюджеты на кибербезопасность [90], что сказывается на возможности реализации программ и инициатив. Без достаточных ресурсов сложно внедрять современные технологии и обучать специалистов.

ЕАЭС объединяет страны, такие как Россия, Беларусь, Казахстан, Армения и Киргизия. В условиях растущих угроз кибербезопасности для стран-членов, актуализируется вопрос о подходах к обеспечению информационной безопасности в рамках ЕАЭС.

Одним из ключевых преимуществ к обеспечению ИПБ является возможность интеграции усилий стран-участниц в борьбе с киберугрозами. Создание общей системы кибербезопасности позволяет более эффективно отслеживать и предотвращать угрозы. Например, в 2020 году был принят «План действий по обеспечению кибербезопасности» в рамках ЕАЭС.

Кроме этого, страны ЕАЭС имеют возможность обмениваться данными и передовыми технологиями в сфере кибербезопасности, что способствует повышению уровня защищенности. Взаимодействие в области исследований и разработок в кибербезопасности позволяет создавать совместные проекты и инициативы [91].

Тем не менее, разные страны ЕАЭС имеют различный уровень развития информационных технологий и кибербезопасности, что затрудняет интеграцию. Например, Россия значительно опережает другие страны по количеству специалистов и развитию инфраструктуры кибербезопасности (Кабалевский 2023). Вместе с тем, многие страны ЕАЭС сталкиваются с ограниченными ресурсами для реализации программ кибербезопасности. Нехватка финансирования и квалифицированных специалистов может снизить эффективность проводимых мероприятий [92].

### 5.4 БРИКС

В настоящее время БРИКС представляет собой одно из наиболее динамично развивающихся межгосударственных объединений. Его расширение в 2024 г. отчетливо дало понять, что БРИКС постепенно превращается в один из ведущих центров силы, что обусловлено объективным проявлением глобальных трансформаций в мировых политических процессах, связанных с окончательным крушением навязанной странами коллективного Запада после окончания “Холодной войны” однополярного мироустройства.

Сегодня в БРИКС входит 10 стран с быстро растущей экономикой и положительной динамикой рынка информационно-телекоммуникационных технологий. БРИКС представляет собой важный геополитический союз, который активно развивает сотрудничество в различных областях, включая разработку передовых информационных технологий и информационную безопасность.

При этом БРИКС как межгосударственное объединение провозгласил одной из основных целей сотрудничество исключительно в области кибербезопасности, долгое время не выделяя ИИ в особое направление регулирования.

Так, например, в рамках БРИКС были созданы рабочих групп по кибербезопасности, появление которых обеспечило платформу для обсуждения

актуальных угроз и выработки совместных решений [93]. БРИКС также способствовал созданию общей правовой базы для борьбы с киберугрозами, что помогло унифицировать подходы к информационной безопасности. Совместные инициативы по разработке международных норм и стандартов в области кибербезопасности [94] способствуют повышению защищенности стран-участниц.

Также страны БРИКС активно проводят совместные учения и тренинги по кибербезопасности, что повышает готовность и способность быстро реагировать на кибератаки [95]. Эти мероприятия способствуют обмену лучшими практиками и подготовке специалистов в области кибербезопасности.

Колме этого, БРИКС поддерживает международное научное сотрудничество. Для этого, в частности, была создана площадка для обмена идеями и результатами исследований CyberBRICS**.** Разработчики проекта CyberBRICS декларируют три цели: сопоставить существующие нормативные акты; выявить лучшие практики и разработать политические предложения в области регулирования кибербезопасности (включая регулирование персональных данных), политики доступа в Интернет и стратегий цифровизации государственных органов в странах БРИКС [96]. Таким образом, проект призван, прежде всего, разработать правовые и политические механизмы регулирования ИКТ, в частности, ИИ. Это отражает и его структура: проект организован и развивается юридической школой Фонда Жетулиу Варгаса (Бразилия) в партнерстве с Высшей школой экономики в Москве, Центром интернета и общества в Нью-Дели, Университетом Фудань в Шанхае, Гонконгским университетом и Университетом Кейптауна.

Члены CyberBRICS уделяют особое внимание проблемам регулирования персональных данных и управления кибербезопасностью. Защита данных и кибербезопасность стали основными приоритетами Партнерства научно-технических предприятий БРИКС **(**BRICS Science & Technology Enterprise Partnership – STEP). Члены CyberBRICS консультируют все заинтересованные стороны по вопросам развития исследований в области кибербезопасности. С начала 2019 г. постоянно действует интернет-сайт CyberBRICS, на котором публикуются профильные исследования и информация о мероприятиях.

Что касается сотрудничества на пространстве БРИКС в сфере развития технологий ИИ, то, прежде всего, такое взаимодействие развивается между отдельными компаниями и научно-исследовательскими центрами. В частности, в октябре 2023 года Сколтех и Университет Шарджи, ОАЭ, создали совместную ИИ-лабораторию, нацеленную на применение технологий ИИ в биомедицине [39]. А “Сбер”, который разработал специальную технологию распознавания рукописей, получившую название “Digital Петр”,

поскольку она использовалась для расшифровки записей российского императора Петра I, предложил в конце 2023 г. свою помощь Египту для расшифровки древних манускриптов [97].

Однако, к сожалению, существуют и примеры недобросовестного использования юрисдикции отдельных стран БРИКС зарубежными компаниями, которые ведут в них деятельность, которая прямо запрещена у себя в стране. Так, например, в начале 2024 г. правительство Эфиопии через свое инвестиционное подразделение Ethiopian Investment Holdings подписало меморандум о взаимопонимании с компанией Data Center Service, которая является дочерним филиалом гонконгской West Data Group. Это партнерство оценивается в районе 250 млн. долл. и направлено, на первый взгляд, на создание в Эфиопии сложных учебных центров в сфере ИИ. Однако есть основания полагать, что на самом деле это совместное предприятие будет заниматься добычей биткойнов. И это несмотря на то, что правительство страны на официальном уровне выступает против торговли криптовалютами [98].

На наш взгляд, данное обстоятельство связано с тем, что Эфиопия рассматривает технологии ИИ исключительно как крайне эффективный инструмент, способный помочь в решении многих стоявших перед страной социально-экономических задач. В результате, в своем стремлении привлечь большое количество разработчиков ИИ-решений со своими технологиями и вычислительными мощностями правительство Эфиопии взяло курс на создание благоприятных условий для работы иностранных компаний, преимущественно китайских, некоторые из которых оказываются не совсем добросовестными и рассматривают эту страну в качестве удобного места, в котором можно безбоязненно вести деятельность по добыче криптовалюты и торговле ею, которая запрещена в самом Китае.

Это означает, что странам БРИКС необходимо подумать относительно разработке единых стандартов, правил и норм применения технологий ИИ на всем пространстве БРИКС. Однако, до недавнего времени непосредственно тематика, связанная с развитием технологий ИИ в странах БРИКС не становилась самостоятельным предметом обсуждения на форумах, проходящих под эгидой данного Объединения несмотря на то, что вопросы развития информационных технологий нередко поднимались на Саммитах БРИКС.

Так, в частности, в ноябре 2016 г. участники Объединения приняли “Совместную программу развития и план действий по ИКТ”. Но технологии ИИ как самостоятельное направление в Плане не фигурировали. В Йоханнесбургской декларации 2018 г. было отмечено, что Четвертая промышленная революция несет не только несомненные выгоды,

но и новые вызовы и угрозы, связанные с растущим злоупотреблением ИКТ в преступных целях государственными и негосударственными субъектами. А на состоявшемся в 2019 г. саммите БРИКС в Бразилии были закреплены намерения стран БРИКС развивать международное сотрудничество в области обеспечения безопасности в сфере использования ИКТ. Также, появилось сообщение о том, что страны БРИКС планируют создать Альянс по развитию ИИ, основная миссия которого будет заключаться в разработке единых стандартов для технологий ИИ. Однако данная идея на тот момент не получила должного развития. Возможно, впервые Пекинская декларация БРИКС 2022 г. четко подчеркнула обеспокоенность рисками развития ИИ, включая злонамеренное использование ИИ в сфере ИПБ, хотя сами термины в документе не используются. Зато на состоявшемся в следующем 2023 г. в Йоханнесбурге, ЮАР Саммите БРИКС, Председатель КНР Си Цзиньпин однозначно заявил о необходимости расширения сотрудничества в области ИИ, в том числе и по предотвращению рисков, исходящих от этих технологий. В этой связи он предложил сформировать единый подход к использованию и контролю ИИ, и создать совместную структуру управления ИИ.

На саммите в Йоханнесбурге был учрежден специализированный исследовательский комитет в сфере ИИ, благодаря которому страны-участницы Объединения планируют увеличить доступ к технологическим мощностям, необходимым для создания и внедрения ИИ. Предполагается, что эта инициатива будет способствовать развитию инноваций в сфере ИИ на всем пространстве БРИКС. В частности, этот Комитет “сможет проводить оценку наработок на основе ИИ и давать заключение в каких отраслях и какой аудитории можно использовать решение на основе ИИ” [99].

С целью интенсификации дальнейшего переговорного процесса, направленного на формирования единой ИИ-экосистемы БРИКС Россия в декабре 2023 г. внесла предложение включить вопрос внедрения технологий ИИ на пространстве БРИКС в повестку Делового совета БРИКС [100].

Понимая важность данного направления работы, Россия приступила к обсуждению темы, связанной с выработкой совместных подходов в сфере правого регулирования и стандартизации технологий ИИ с отдельными странами БРИКС на двустороннем уровне. Так, в частности, между Россией и Индией еще осенью 2023 г. был подписан Меморандум по созданию межгосударственной российско-индийской системы оценки соответствия технологий ИИ. Результатом работы в этом направлении стала подготовка “Белой книги”, в которой были представлены совместные подходы к стандартизации и этическому регулированию технологий ИИ в здравоохранении и сельском хозяйстве. А между

Россией и Ираном 28 февраля 2024 г. был подписан Меморандум о взаимопонимании Ирана и России в области этики искусственного интеллекта [101].

Следующий раунд обсуждений состоялся на площадке Академического форума БРИКС, который прошел в Москве в период с 22 по 24 мая 2024 г. Одной из, центральной тем Форума стали вопросы дальнейшего развития технологий ИИ, прежде всего, связанные с выработкой единых стандартов, этических норм, правил поведения и направлений дальнейших исследований в этой сфере. Дальнейшее обсуждение этих вопросов произошло на Саммите БРИКС в Казани, состоявшемуся 22-24 октября 2024 г., на котором Президент Путин предложил странам БРИКС объединить усилия в борьбе с недобросовестным применением ИИ. В частности, он предложил регламентировать технологии ИИ и высказал идею создания Альянса БРИКС в области ИИ [102].

Однако, несмотря на, в целом, имеющийся не плохой потенциал для дальнейшего развития технологического сотрудничества, говорить о создании единого рынка передовых информационных технологий на всем пространстве БРИКС пока преждевременно. Обусловлено это тем, что страны Объединения имеют как разный уровень технологического развития, так и различные взгляды на проблему стандартизации и регулирования указанных технологий.

Так Китай, являясь бесспорным лидером среди всех стран БРИКС по развитию искусственного интеллекта, проводит жесткое государственное регулирование любых технологических новаций. России для того, чтобы не остаться на периферии Четвертой промышленной революции, следует активизировать разработку собственных ИИ-решений, восполнив, тем самым, возникший дефицит, связанный с уходом с российского рынка мировых IT-гигантов. Бразилия, наоборот, стремится к сотрудничеству с западными корпорациями, что негативно может сказаться на технологическом суверенитете страны, а ОАЭ поставили перед собой цель превращения в мировой ИИ-хаб. В этой связи они взяли курс на создание благоприятных условий для деятельности иностранных компаний и в целом на привлечение широкого потока зарубежных инвестиций, направленных на развитие технологий ИИ со всего мира: из США, ЕС, Китая, России, других стран. Эфиопия же только пока формирует свою политику в сфере развития ИИ и, принимая во внимание ее общий не очень высокий уровень социально-экономического развития, нельзя сказать, что ИИ является абсолютным приоритетом, несмотря на соответствующие заявления представителей правительства.

Тем не менее, отрадно осознавать, что постепенно проблема создания единой ИИ-экосистемы на пространстве БРИКС становится предметом обсуждения на Саммитах БРИКС. Однако, опираясь на проведенный выше анализ, следует признать, что из-за

различных представлений отдельных стран, входящих в Объединение, о том, каким образом технологии ИИ должны развиваться в обозримой перспективе, выработка подобных единых подходов может потребовать дополнительных раундов обсуждений.

В этой связи более перспективным, на наш взгляд, будет являться, на первом этапе, активизация двустороннего межгосударственного сотрудничества между странами БРИКС, направленное на подписание меморандумов о взаимопонимании по наиболее болезненным и дискуссионным вопросам.

После проведения подобных широкомасштабных обсуждений на двустороннем уровне станет возможным, на следующем этапе, разработать единую ИИ-стратегию стран БРИКС, на основе которой, на заключительном этапе можно будет выработать единые подходы к стандартизации и регулированию технологий ИИ на всем пространстве БРИКС, что, в конечном итоге и приведет к формированию общей ИИ-экосистемы БРИКС.

## 5.5 Оценка преимуществ и недостатков подходов к обеспечению ИПБ общества, принятых в России и интеграционных объединениях, в которых Россия принимает наиболее активное участие (ШОС, ЕАЭС, ОДКБ, БРИКС)

Подходы к обеспечению информационной безопасности в объединениях с участием России имеют как преимущества, так и недостатки.

### 5.5.1 Преимущества подходов к обеспечению ИПБ

1) Многоуровневое и межгосударственное сотрудничество:

Россия использует интеграционные объединения, такие как ШОС и ОДКБ, как платформы для создания согласованных подходов к обеспечению ИПБ, что позволяет развить общие политические и организационные меры. Это особенно важно для реагирования на гибридные угрозы, которые включают информационное и психологическое давление со стороны других государств.

В частности, в рамках ШОС действует Программа сотрудничества по борьбе с терроризмом, сепаратизмом и экстремизмом, ориентированная на обмен информацией между странами-участницами, организацию совместных учений и создание баз данных для мониторинга и нейтрализации потенциальных угроз. В рамках ОДКБ Россия сотрудничает с другими странами для создания общей правовой базы, направленной на защиту от информационного воздействия, подразумевающую юридическую координацию для создания более устойчивого информационного пространства

2) Акцент на уязвимых социальных группах и развитие образовательных программ:

В рамках реализуемого управленческого дискурса наблюдается активная приоретизация молодёжи как одной из основных социальных групп, подверженных деструктивному информационно-психологическому влиянию. Молодёжь восприимчива к манипуляциям в силу возрастных и психологических особенностей, а также в силу большого влияния социальных платформ в их жизни.

Для борьбы с деструктивным влиянием на молодёжь Россия внедряет практики, которые охватывают не только непосредственную защиту, но и профилактику. Российские подходы акцентируют внимание на обучении молодежи способам фильтрации деструктивного контента и на развитии образовательных программ, которые включают элементы психологической устойчивости. В частности, разрабатываются методики выявления деструктивного контента и навыки распознавания ложной информации. Психологическая устойчивость в этом контексте понимается как способность распознавать манипулятивные техники и не поддаваться влиянию.

Россия ретранслирует в международном управленческом дискурсе внимание к молодёжи и её информационной адаптации под деструктивный контент. Например, российские инициативы, реализуемые в рамках БРИКС, включают образовательные форумы и программы для молодежи, такие как Молодежный саммит БРИКС, где обсуждаются вопросы информационной безопасности и цифровой грамотности. Такой подход помогает обеспечить проактивную роль молодёжи в процессе противостояния манипуляциям в цифровой среде. Многостороннее сотрудничество позволяет создать базу для общих стандартов защиты молодёжи в условиях усиленного информационного противоборства.

5.5.2 Недостатки подходов к обеспечению ИПБ

1) Ограниченное влияние на глобальные информационные платформы и цифровые медиаресурсы:

Влияние России и её партнеров в интеграционных объединениях на глобальные цифровые платформы (такие как X и YouTube), которые доминируют в информационном пространстве, остается ограниченным. Это затрудняет реализацию российских и международных стратегий по ИПБ, так как значительная часть деструктивного контента может распространяться через эти платформы из-за рубежа. Такие компании часто подчиняются правилам стран их происхождения, что усложняет возможность ограничения негативного контента в рамках российских законодательных инициатив.

Ограниченные возможности для регулирования глобальных медиаплатформ препятствуют эффективной защите информационного пространства и требуют развития и

популяризации уже существующих собственных национальных платформ для создания альтернативных каналов коммуникации и распространения контента. Однако создание замкнутой информационной экосистемы также ограничивает возможности для международного обмена.

2) Сложности в координации и гармонизации между странами с разными подходами и интересами:

В рамках интеграционных объединений, таких как ШОС и БРИКС, страны-участницы имеют различные взгляды и интересы в вопросах информационной безопасности. Это затрудняет создание единой стратегии ИПБ и может приводить к неэффективности некоторых принятых мер. Различия в законодательных и организационных структурах стран-участниц могут препятствовать унификации стандартов и затруднять реализацию программ, направленных на защиту молодёжи и общества в целом.

Например, в отличие от ЕС, где страны имеют схожие законодательные нормы, в ШОС и БРИКС политические и правовые различия между странами делают согласование подходов трудным процессом. Это усложняет выработку универсальных норм, снижая способность оперативно реагировать на гибридные угрозы и задерживая потенциальную реализацию совместных инициатив.

### 5.5.3 Выводы и рекомендации

Таким образом, подходы России и её партнеров в интеграционных объединениях к обеспечению ИПБ обладают значительными преимуществами, такими как координация на многостороннем уровне, внедрение образовательных технологий для противодействия информационным угрозам, а также акцент на защите молодёжи через усиление её субъектности. Тем не менее, существующие недостатки – ограниченное влияние на глобальные платформы и сложности в координации стран с различными интересами – указывают на необходимость доработки подходов и расширения международного сотрудничества. Успешная реализация стратегий ИПБ требует преодоления барьеров для выработки универсальных стандартов и норм в рамках интеграционных объединений.

Важно стремиться к улучшению баланса между эффективной защитой информации и соблюдением прав граждан, также необходима работа над повышением прозрачности действий государственных органов и улучшением взаимодействия с частным сектором. Многостороннее сотрудничество и совместные учения способствуют повышению уровня безопасности, однако отсутствие единых стандартов и политическая напряженность затрудняют реализацию эффективных мер. Для повышения эффективности работы

организаций в этой области необходимо разработать общие стандарты и обеспечить финансирование программ кибербезопасности.

Для оптимизации работы организаций с участием России в области информационной безопасности рекомендуются следующие меры:

1. Разработка единых стандартов кибербезопасности для всех стран-участниц объединений.
2. Разработка механизмов финансирования совместных программ кибербезопасности.
3. Углубление политического диалога для снижения напряженности между членами организаций.
4. Повышение уровня квалификации специалистов в области киберзащиты, в т.ч. путем многостороннего обмена и стажировок, создания общих обучающих программ для специалистов в области кибербезопасности.

Такой комплексный подход поможет эффективно справляться с вызовами современного мира в области информационной безопасности.

### 5.6 Практические примеры операций обеспечения ИПБ в России и тех интеграционных объединениях, в которых Россия принимает наиболее активное участие (ШОС, ОДКБ, ЕАЭС, БРИКС)

ШОС активно развивает программы по борьбе с экстремизмом, терроризмом и деструктивными нарративами, особенно среди молодёжи. Эти меры позволяют странам-участницам оперативно обмениваться информацией и координировать усилия по обеспечению ИПБ. Операции повышают эффективность в минимизации воздействия экстремистских нарративов. Практическая отработка сценариев по противодействию деструктивному воздействию способствует укреплению взаимодействия между странами, однако остаются проблемы с согласованностью правовых рамок в каждой стране.

В рамках БРИКС Россия развивает инициативы по повышению уровня цифровой грамотности и информационной безопасности среди молодёжи. Примеры включают Молодежный саммит БРИКС и Всемирный фестиваль молодёжи, где обсуждаются вопросы кибербезопасности, цифровой грамотности и информационного суверенитета. В СНГ активно поддерживаются образовательные инициативы для повышения осведомлённости молодёжи о рисках деструктивного контента и развития навыков критического мышления.

Эти программы играют большую роль в долгосрочном укреплении ИПБ. Повышение медиаграмотности и цифровой грамотности способствует тому, что молодёжь

становится более устойчива к манипуляциям и способна отличать достоверную информацию от дезинформации. В результате уменьшается влияние внешнего деструктивного воздействия, а участники таких программ получают возможность критически оценивать цифровой контент. Однако ключевой уязвимостью таких инициатив является их отложенный эффект, не позволяющий оперативно получить результат. Эта особенность адаптивных мер вызвана их накопительным свойством, которое нередко противопоставляется потребности в быстром реагировании.

Также Россия провела онлайн-турнир по кибербезопасности BRICS+ Capture The Flag (BRICS+ CTF). Он прошел в два этапа: первый, отборочный, — 5–6 октября, а финал — 16 ноября 2024 г. В отборочном этапе участвовало 1257 команд из 105 стран мира. В финале соревновались 20 из 8 государств. Из стран – основательниц БРИКС в турнире участвовало 608 команд: российских — 389, индийских — 102, китайских — 98, южноафриканских — 11, бразильских — 8. В топ-10 участников вошли пять российских команд и две китайские.

Как следует из итогового пресс-релиза мероприятия, задания для участников были подготовлены на 13 языках программирования. В финале, прошедшем в формате Attack-Defence, участникам необходимо было обнаружить уязвимости на своем сервере и попытаться закрыть их, не нарушив работоспособности сервисов, и при этом провести атаки на сервера других команд — «захватить флаг» (определенную секретную информацию).

«Поскольку кибербезопасность была названа лидерами стран БРИКС одним из главных вызовов современности, программа турнира BRICS+ CTF, проходящего в год российского председательства в БРИКС, нацелена на формирование кадрового потенциала для обеспечения информационной безопасности Российской Федерации, стран БРИКС и БРИКС+,— говорится в сообщении.— Не случайно турнир вызвал серьезное противодействие среди зарубежных враждебных сил: в ходе отборочного этапа организаторы успешно справились с волновыми атаками на игровую инфраструктуру, отразив более 55 миллионов пакетов за 40 минут» [103].

Международный проект по совершенствованию навыков молодых IT-специалистов имеет одной из целей продвижение России как страны, предлагающей передовые технологии в области информационной безопасности и готовой к сотрудничеству с прогрессивными представителями стран мирового большинства. Вовлечение в российские IT-проекты с международной ориентацией ведущих зарубежных программистов из стран БРИКС+ способствует продвижению задач российской проактивной повестки,

выстраиванию процесса работы с талантливыми зарубежными кадрами и созданию привлекательного образа нашей страны как ведущей технологической державы [103].

В рамках СНГ Россия и другие страны используют специализированные платформы для мониторинга экстремистского и террористического контента (Антитеррористический центр СНГ), включая базы данных по подозрительным аккаунтам, группам и публикациям. Эти меры направлены на предотвращение вовлечения молодёжи в экстремистские движения и обеспечение мониторинга. Однако эффективность таких платформ ограничена сложностью мониторинга закрытых социальных сетей и шифрованных мессенджеров. В условиях увеличивающейся приватности и защиты данных сложно отслеживать деятельность на платформах с ограниченным доступом.

Интересен также и опыт отдельных стран, который может быть учтен при разработке мер по нейтрализации угроз ИПБ России и ее партнеров. В ОАЭ, в частности, разработаны правовые меры противодействия ЗИИИ, в частности, дипфейков. Они в значительной степени зависят от характера и последствий использования дипфейков. Если дипфейки приводят к диффамации, то согласно *Федеральному закону № 31 от 2021 г.* [*Federal Decree-Law No. 31 of 2021 on Promulgating the Crimes and Penalties Law,* 2021] это может быть наказуемо по *статьям 425 или 426*, что может включать тюремное заключение или наложение штрафа. Для осуществления диффамации при использовании цифровых средств, *статья 44 Закона ОАЭ о киберпреступлениях* увеличивает наказание до одного года тюрьмы и/или штрафа от 250 тыс. до 500 тыс. дирхамов за каждое нарушение. Также, если действия, связанные с дипфейками, представляют собой акт мошенничества, то *статья 451 Уголовного кодекса ОАЭ* предполагает наказание в виде лишения свободы или штрафа. При этом, согласно Закону о киберпреступлениях, такое мошенничество может повлечь за собой тюремный срок минимум на год и штраф от 250 тыс. до 1 млн дирхамов. Аналогично, законы предусматривают ответственность за нарушение личной неприкосновенности. Таким образом, использование дипфейков в ОАЭ сопряжено с серьёзными правовыми рисками и может повлечь за собой суровые наказания, включая тюремное заключение. Законы, направленные на защиту частной жизни граждан, репутации и национальной безопасности, отражают решимость государства бороться с угрозами, исходящими от цифровых технологий, используемых в злонамеренных целях.

Эти примеры демонстрируют, что Россия и её партнёры активно работают над обеспечением ИПБ через различные целевые инициативы. Ключевыми факторами их эффективности являются:

1. *Комплексность и многоуровневость*. Программы включают как технические, так и образовательные меры, что обеспечивает интегрированный подход к укреплению ИПБ.
2. *Акцент на превентивные меры*. Программы направлены на повышение цифровой грамотности и молодёжный диалог, что укрепляет защиту общества от деструктивного влияния на долгосрочную перспективу.
3. *Межгосударственное сотрудничество*. Совместные инициативы способствуют обмену передовым опытом и лучшими практиками, что повышает способность государств справляться с новыми угрозами.

Непосредственно практические примеры операций обеспечения ИПБ в России и тех интеграционных объединениях, в которых Россия принимает наиболее активное участие раскрываются в Таблице 4.1:

Таблица 4.1 – Практические примеры операций обеспечения ИПБ в России и тех интеграционных объединениях, в которых Россия принимает наиболее активное участие

| **Международная организация/ структура** | **Инициативы** | **Акценты и риторика России** |
|---|---|---|
| **ООН / ЮНЕСКО** | - Участие в Программе ЮНЕСКО «Информация для всех»<br>- Продвижение международных норм и стандартов в ООН | - Акцент на создании безопасного информационного пространства для молодежи<br>- Взаимодействие в рамках РГОС |
| **БРИКС** | - Молодёжный саммит БРИКС (2024)<br>- Заседание Рабочей группы по безопасности ИКТ (2024) | - Призыв к продвижению цифровой грамотности среди молодежи<br>- Сохранение приверженности мирному использованию ИКТ<br>- Акцент на наращивании взаимодействия в сфере науки, технологий и инноваций |
| **ШОС** | - Программа сотрудничества по борьбе с терроризмом, сепаратизмом и экстремизмом<br>- Программа действий по предупреждению вовлечения молодежи в деструктивные структуры | - Акцент на борьбе с киберугрозами, направленными на молодежь<br>- Поддержка международного сотрудничества в сфере контроля за интернетом<br>- Противодействие использованию информационного пространства для распространения экстремистской идеологии |
| **СНГ** | - Деятельность Антитеррористического центра СНГ<br>- Работа Совета по делам молодежи СНГ | - Поддержка гармонизации правовой базы и практической работы с молодежью<br>- Акцент на адаптации молодежи к современным вызовам и умение распознавать лживую пропаганду |
| **Международные** | - Цифровая гигиена в | - Приверженность международному |

| | | |
|---|---|---|
| **форумы (Всемирный фестиваль молодёжи и др.)** | киберпространстве<br>- Темы цифровых трендов и ментального здоровья | диалогу по защите молодежи<br>- Вовлечение молодежи в обсуждение информационной безопасности<br>- Поддержка создания безопасного информационного пространства для детей и подростков |

Однако, несмотря на наличие такого количества разных программ, следует отметить, что их реализация сталкиваются с целым рядом ограничений:

- *Различие в правовых нормах*. Разные законодательные подходы стран-участниц к регулированию информационного пространства иногда затрудняют унификацию стандартов, что снижает гибкость и оперативность мер.

- *Ограниченные возможности контроля глобальных платформ*. Программы ориентированы на внутренние каналы и системы мониторинга, что затрудняет контроль за деструктивным контентом на глобальных цифровых платформах.

- *Сложность интеграции новых технологий*. Разный уровень технологического развития между странами может ограничивать эффективную интеграцию систем мониторинга и анализа данных.

## ЗАКЛЮЧЕНИЕ

Поставленные в 2024 г. исследовательские задачи были решены в полном объеме. По результатам проведенного исследования были сделаны следующие выводы:

1. На современном этапе стратегической конкуренции все более заметную роль играет целенаправленное деструктивное идеологическое и психологическое воздействие в информационной среде. Поэтому выработка коллективной политики в области обеспечения информационно-психологической безопасности представляется сегодня одним из основных приоритетов государств и их союзов.

2. Когнитивная война – современный вид информационного противоборства, связанный с оказанием деструктивного воздействия на процессы потребления человеком информации и его психику с использованием передовых информационных и нейротехнологий. Способы обеспечения когнитивной безопасности в глобальном измерении связаны с выявлением внутренних связей между глобальными рисками и информационными вызовами и угрозами, возникшими благодаря развитию искусственного интеллекта, росту технологических возможностей анализа больших данных и интенсивному использованию достижений когнитивных наук и технологий. Это, в первую очередь, касается использования когнитивной психологии и лингвистики, нейробиологии и когнитивной антропологии, социологических и культурологических практик, то есть всей палитры естественнонаучных и гуманитарных знаний в военной науке и методов ведения когнитивной войны. Ответные меры на эти деяния заключаются в разработке теоретико-методологических оснований когнитивной безопасности, комплекса когнитивных технологий и практик, издание научной и учебной литературы, подготовка научных кадров, организация научных центров и лабораторий для ведения многопрофильной деятельности.

3. Сегодня необходимо активизировать, подкрепленную философскими и научными исследованиями практическую деятельность федеральных и региональных органов государственной власти по защите от «внешнего деструктивного информационно-психологического воздействия» и «формированию безопасного информационного пространства, защите российского общества от распространения деструктивной идеологии», как это предусмотрено в «Основах государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей (Утверждены Указом Президента Российской Федерации от 9 ноября 2022 г. № 809).

4. Центральную роль в процессе противодействия информационно-психологическим и когнитивным угрозам играет наполнение конкретно-историческим

содержанием сформулированных в нормативно-правовом поле аксиологических концептов, которые, проявляясь в субъективных репрезентациях современной действительности граждан, будут в наибольшей степени соответствовать приоритетам национальной безопасности России.

5. Основа успеха в гибридной войне заключается в психолого-идеологической обработке общества противника, представляющей собой комплекс мероприятий, направленных на подрыв *столпов поддержки* действующей власти путем постепенного перетягивания на свою сторону источников власти от представителей интеллигенции и предпринимателей, чиновников и силовых структур до простых граждан.

6. Ложные новости и дезинформация продолжают оставаться ключевым инструментов при проведении информационно-психологических операций, а возможности генеративного ИИ существенно упрощают задачу создания фейковых новостей, что ведет к окончательной фейковизации современного информационного пространства.

7. Противодействие дальнейшему распространению ложных новостей и дезинформации лежит в трех плоскостях: технической, регуляторной и просветительской. Техническая предполагает разработку программных методов по выявлению фейкового контента. Но проблема заключается в том, что сейчас не существует технологии, способной определить фейки со 100-процентной вероятностью. Регуляторный аспект предполагает ограничить распространение дипфейков на законодательном уровне. Но эти меры также не смогут обеспечить 100% защиту граждан от распространения токсичного контента. Единственный способ, при помощи которого мы можем в определенной степени нивелировать угрозу, исходящую от злонамеренного распространения ложных новостей, заключается в повышении уровня информационной культуры населения и его медиаграмотности. При этом государству необходимо при помощи СМИ и проведения различных специализированных тренингов прививать людям навыки уверенного ориентирования в быстро растущем информационном потоке.

8. Ключевым элементом, способным нивелировать исходящие со стороны стран коллективного Запада гибридных угроз продолжает оставаться всесторонняя поддержка правящей власти со стороны местного населения, поскольку именно проживающие на территории того или иного государства люди и формируют те самые столпы поддержки действующей власти, которые так стремятся разрушить архитекторы «цветных революций» используя для этого различные манипулятивные приемы.

9. Бурное развитие и внедрение технологий ИИ в последние годы подтверждает тот факт, что человечество вступает в очередную промышленную революцию, и

технологические закономерности меняются. Сама природа технологической революции, основанной на ИИ, её огромные возможности и, в то же время, экзистенциальные риски, с которыми сталкивается человечество, впервые потребуют от человека пройти процесс инновационных физических и когнитивных изменений. Обретение новых способностей потребует качественно нового уровня социальной организации и ответственности, чтобы не потерять контроль над технологиями и тем самым избежать наступления технологической сингулярности.

10. Россия сталкивается с внутренними и внешними угрозами информационно-психологической безопасности посредством ЗИИИ. Причем последние явно усиливаются по мере роста международной напряженности, проведения США и их союзниками активной гибридной войны против России. Очевидно, что с развитием систем ИИ в различных государствах вероятность использования конкретных ИИ-технологий злонамеренного воздействия в незаконных целях возрастает. Таким образом, представляется целесообразным развивать международное сотрудничество с целью совместной разработки мер противодействия ЗИИИ, в том числе тех, при которых используются персональные данные, угрожающие безопасности всех стран. К сожалению, такое сотрудничество в крайне напряженной международной обстановке представляется возможным реализовать не на глобальном уровне, а в рамках влиятельных международных объединений и организаций в которых Россия играет важную роль, таких как БРИКС, ШОС, ЕАЭС и ОДКБ и др., не закрывая двери для соглашений в более широких форматах при более благоприятной обстановке.

11. Подходы к обеспечению информационной безопасности в объединениях с участием России имеют как преимущества, так и недостатки. Важно стремиться к улучшению баланса между эффективной защитой информации и соблюдением прав граждан, также необходима работа над повышением прозрачности действий государственных органов и улучшением взаимодействия с частным сектором. Многостороннее сотрудничество и совместные учения способствуют повышению уровня безопасности, однако отсутствие единых стандартов и политическая напряженность затрудняют реализацию эффективных мер. Для повышения эффективности работы организаций в этой области необходимо разработать общие стандарты и обеспечить финансирование программ кибербезопасности.

12. Вопросы информационно-психологического противоборства прочно укрепились в политической повестке ОДКБ по обеспечению коллективной безопасности. Комплекс задач, связанных с обеспечением информационно-психологической безопасности, диктует острую необходимость вовлечения в этот процесс, помимо силовых

структур, которые в настоящий момент выступают основным субъектами коллективных действий в данной сфере, но и академические сообщества, структуры крупного бизнеса, прежде всего предприятий реального сектора экономики, IT-компании, общественные и некоммерческие организации.

13. Локомотивом развития сотрудничества в области ИИ в БРИКС являются, прежде всего, двусторонние соглашения между странами, ориентированные на экономическое сотрудничество. При этом основной акцент делается на применении ИИ в позитивных целях, прежде всего, на поддержке добывающих отраслей, промышленности, здравоохранения.

14. БРИКС как институт, провозгласивший одной из основных целей сотрудничество в области кибербезопасности, не выделяет ИИ в особое направление регулирования, что говорит об определенном отставании осмысления политическими институтами реальной экономической практики. Безусловно, широта рассмотрения проблем ИКТ усиливает механизмы поиска решений на начальном этапе развития. Однако страны БРИКС не только активно осваивают ИИ, но и сталкиваются с рисками и угрозами ИПБ, связанными со злонамеренным использованием ИИ, уже сегодня. ЗИИИ лучше рассматривать в рамках отдельного направления и в силу специфики ИИ (его разнообразия, автономности, самообучаемости и т. п.). На этом фоне ощущается острая нехватка исследований и инициатив в области обеспечения ИПБ на уровне БРИКС (возможно, это связано с трудностью финансирования). Однако организация закрепила в своих декларациях намерение сообща противодействовать злонамеренному использованию ИКТ, и у всех государств-членов есть возможность принять активное участие в разработке общих механизмов противодействия злонамеренному использованию ИИ.

15. Страны БРИКС в совокупности обладают всеми необходимыми знаниями и технологиями, экономическим потенциалом, финансами и, самое главное, компетентными кадрами, должны будут продемонстрировать миру собственные решения и подходы к социально ориентированному использованию технологий ИИ, дающие эффективный ответ на возникающие угрозы. Делать это придется в сложной геополитической ситуации, в условиях нарастающего ускорения глобального хода событий.

Полученные в процессе выполнения заключительного этапа НИР научные результаты могут быть использованы:

1) при разработке коммуникационных стратегий защиты государства или межгосударственного образования, а также предприятий реального сектора экономики от информационно-психологических угроз, при формировании элементов корпоративной

культуры, направленных на предотвращение и минимизацию воздействия террористической пропаганды на сотрудников предприятий,

2) при подготовке аналитических материалов (записок) для органов государственной власти, таких, как Министерство иностранных дел, Министерство обороны, Федеральная служба безопасности,

3) при подготовке правовых и политических документов, в частности документов стратегического планирования (стратегий, концепций и доктрин), в которых затрагиваются проблемы информационно-психологической безопасности как компонента национальной и международной безопасности,

4) при совершенствовании работы специальных групп и подразделений, специализирующихся на борьбе с информационно-психологическими и киберугрозами, как в государственных органах, так и в рамках проектов государственно-частного партнерства в области информационно-психологической безопасности.

Эмпирический материал, выводы и результаты исследования могут быть использованы при создании обобщающих трудов по политологии, социологии, новейшей истории, а также в процессе преподавания курсов политологии, новейшей истории, социологии, спецкурсов по проблемам информационной и информационно-психологической безопасности, терроризма и антитеррористической деятельности.

## СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ


1. Blechman B., Kaplan S. Force Without War: U.S. Armed Forces as a Political Instrument. - Washington, D.C.: Brookings Institution, 1978. – 604 p.

2. Концепция внешней политики Российской Федерации (утверждена Указом Президентом Российской Федерации от 31 марта 2023 №229). - URL: http://www.kremlin.ru/acts/bank/49090 (дата обращения: 16.02.2024).

3. Du Cluzel F. Cognitive Warfare. - Innovation Hub, 2020. – 45 p.

4. Лекторский В.А. О философских проблемах искусственного интеллекта и когнитивных исследований// Философские науки. Том 64. - 2021 . - N 1. - С. 7 - 12 .

5. Доктрина информационной безопасности Российской Федерации (утверждена Указом Президента Российской Федерации от 05.12.2016 № 646) . - URL: http://www.kremlin.ru/acts/bank/41460 (дата обращения: 23.02.2024).

6. Дубровский Д.И. Критический анализ теории сознания Пенроуза-Хамероффа. Часть 2// Философия науки и техники. Том 22. - 2017 . - N 2. - С. 89 - 102 .

7. Krivko M., Bolgov R. Special Aspects of Modern Hybrid Warfare on the Internet: Ontological Analysis and Russian Experience// Proceedings of Topical Issues in International Political Geography / Bolgov R., Atnashev V., Gladkiy Y., Leete A., Tsyb A. and Pogodin S. (eds.) - Springer, Cham, 2021.

8. Hoffman F. Hybrid Threats': Neither Omnipotent Nor Unbeatable// Orbis. Vol. 54. - 2010 . - N 3. – P. 441 - 455.

9. NATO Allied Command Transformation / Bi-SC Input to a New NATO Capstone Concept for the Military Contribution to Countering Hybrid Threats, 2010. - URL: https://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf (дата обращения 17.06.2024).

10. НАТО приняла стратегию против "гибридных войн"/ NewsLand, 2015. - URL: https://newsland.com/post/4854888-nato-priniala-strategiiu-protiv-quotgibridnykh-voinquot (дата обращения 19.03.2024).

11. Безопасная Европа: Противодействие гибридным угрозам / European External Action Service, 2021. - URL: https://eeas.europa.eu/headquarters/headquarters-homepage_ru/46536/Безопасная Европа: Противодействие гибридным угрозам (дата обращения 23.05.2024).

12. Военная доктрина Российской Федерации (утверждена Указом Президентом Российской Федерации от 25 декабря 2014 г. № Пр-2976).

13. Котляр В. К вопросу о «гибридной войне» и о том, кто же ее ведет на Украине// Международная жизнь. - 2015 . - N 8. - С. 57 - 72 .

14. Герасимов В. В. Ценность науки в предвидении// Военно-промышленный курьер. - 2013 . - N 8(476).

15. OM-TV. - URL: https://www.youtube.com/channel/UCkp0Tc7ll67bChomTyB1ezQ (дата обращения 01.07.2024).

16. KhodorkovskyLive. - URL: https://www.youtube.com/@khodorkovskylive (дата обращения 01.07.2024).

17. Дневник депутата. - URL: https://www.youtube.com/@bondarenko_blog (дата обращения 01.07.2024).

18. Соловьиный помет. - URL: t.me/slvn_pomet (дата обращения 01.07.2024).

19. Zorpette E. S. The AI Apocalypse: a Scorecard: How worried are top AI experts about the threat posed by large language models like GPT-4?// IEEE Spectrum. - 2023 . - URL: https://spectrum.ieee.org/artificial-general-intelligence (дата обращения 10.07.2024).

20. Bove T. CEO of Google's DeepMind says we could be 'just a few years' from A.I. that has human-level intelligence// YahooFinance. - 2023 . - URL: https://finance.yahoo.com/news/ceo-google-deepmind-says-could-213237542.html (дата обращения 10.07.2024).

21. Nellis S. Nvidia CEO says AI could pass human tests in five years // Reuters. - 2024 . - URL: https://www.reuters.com/technology/nvidia-ceo-says-ai-could-pass-human-tests-five-years-2024-03-01 (дата обращения 10.07.2024).

22. The AI Index 2024 Annual Report / AI Index Steering Committee, Institute for Human-Centered AI, Stanford University, Stanford, CA, 2024. - URL: https://aiindex.stanford.edu/report (дата обращения 25.06.2024).

23. Бегин А. Статистика искусственного интеллекта (июнь 2024).// ИНКЛИЕНТ. - 2024 . - URL: https://inclient.ru/ai-stats (дата обращения 10.07.2024).

24. Питухина М. А., Гуртов В. А., Белых А. Д. Технологические инновации и применение искусственного интеллекта в развитии мирохозяйственных процессов: опыт стран БРИКС// Вестник Забайкальского государственного университета. Том 30. - 2024 . - N 1. - С. 119 - 129 .

25. Bazarkina D., Mikhalevich E, Pashentsev E., Matyashova D. The Threats and Current Practices of Malicious Use of Artificial Intelligence in Psychological Security in China// The Palgrave Handbook of Malicious Use of AI and Psychological Security / Pashentsev E. (eds.) - Palgrave Macmillan, Cham, 2023. – P. 335-375.

26. Faggella D. AI in China—Recent history, strengths and weaknesses of the ecosystem // Emerj. - 2019 . - URL: https://emerj.com/ai-market-research/ai-in-china-recent-history-strengths-and-weaknesses-of-the-ecosystem (дата обращения 15.06.2024).

27. Козюлин В. Б. Искусственный интеллект в БРИКС: возможна ли синергия?//

Шестая буква БРИКС: Международная безопасность и интересы России. Доклад ПИР-центра / гл. ред. В. А. Орлов – М.: ПИРПРЕСС, 2021. – С. 14-17.

28. Китай стал лидером по цитируемым научным статьям (данные NISTEP и NATURE INDEX) // SecurityLab.ru - 2023. - https://habr.com/ru/articles/683718 (дата обращения 12.08.2024).

29. Hughes S., Bae M., Li M. Hallucination Leaderboard // Github. - 2023 . - URL: https://github.com/vectara/hallucination-leaderboard (дата обращения 25.08.2024).

30. Calvi T. China presents its 'ethical specifications for next-generation artificial intelligence.'// AcuIA - 2021 . - URL: https://www.actuia.com/english/china-presents-its-ethical-specifications-for-next-generation-artificial-intelligence (дата обращения 15.06.2024).

31. Birnbaum E. Trump tech chief criticizes Chinese surveillance in first major international remarks // The Hill - 2019 . - URL: https://thehill.com/policy/technology/469433-trumps-chief-technology-officer-criticizes-chinese-surveillance-in-first (дата обращения 15.06.2024).

32. Bergman J. China: The perfect high-tech totalitarian state // Gatestone Institute - 2019 . - URL: https://www.gatestoneinstitute.org/14365/china-totalitarian- technology (дата обращения 15.06.2024).

33. Каминский Б. Китай представил пятилетний план с акцентом на технологическое доминирование // Forklog - 2021. - URL: https://forklog.com/kitaj-predstavil-pyatiletnij-plan-s-aktsentom-na-tehnologicheskoe-dominirovanie (дата обращения 15.06.2024).

34. Капранов О. Дмитрий Чернышенко: Вклад искусственного интеллекта в ВВП России к 2025 году может составить до 2% // Российская газета - 2023 . – 16 января. – URL: https://rg.ru/2023/01/16/dmitrij-chernyshenko-vklad-iskusstvennogo-intellekta-v-vvp-rossii-k-2025-godu-mozhet-sostavit-do-2.html (дата обращения 15.06.2024) .

35. Faggella D. Artificial Intelligence in India—Opportunities, Risks, and Future Potential. // Emerj. - 2019 . - URL: https://emerj.com/ai-market-research/artificial-intelligence-in-india (дата обращения 15.06.2024).

36. Bazarkina D., Pashentsev E. Malicious Use of Artificial Intelligence: Risks to Psychological Security in BRICS Countries// The Palgrave Handbook of Malicious Use of AI and Psychological Security / Pashentsev E. (eds.) - Palgrave Macmillan, Cham, 2023. – P. 297-334.

37. Brazil AI: Brazil Artificial Intelligence Strategy / Rebellion Research, 2021. - URL: https://www.rebellionresearch.com/brazil-artificial- intelligence- strategy (дата обращения 17.06.2024).

38. UAE Strategy for Artificial Intelligence 2031. - URL: https://ai.gov.ae/strategy (дата обращения: 21.05.2024).

39. ИИ 2024: перспективы и риски // Деловые Эмираты. Выпуск 1/103 - 2024 . - URL: https://www.businessemirates.ae/content/pr/-6/13930 (дата обращения 21.06.2024).

40. Falcon 40B из ОАЭ возглавляет рейтинг: мировой лидер независимой проверки моделей ИИ с открытым кодом Hugging Face // Интерфакс - 2023 . - URL: https://www.interfax.ru/pressreleases/903911 (дата обращения 21.06.2024).

41. Saudi Vision 2030. - URL: https://www.vision2030.gov.sa/en (дата обращения: 21.05.2024).

42. Как в арабских странах развивают и используют искусственный интеллект / Хабр, 2023. - https://habr.com/ru/companies/onlinepatent/articles/749420 (дата обращения 12.08.2024).

43. Каминский Б. Иран заявил о намерении стать лидером в области ИИ // Forklog - 2022. - URL: https://forklog.com/news/ai/iran-zayavil-o-namerenii-stat-liderom-v-oblasti-ii (дата обращения 15.06.2024).

44. Egypt National Artificial Intelligence Strategy. - URL: https://mcit.gov.eg/Upcont/Documents/Publications_672021000_Egypt-National-AI-Strategy-English.pdf (дата обращения: 21.05.2024).

45. Mauritius Artificial Intelligence Strategy. - URL: https://ncb.govmu.org/ncb/strategicplans/MauritiusAIStrategy2018.pdf (дата обращения: 21.07.2024).

46. Government AI Readiness Index 2023 / Oxford Insights. - URL: https://www.mzaghi.com/wp-content/uploads/2024/02/2023-Government-AI-Readiness-Index-2.pdf (дата обращения 25.06.2024).

47. Artificial intelligence in Africa: National strategies and initiatives / DIPLO, 2022. - URL: https://www.diplomacy.edu/resource/report-stronger-digital-voices-from-africa/ai-africa-national-policies (дата обращения 25.06.2024).

48. Summary Report & Recommendations: Presented by the Commission on the Fourth Industrial Revolution // Government Gazette. - 2020. - URL: https://www.gov.za/sites/default/files/gcis_document/202010/43834gen591.pdf (дата обращения 10.07.2024).

49. Akinwamide N. Kudi AI is putting a human feel to online payments in Nigeria. - 2017 . - URL: https://techpoint.africa/2017/02/08/kudi-ai-online-payments-nigeria (дата обращения 10.07.2024).

50. Ndiomewese I. Startup Profile: Lara — get step-by-step public transportation

directions to any destination. - 2017 . - URL: https://techpoint.africa/2017/04/17/lara-profile (дата обращения 10.07.2024).

51. FarmDrive. - URL: https://farmdrive.co.ke (дата обращения 01.07.2024).

52. Sophie Bot. - URL: http://sophiebot.tk (дата обращения 01.07.2024).

53. Agrix Technology. - URL: https://www.agrixtech.com (дата обращения 01.07.2024).

54. Палмер Дж. Молодежь Эфиопии использует потенциал искусственного интеллекта // Cryptopolitan - 2023. - URL: https://www.cryptopolitan.com/ru/молодежь-эфиопии-использует-потенциал-искусственного-интеллекта (дата обращения 15.06.2024).

55. Matuluko M. There is no tech ecosystem in Nigeria – Emeka Okoye, industry veteran // TechpointAfrica - 2017. - URL: https://techpoint.africa/2017/03/16/no-tech-ecosystem-nigeria-emeka-okoye (дата обращения 15.06.2024).

56. Miley J. Google Opens its First African AI Center in Ghana // Interesting Engineering - 2019. - URL: https://interestingengineering.com/innovation/google-opens-its-first-african-ai-center-in-ghanaokoye (дата обращения 15.06.2024).

57. A roadmap for artificial intelligence for development in Africa. - URL: https://ai4d.ai/blog-africa-roadmap (дата обращения 25.06.2024).

58. Data Center Map. - URL: https://baxtel.com/map (дата обращения 25.06.2024).

59. Africa Data Centers. - URL: https://www.africadatacentres.com/about-us (дата обращения 25.06.2024).

60. Indonesia: Artificial Intelligence. - URL: https://asiasociety.org/policy-institute/raising-standards-data-ai-southeast-asia/ai/indonesia (дата обращения: 18.09.2024).

61. Kata.ai. - URL: https://kata.ai/products/kata-platform (дата обращения 18.09.2024).

62. Indonesia’s Silicon Valley. - 2021. - URL: https://www.thejakartapost.com/academia/2021/04/29/indonesias-silicon-valley.html (дата обращения: 18.09.2024).

63. Еременко П. Крушение Боинга в Эфиопии: виноват искусственный интеллект. - 2019 . - URL: https://dzen.ru/a/XInf3tku5wCzBv4S (дата обращения 10.07.2024).

64. Azamfiery R., Kudchadkar S. R., Fackler J. Large language models and the perils of their hallucinations // Critical Care. 2023. - Vol. 27. - URL: https://ccforum.biomedcentral.com/articles/10.1186/s13054-023-04393-x (дата обращения 17.08.2024).

65. Iwugo D. Large Language Models and Cybersecurity – What You Should Know.-

2023 . - URL: https/www.freecodecamp.org/news/large-language-models-and-cybersecurity (дата обращения 15.08.2024).

66. Лактюшин Н. Дипфейки в Китае заменили стримеров: торгуют онлайн без перерывов и выходных // @Hi-tech - 2022. - URL: https://hi-tech.mail.ru/news/103040-dipfejki-v-kitae-zamenili-strimerov-torguyut-onlajn-bez-pereryivov-i-vyihodnyih (дата обращения 15.06.2024).

67. Китайская Tencent научилась создавать клонов людей за 24 часа [Электронный ресурс]. - https://www.securitylab.ru/news/537879.php (дата обращения 12.08.2024).

68. Иванов В. Г., Игнатовский Я. Р. Deepfakes: применение в политике и угрозы для личности и национальной безопасности // РУДН. Серия: Государственное и муниципальное управление. - 2020 . Вып.: 7. - N 4. - С. 379 - 386 .

69. The Conversation Weekly podcast ‘Deepfakes and disinformation swirl ahead of Indonesian election. - 2024. - URL: https://cdn.theconversation.com/static_files/files/3074/Indonesia_Deepfakes_Transcript.docx.pdf?1709054499) (дата обращения 16.09.2024).

70. Lee C. Unmasking hypnotized AI: The hidden risks of large language models // SecurityIntelligence - 2023 . - URL: https://securityintelligence.com/posts/unmasking-hypnotized-ai-hidden-risks-large-language-models (дата обращения 15.07.2024).

71. Линдре Ю. Так ли страшен ChatGPT и аналогичные ему большие языковые модели? // РСМД. - 2023 . - URL: https://russiancouncil.ru/analytics-and-comments/analytics/tak-li-strashen-chatgpt-i-analogichnye-emu-bolshie-yazykovye-modeli (дата обращения 10.07.2024).

72. Pashentsev E. Malicious Use of AI and Challenges to Psychological Security: Future Risks // RIAC. - 2024 . - URL: https://russiancouncil.ru/en/analytics-and-comments/analytics/malicious-use-of-ai-and-challenges-to-psychological-security-future-risks (дата обращения 10.07.2024).

73. GPT-5 – чего ожидать от новой модели от OpenAI? Возможности и потенциал искусственного интеллекта / Хабр, 2024. - https://habr.com/ru/companies/ru_mts/articles/804591 (дата обращения 12.08.2024).

74. Kim W. C., Mauborgne R. Blue Ocean Strategy. - Harvard Business Press Books, 2015. – 320 p.

75. McAuliffe M., Blower J. Migration, mobility and digital technology in a post-COVID-19 world: initial reflections on transformations underway // Research handbook on international migration and digital technology / - Edward Elgar Publishing, 2021. – P. 406-422.

76. Holleran M., Notting M. Mobility guilt: Digital nomads and COVID-19 // Tourism

Geographies - 2023 . - N 25(5). - P. 1341-1358 .

77. Лещенко Ю. Г. Национальные интересы в контексте обеспечения экономической безопасности государства в условиях глобальной интеграции: эволюционно-теоретический аспект // Вопросы инновационной экономики. Том 10. - 2020 . - N 10. - С. 2375-2390 .

78. Yannakogeorgos P. A. Internet governance and national security // Strategic Studies Quarterly. Vol. 6. - 2012 . - N 3. - P. 102-125 .

79. Cattaruzza A., Danet D., Taillat S., Laudrain A. Sovereignty in cyberspace: Balkanization or democratization// 2016 International Conference on Cyber Conflict (CyCon US). - IEEE, 2016.

80. Munn L. Porous Territories: The Internet Beyond Borderless Versus Balkanized// Glocalism: Journal of Culture. Politics and Innovation. Vol 1. - 2020. URL: http://dx.doi.org/10.12893/gjcpi.2020.1.3.

81. Frieden R. Without public peer: the potential regulatory and universal service consequences of Internet Balkanization. - 1998 . - URL: http://dx.doi.org/10.2139/ssrn.102927 (дата обращения 15.06.2024).

82. Sagawa P.I. The balkanization of the Internet // The McKinsey Quarterly. - 1997 . - N 1.

83. Srnicek N. Platform capitalism. - John Wiley and Sons, 2017. – 120 p.

84. Zuboff S. . The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. - Public Affairs, 2019. – 704 p.

85. Taylor R.D. “Data localization”: The Internet in the balance// Telecommunications Policy. Vol. 44. - 2020 . - N 8. - P. 102-108 .

86. Ислаев А. Киберугрозы и безопасность: опыт ШОС// Журнал международной безопасности - 2020 . - N 2(3). - С. 45-56.

87. Петров В. Совместные учения по кибербезопасности в ШОС: анализ и результаты// Национальная безопасность и военное искусство - 2021 . - N 1(4). - С. 67-75.

88. Кузнецов Р. Единые стандарты в области кибербезопасности: необходимость для ШОС// Аналитический обзор безопасности - 2023 . - N 4(1). - С. 12-19.

89. Морозов С. Геополитические аспекты сотрудничества в ШОС// Вопросы геополитики - 2021 . - N 2(5). - С. 88-95.

90. Тарасов Е. Финансирование кибербезопасности в странах ШОС: текущие проблемы// Экономика безопасности - 2022 . - N 3(6). - С. 54-60.

91. Бурцев А. Взаимодействие стран ЕАЭС в области кибербезопасности// Журнал международной безопасности - 2021 . - N 5(3). - С. 32-45.

92. Иванов Е. Финансирование программ кибербезопасности в ЕАЭС: текущие проблемы и перспективы// Экономика безопасности – 2021 . - N 2(3). - С. 30-39.

93. Ковалев А. Кибербезопасность в БРИКС: новые подходы и инициативы// Журнал международной безопасности - 2022 . - N 5(2). - С. 23-34.

94. Чжун Л. Киберугрозы и безопасность: опыт ШОС// Правовая база кибербезопасности в странах БРИКС - 2023 . - N 6(1). - С. 12-18.

95. Иванов Е. Совместные учения по кибербезопасности в БРИКС: практический опыт// Научный вестник безопасности – 2021 . - N 4(3). - С. 45-55.

96. CyberBRICS. - URL: https://cyberbrics.info/about-us (дата обращения 03.10.2024).

97. “Сбер” займется расшифровкой древних египетских манускриптов// RBK. - 2023. - URL: https://www.rbc.ru/technology_and_media/20/11/2023/655b72fc9a79473e111934726/13930 (дата обращения 21.06.2024).

98. Эфиопия приступает к реализации проекта в области данных и искусственного интеллекта стоимостью 250 миллионов $ с гонконгской фирмой // Coin Edition. - 2024. - URL: https://coinedition.com/ru/эфиопия-приступает-к-реализации-прое (дата обращения 21.08.2024).

99. БРИКС сформирует общую структуру управления ИИ. Что ждет стран-участниц?// Искусственный интеллект Российской Федерации. - 2023. - URL: https://ai.gov.ru/mediacenter/briks-sformiruet-obshchuyu-strukturu-upravleniya-ii-chto-zhdet-stran-uchastnits- (дата обращения 21.08.2024).

100. Уварчев Л. РФ предложила включить вопрос внедрения технологий ИИ в повестку Делового совета БРИКС // Коммерсант. - 2023 . - URL: https://www.kommersant.ru/doc/6397157 (дата обращения 10.07.2024).

101. Меморандум о взаимопонимании России и Ирана в области этики искусственного интеллекта. - URL: https://overclockers.ru/blog/BulgarNews/show/145021/Memorandum-o-vzaimoponimanii-Irana-i-Rossii-v-oblasti-etiki-iskusstvennogo-intellekta (дата обращения: 16.08.2024).

102. Путин предложил странам БРИКС вместе бороться с недобросовестным применением ИИ // ТАСС. - 2024. - URL: https://tass.ru/ekonomika/22198879?ysclid=m3pc4dcy2k7975112 (дата обращения 29.10.2024).

103. Черненко Е. Россия провела крупный турнир по кибербезопасности с участием стран БРИКС // Коммерсант. - 2024 . - URL: https://www.kommersant.ru/doc/7310233 (дата обращения 23.11.2024).