МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ КАЗЕННОЕ УЧРЕЖДЕНИЕ
«ГЛАВНЫЙ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЙ ЦЕНТР»

ОБЗОР ОТДЕЛЬНЫХ ВОПРОСОВ В ОБЛАСТИ БОЛЬШИХ ДАННЫХ И ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

VI ВЫПУСК

МОСКВА 2021

Обзор отдельных вопросов в области
больших данных и искусственного интеллекта.
VI выпуск.
М.: ФКУ «ГИАЦ МВД России», 2021. – 338 с.

В обзоре представлены материалы, касающиеся вопросов использования больших данных и развития искусственного интеллекта в мире. Отдельно отражены актуальные вопросы использования ИИ в правоохранительной системе.

ОГЛАВЛЕНИЕ

UNITED NATIONS
OFFICE OF COUNTER-TERRORISM
UN Counter-Terrorism Centre (UNCCT)

unicri
United Nations
Interregional Crime and Justice
Research Institute

АЛГОРИТМЫ И ТЕРРОРИЗМ: ЗЛОНАМЕРЕННОЕ ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ТЕРРОРИСТИЧЕСКИХ ЦЕЛЯХ

Перевод с английского совместного доклада ЮНИКРИ
и Контртеррористического центра ООН

Отказ от ответственности

Мнения, выводы, заключения и рекомендации, изложенные в настоящем документе, не обязательно отражают мнения Организации Объединенных Наций, правительства Королевства Саудовской Аравии или любых других заинтересованных национальных, региональных или глобальных организаций.

Используемое обозначение и материалы, представленные в этой публикации, не подразумевают выражения какого-либо мнения со стороны Секретариата Организации Объединенных Наций относительно правового статуса какой-либо страны, территории, города или района ее властей или относительно делимитации ее границ.

Содержание этой публикации может цитироваться или воспроизводиться при условии, что источник информации подтвержден. Авторы хотели бы получить копию документа, в котором используется или цитируется эта публикация.

Благодарности

Настоящий доклад является результатом совместной исследовательской инициативы по борьбе с терроризмом в эпоху искусственного интеллекта Группы кибербезопасности и новых технологий Контртеррористического центра Организации Объединенных Наций (КТЦООН) Управления Организации Объединенных Наций по борьбе с терроризмом (ЮНОКТ)

и Межрегионального научно-исследовательского института Организации Объединенных Наций по вопросам преступности и правосудия (ЮНИКРИ) через его Центр искусственного интеллекта и робототехники. Совместная исследовательская инициатива финансировалась за счет щедрых взносов Королевства Саудовской Аравии.

Предисловие

За последнее десятилетие мы стали свидетелями быстрого внедрения решений в области искусственного интеллекта (ИИ) в различных отраслях промышленности, как в государственном, так и в частном секторах. Прогнозируется, что к 2025 году мировой рынок ИИ превысит 100 миллиардов долларов и системы с поддержкой ИИ будут продолжать поддерживать многие сектора – здравоохранение, образование, торговлю, банковские и финансовые услуги, критически важную инфраструктуру и безопасность, среди многих других.

Генеральный секретарь Организации Объединенных Наций Антониу Гутерриш в своей Стратегии по новым технологиям на 2018 год заявил: «Хотя эти технологии имеют большие перспективы, они не свободны от рисков, а некоторые вызывают беспокойство и даже страх. Они могут быть использованы в злонамеренных целях или иметь непреднамеренные негативные последствия». Потенциальные преимущества ИИ для человечества неоспоримы, и все же исследования по вредоносному использованию ИИ все еще находятся в зачаточном состоянии.

Было замечено, что террористы являются ранними приверженцами новых технологий, которые, как правило, недостаточно регулируются и управляются, и ИИ не является исключением. Учитывая международные связи и трансграничные последствия многих технологических систем, региональный и международный подход становится жизненно важным для обеспечения того, чтобы террористы не имели возможности использовать пробелы в регулировании, которые могут выявить уязвимости в системах ИИ.

Нам необходимо создать устойчивые структуры управления, которые могли бы быстро и эффективно реагировать и смягчать последствия злонамеренного использования ИИ террористами.

Организация Объединенных Наций отвечает на эту потребность широким спектром инициатив. Дорожная карта Генерального секретаря по цифровому сотрудничеству определяет «Поддержку глобального сотрудничества в области искусственного интеллекта» в качестве одной из восьми ключевых областей действий. В соответствии с этой Дорожной картой Контртеррористический центр Организации Объединенных Наций при Управлении Организации Объединенных Наций по борьбе с терроризмом также реагирует на эту проблему в рамках своей Глобальной контртеррористической программы по кибербезопасности и новым технологиям.

Этот доклад, разработанный совместно с Межрегиональным научно-исследовательским институтом Организации Объединенных Наций по вопросам преступности и правосудия, должен послужить ранним предупреждением о возможном злонамеренном использовании и злоупотреблении ИИ террористами и помочь мировому сообществу, промышленности и правительствам активно подумать о том, что мы можем сделать коллективно, чтобы обеспечить использование новых технологий во благо, а не во вред.

Я хотел бы воспользоваться этой возможностью, чтобы поблагодарить международных экспертов, которые участвовали в разработке рекомендаций этого доклада. Мое Управление готово оказать поддержку государствам-членам и другим партнерам по борьбе с терроризмом в противодействии угрозе ИИ со стороны террористов.

Владимир Воронков Заместитель Генерального секретаря
Управление Организации Объединенных Наций по борьбе с терроризмом Исполнительный директор Контртеррористического центра Организации Объединенных Наций

Предисловие

Искусственный интеллект (ИИ), возможно, является квинтэссенцией новейших технологий нашего времени. Вот уже несколько лет Межрегиональный научно-исследовательский институт Организации Объединенных Наций по вопросам преступности и правосудия через свой Центр ИИ и робототехники изучает ИИ и то, что мы увидели, является чрезвычайно многообещающим. В контексте сегодняшнего дня ИИ, например, сыграл определенную роль в содействии значительному ускорению разработки вакцин на основе рибонуклеиновой кислоты – мессенджера (мРНК), подобных тем, которые в настоящее время используются для сдерживания пандемии COVID-19. В наших работах в области правосудия, предупреждения преступности, безопасности и верховенства закона мы видели многообещающие применения ИИ, в том числе его способность помогать находить давно пропавших детей, сканировать незаконную секс-рекламу для выявления и пресечения сетей торговли людьми, а также выявлять финансовые транзакции, которые могут указывать на отмывание денег.

Но мы также видели и темную сторону ИИ – сторону, которой не уделялось столько внимания и которая остается недостаточно изученной. Реальность такова, что ИИ может быть чрезвычайно опасным, если его использовать со злым умыслом. Обладая проверенным опытом в мире киберпреступности, это мощный инструмент, который, возможно, может быть использован для содействия терроризму и насильственному экстремизму, способствующим терроризму, например, путем предоставления новых способов физических атак с помощью беспилотных летательных аппаратов или самоуправляемых автомобилей, усиления кибератак на критически важную инфраструктуру или обеспечения более быстрого и эффективного распространения разжигания ненависти и подстрекательства к насилию.

Является ли ИИ будущим терроризма? Как указывается в настоящем докладе, это еще предстоит выяснить. И все же мы никогда не должны забывать, что терроризм – это развивающаяся угроза, которую не следует

недооценивать. Более двух десятилетий в 21 веке мы видели множество примеров того, как террористы обращаются к новым и появляющимся технологиям, таким как беспилотные летательные аппараты, виртуальные валюты и социальные сети. Поскольку ИИ становится все более доступным, крайне важно быть на шаг впереди и быть готовым к любым неожиданностям, связанным с его неправильным использованием.

Поэтому мы с гордостью представляем этот доклад совместно с Контртеррористическим центром Организации Объединенных Наций в Управлении Организации Объединенных Наций по борьбе с терроризмом, что стало возможным благодаря щедрой поддержке Королевства Саудовская Аравия. Мы надеемся, что это станет началом разговора о злонамеренном использовании ИИ в террористических целях.

Антония Мари Де Мео Директор
Межрегионального научно-
исследовательского института
Организации Объединенных Наций по
вопросам преступности и правосудия

Резюме

Новые технологии и искусственный интеллект (ИИ), в частности, могут быть чрезвычайно мощными инструментами, позволяющими добиться больших успехов в медицине, информационных и коммуникационных технологиях, маркетинге, транспорте и многих других областях исследований. Однако, они также могут быть использованы в злонамеренных целях, когда попадают в чужие руки. Цель этого доклада – *Алгоритмы и терроризм: Злонамеренное использование искусственного интеллекта в террористических целях* – способствовать пониманию потенциального риска попадания ИИ в руки террористов.

Хотя террористические организации в определенной степени традиционно склонны использовать различные формы «низкотехнологичного терроризма», такие как огнестрельное оружие, лезвия и транспортные средства, терроризм сам по себе не является постоянной угрозой. Как только ИИ получит более широкое распространение, барьеры для входа будут снижены за счет сокращения навыков и технических знаний, необходимых для его использования. Поэтому вопросы, на которые стремится ответить этот доклад, заключаются в том, станет ли – или, возможно, лучше «когда» – ИИ инструментом в арсенале терроризма и, если это произойдет, чего может разумно ожидать международное сообщество.

Настоящий отчет состоит из девяти глав:

В первой главе представлен общий обзор, в котором приводятся статистические данные, демонстрирующие растущую озабоченность экспертов по поводу злонамеренного использования этой технологии, в том числе террористами.

Глава вторая описывает общий ландшафт ИИ. Он начинается с определения ИИ и связанных с ним терминов, включая машинное обучение и глубокое обучение, а также такие понятия, как узкий и общий интеллект. Затем в нем дается обзор различных областей, в которых в настоящее время используются алгоритмы и приложения ИИ, такие как обработка естественного языка и распознавание изображений, а также возможные будущие тенденции в использовании этой технологии.

В третьей главе демонстрируется потенциальная угроза использования террористическими группами и отдельными лицами новых технологий, приводя несколько примеров террористических атак, в которых такие технологии, как Интернет и социальные сети, были ценными и мощными инструментами.

В четвертой главе предпринята попытка дополнительно контекстуализировать злонамеренное использование ИИ путем изучения трех категорий угроз – кибернетических, физических и политических, – которые

были определены в существующей литературе, чтобы продемонстрировать, как ИИ может быть использован в малийских целях.

В пятой главе рассматривается вопрос о том, может ли терроризм с использованием ИИ быть мыслимой реальностью или это не более чем научная фантастика. С этой целью в нем представлены примеры террористических групп, которые продемонстрировали интерес к ИИ или связанным с ним технологиям, в том числе к видео с использованием распознавания лиц или беспилотных летательных аппаратов, также известных как «дроны».

Вслед за этим в шестой главе содержится подробный обзор нынешнего и возможного будущего злонамеренного использования ИИ террористическими группами и отдельными лицами. Этот обзор включает как пользователей-злоумышленников, которые задокументированы и были выявлены в ходе исследований, так и тех, которые, несмотря на отсутствие доказательств или литературы, могут стать реальностью в будущем.

В седьмой главе представлены три вымышленных сценария для поддержки визуализации того, как ИИ может быть злонамеренно использован в террористических целях. Эти сценарии сосредоточены на использовании подбора паролей с использованием ИИ, программ-вымогателей, беспилотных летательных аппаратов с распознаванием лиц, подделок и измененных паспортов, доступных через подпольный форум в бизнес-модели «преступление как услуга».

Основываясь на информации, представленной в предыдущих главах, в восьмой главе оценивается есть ли основания для беспокойства по поводу террористических групп и отдельных лиц, непосредственно использующих ИИ, например, для улучшения или усиления атаки. В этой связи анализируются понятия намерения и способности для достижения объективных выводов.

Глава девятая подводит отчет к завершению, предлагая ряд рекомендаций для органов по борьбе с терроризмом и правоохранительных органов, а также для директивных органов, промышленности и научных кругов, которые следует

рассмотреть на будущее, и предлагая несколько последующих действий по наращиванию потенциала для подготовки к возможному будущему терроризма с использованием ИИ.

При подготовке настоящего доклада УНП ООН и ЮНИКРИ опирались в основном на кабинетные исследования и информацию из открытых источников, такую как статьи, официальные отчеты и сообщения средств массовой информации. Совещание Группы экспертов было фактически организовано 9 февраля 2021 года, чтобы дополнить выводы, сделанные на основе информации из открытых источников, и собрать информацию для представленных стратегических рекомендаций и последующих действий.

I. ВСТУПЛЕНИЕ

Искусственный интеллект (ИИ) – мощный инструмент. Он используется во всем государственном и частном секторах, чтобы сделать людей и общество в целом счастливее, здоровее, богаче и безопаснее. Генеральный секретарь Организации Объединенных Наций Антониу Гутерриш указал, что при надлежащем использовании и закреплении ценностей и обязательств, определенных Уставом Организации Объединенных Наций и Всеобщей Декларацией прав человека, ИИ может сыграть определенную роль в выполнении Повестки дня в области устойчивого развития на период до 2030 года, способствуя искоренению нищеты, защите планеты и обеспечению мира и процветания для всех. Тем не менее, ИИ может иметь и темную сторону: как технология общего назначения, ИИ может в равной степени использоваться злоумышленниками. В недавнем докладе Европола, Trend Micro и ЮНИКРИ были освещены некоторые из многих способов, которыми киберпреступники уже используют ИИ как вектор атаки, так и поверхность атаки. Точно так же, как ИИ может использоваться в преступных целях, он также может злонамеренно использоваться группами и отдельными лицами для повышения интенсивности террористических атак или для усиления потенциала этих групп или отдельных лиц

для распространения экстремистской пропаганды и подстрекательства к насилию.

В августе 2020 года MIT Technology Review Insights опросил 301 старшего бизнес-лидера и академика по широкому кругу вопросов, связанных с ИИ, включая их опасения по поводу ИИ. Опрос показал, что, хотя такие проблемы, как отсутствие прозрачности, предвзятость, отсутствие управления при разработке ИИ и возможность автоматизации, способной вызвать значительную безработицу, были источником беспокойства, участники больше всего беспокоились о том, что ИИ попадет в чужие руки.

Исследование, проведенное Контртеррористическим центром Организации Объединенных Наций (КЦООН) Управления Организации Объединенных Наций по борьбе с терроризмом (ЮНОКТ) и ЮНИКРИ через его Центр искусственного интеллекта и робототехники на Совещании Группы экспертов, призванном рассмотреть и утвердить настоящий доклад, продемонстрировало аналогичную озабоченность. Из 27 представителей правительства, промышленности, научных кругов и международных и региональных организаций 44% считают, что злонамеренное использование ИИ в террористических целях «очень вероятно», а 56% считают, что это «несколько вероятно». Что характерно, ни один из опрошенных участников не счел, что злонамеренное использование ИИ таким образом «маловероятно».

В ходе обсуждения, последовавшего за опросом, участники определили четыре фактора, которые в значительной степени способствовали их озабоченности по поводу потенциального злонамеренного использования ИИ в террористических целях:

Во-первых, «демократизация» новых технологий, таких как ИИ. Понятие «демократизация» относится к тому факту, что то, что когда-то было исключительно передовой технологией, понимаемой и используемой только очень ограниченным сообществом, обладающим существенными ресурсами и опытом, становится все более доступным для всех и может использоваться

без крупных инвестиций или даже с ограниченными техническими знаниями. На самом деле, многие из наиболее популярных алгоритмов уже имеют открытый исходный код и не требуют исключительно высокого уровня знаний для использования. Несмотря на то, что демократизация технологий в целом может стать движущей силой развития и процветания, в результате риск возможного злонамеренного использования в равной степени возрастает. Более того, учитывая также возможность аутсорсинга таких групп в форме все более актуальной бизнес-модели «преступление как услуга», используемой преступными группами, которая «стимулирует цифровую подпольную экономику, предоставляя широкий спектр коммерческих услуг, которые облегчают практически любой тип киберпреступности», барьеры для входа в использование ИИ были значительно снижены для субъектов со злым умыслом.

Во-вторых, масштабируемость ИИ. Масштабируемость можно понимать как способность технологии «расти» в размерах или объеме и управлять возросшим спросом. Как правило, масштабируемость относится к тому, чтобы сделать часть технологии больше и шире с точки зрения ее использования. Участники отметили, что в свете особенно масштабируемого характера ИИ тем, кто отвечает за защиту от потенциального вредоносного использования ИИ, придется готовиться и защищаться не только от угрозы отдельных атак, но и от увеличения объема атак в любой момент времени. Ярким примером этого является угроза автономных полетов беспилотных летательных аппаратов.

В-третьих, присущая терроризму/борьбе с терроризмом асимметрия. Было высказано предположение, что даже если злонамеренное использование ИИ в террористических целях не удастся из-за, например, отсутствия технического опыта у отдельных злоумышленников, все равно может быть значительное психологическое воздействие с точки зрения внушения страха. Например, неудачный взрыв бомбы, тем не менее, несет в себе мощный сигнал. В то же время эта асимметрия проявляется в проблемах, с которыми

сталкиваются контртеррористические организации и террористы в связи с использованием ИИ. Для многих организаций, стремящихся использовать ИИ, требуется тщательное рассмотрение его использования для обеспечения гражданских свобод и основных прав и свобод человека. Однако злоумышленники, такие как террористические группы и отдельные лица, скорее всего, не будут зацикливаться на таких проблемах, тем самым во многих отношениях упрощая их возможное использование ИИ.

В-четвертых, растущая зависимость общества от данных и технологий. Было отмечено, что общество в целом все больше зависит от целостности и доступности Интернета и надежности данных для его функционирования. Благодаря прогрессу в области ИИ в последние годы наблюдается быстрая интеграция ИИ в повседневную жизнь с помощью интеллектуальных устройств и интеллектуальных городов, включая критически важные инфраструктуры, такие как медицинские учреждения, поставщики энергии, биологические и ядерные объекты. Хотя это дает много преимуществ, это в равной степени представляет повышенную уязвимость к кибератакам с поддержкой ИИ или более традиционным атакам на системы ИИ в рамках таких инфраструктур или данных, на которых работают эти системы.

Хотя, как будет описано в этом отчете, нет четких доказательств или указаний на фактическое прямое использование ИИ террористическими организациями, можно опираться и учиться на тенденциях и событиях в области злонамеренного использования ИИ в других областях – в частности, киберпреступники, которые уже давно являются первыми пользователями технологий. В этой связи, а также учитывая экспоненциальный рост индустрии ИИ в последние годы и вышеперечисленные факторы, потенциал злонамеренного использования этой технологии в террористических целях заслуживает пристального внимания международного сообщества в будущем.

II. ЧТО ТАКОЕ ИИ?

Чтобы понять, как можно использовать ИИ или, в зависимости от обстоятельств, как его можно использовать не по назначению в террористических целях, важно начать с установления основополагающего понимания самой технологии.

1. Ключевая терминология и основные понятия

ИИ – это область компьютерных наук, посвященная теории и разработке компьютерных систем, способных выполнять задачи, обычно требующие человеческого интеллекта, такие как визуальное восприятие, распознавание речи, перевод с одного языка на другой, принятие решений и решение проблем. Этими интеллектуальными системами могут быть, например, программные приложения, роботы и автономные автомобили. ИИ – это обобщающий термин, включающий множество различных подполей, наиболее заметные из которых описаны ниже.

Машинное обучение – это область ИИ, которая включает алгоритмы, которые могут «учиться» на основе данных, т.е. постепенно повышать производительность при выполнении конкретной задачи. В отличие от других компьютерных программ, алгоритмы машинного обучения не требуют явных инструкций от людей. Вместо этого они извлекают шаблоны и изучают неявные правила из значительного числа примеров, включенных в базу данных. Таким образом, система ИИ может включать алгоритм машинного обучения для выполнения определенной задачи, а также датчики и внешние устройства, необходимые для выполнения этой задачи. Например, система ИИ компьютерного зрения состоит из программного обеспечения для распознавания изображений и одной или нескольких камер для захвата изображения, которое будет обрабатываться алгоритмом.

Глубокое обучение, в свою очередь, является подразделом машинного обучения, которое имеет дело с меньшим семейством алгоритмов, известных как нейронные сети. Это алгоритмы, вдохновленные человеческим мозгом,

которые стремятся учиться на больших объемах данных, выполняя задачу многократно, каждый раз внося незначительные изменения в ее внутренние функции для улучшения результата. Термин «глубокое обучение» происходит от нескольких (или «глубоких») слоев нейронной сети.

На изображении ниже показана взаимосвязь между ИИ, машинным обучением и глубоким обучением

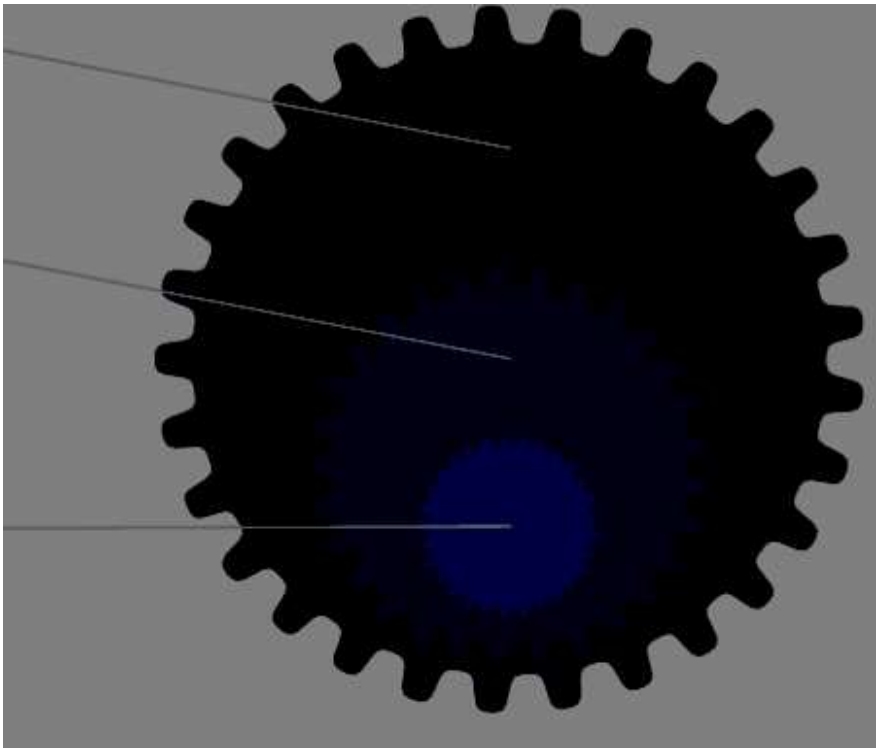

Рисунок 1.

Существующие сегодня системы ИИ состоят из так называемых «узких» приложений ИИ. Это системы ИИ, запрограммированные на выполнение одной задачи, такой как прогнозирование погоды, игра в шахматы или анализ медицинских изображений. В результате их «узкого» программирования эти системы плохо работают за пределами одной задачи, для выполнения которой они предназначены.

Однако, преуспевая в выполнении конкретных задач, эти системы могут выступать в качестве строительных блоков более интеллектуальных систем ИИ, которые могут быть разработаны в ближайшем будущем.

В связи с этим еще одним понятием, обычно возникающим в литературе, является искусственный общий интеллект (ИОИ), который относится к системам, способным успешно выполнять любую интеллектуальную задачу, на которую способен человек. В отличие от узкого ИИ, который специально создан для выполнения ограниченной задачи, ИОИ сможет учиться, планировать, рассуждать, общаться на естественном языке, интегрировать все эти навыки и применять их к любой задаче. ИОИ долгое время был святым граалем ИИ, и эксперты активно обсуждали, появится ли ОН, и если да, то когда.

Выход за рамки ИОИ – это концепция искусственного суперинтеллекта (ИСИ). Это концепция, приписываемая машинам, которые смогут превзойти человеческий интеллект во всех аспектах. От творчества до решения проблем, сверхразумные машины превзойдут человеческий интеллект как отдельных людей, так и общества. Этот тип ИИ вызвал множество философских споров, и некоторые эксперты утверждают, что он может даже представлять экзистенциальную угрозу человечеству.

2. Алгоритмы и приложения

В семействе глубокого обучения существует множество архитектур нейронных сетей, которые позволяют использовать их в различных приложениях.

Сверточные нейронные сети – это класс нейронных сетей, наиболее часто применяемых для анализа изображений. Вдохновленные зрительной корой головного мозга животных, эти алгоритмы используют несколько слоев отдельных блоков или узлов для постепенного извлечения объектов более высокого уровня из необработанных входных данных. Например, если входным сигналом является изображение, первые слои нейронной сети могут

идентифицировать линии и кривые, в то время как последние слои могут идентифицировать буквы или лица. Эта характеристика позволяет сверточным нейронным сетям идентифицировать объекты, что, в свою очередь, позволяет распознавать объекты, а затем распознавать лицо.

Еще одной областью, которой уделяется большое внимание, является обработка естественного языка (NLP). Тип архитектуры, наиболее часто используемый в NLP, известен как Рекуррентные нейронные сети (РНС). В РНС сетевые узлы соединены во временной последовательности. Опираясь на внутреннюю память, которая обрабатывает последовательности входных данных, машина, использующая РНС, может выполнять распознавание речи, понимая последовательности слов и их морфосинтаксическую и семантическую функцию.

Помимо распознавания речи, NLP также может использоваться для генерации текста, который составляет основу «чат-ботов» – программных программ, которые работают в режиме онлайн и могут быть запрограммированы для имитации основного разговора. Генерация контента, такого как текст и изображения, возможна благодаря другому типу нейронной сети, известной как Генеративные состязательные сети (GAN). Эта инновационная архитектура, изобретенная в 2014 году, произвела революцию в области глубокого обучения. Модели GAN состоят из двух искусственных нейронных сетей: генеративной сети и дискриминационной сети. В то время как генеративная сеть создает новые данные с теми же характеристиками, что и обучающий набор, дискриминационная сеть отделяет сгенерированные данные от обучающих данных. GAN, обученный работе с фотографиями, может, например, генерировать новые изображения, похожие на набор данных сохраненных изображений. Дискриминатор случайным образом получает фотографии, созданные генератором на основе обучающего набора данных, и пытается идентифицировать их по исходным изображениям. Цель генератора состоит в том, чтобы «обмануть» сеть дискриминаторов, создавая все более совершенных новых кандидатов.

GAN имеют множество приложений, таких как создание текста, изображений, песен и различных видов искусства. GAN также стоят за широко разрекламированным и горячо обсуждаемым явлением, известным как «глубокие подделки». Портфолио «глубокого обучения» и «поддельных МЕДИА», глубокие подделки – это разновидность синтетических МЕДИА, изобретенных в 2017 году. Они предполагают использование методов ИИ для манипулирования или создания поддельного визуального и аудиоконтента, который люди или даже технологические решения не могут сразу отличить от подлинного содержания.

В сочетании с охватом и скоростью Интернета, социальных сетей и приложений для обмена сообщениями, глубокие подделки могут быстро охватить миллионы людей за чрезвычайно короткий промежуток времени. Из-за этого глубокие подделки были определены как мощное оружие в современных войнах дезинформации, в результате которых люди больше не могут полагаться на то, что они видят или слышат.

3. Развивающаяся технология

Предполагаемый рынок продуктов, связанных с ИИ, растет с каждым днем по мере расширения интеграции ИИ в такие области, как медицина, экономика, коммуникации, страхование, финансирование и многие другие области. ИИ используется, например, в автономных транспортных средствах, таких как беспилотные летательные аппараты и самоуправляемые автомобили, поисковые системы, онлайн-умные помощники, фильтрация спама и целевая онлайн-реклама. Он также используется для создания поэзии и других видов искусства, доказательства математических теорем, игры в такие игры, как шахматы и, что несколько противоречиво, для информирования и прогнозирования результатов судебных решений.

С увеличением инвестиций со стороны частного сектора, научных кругов и государственных структур алгоритмы машинного обучения, безусловно, будут продолжать становиться еще более сложными. В сочетании

с непрерывным сбором данных с помощью датчиков и мобильных приложений объем данных, доступных для обучения машинным алгоритмам, будет расти экспоненциально, что приведет к значительному прогрессу в области ИИ, что, в свою очередь, еще больше расширит границы возможностей машин.

Развитие систем ИИ, вероятно, позволит добиться огромных успехов в области интеллекта робототехники. Все более способные роботы или роботизированные инструменты с улучшенными «чувствами» и ловкостью смогут выполнять задачи, которые когда-то считались слишком сложными или неэкономичными для автоматизации. Более того, с расширением возможностей продвинутого ИИ машины, скорее всего, смогут выполнять не только ручные задачи, но и когнитивные задачи, например, в области бухгалтерского учета, маркетинга и управления персоналом.

Стремительное развитие и интеграция ИИ в повседневную деятельность уже изменили многие отрасли и сектора, и эта тенденция, по прогнозам, сохранится. ИИ обязывает участников во всех секторах переосмыслить то, как принимаются решения и как выполняются повседневные задачи. По крайней мере, на данный момент, похоже, что ИИ никуда не денется, и потенциал этой технологии, меняющей правила игры, доступен любому, кто захочет ею воспользоваться.

III. УГРОЗА АЛГОРИТМОВ И ТЕРРОРИЗМА

Хотя тактика терроризма варьируется от группы к группе и от человека к человеку, можно сказать, что в определенной степени террористические организации, как правило, избегают риска, отдавая предпочтение испытанной эффективности оружия, такого как пистолеты и бомбы. Тем не менее, терроризм, несомненно, не является постоянной угрозой. Террористические группы и отдельные лица показали, что они могут очень хорошо адаптироваться и значительно эволюционировали на протяжении десятилетий. Они продемонстрировали потенциал для инноваций, например, в своей организационной структуре, став децентрализованными,

франчайзинговыми и глобальными. Они также значительно эволюционировали с точки зрения тактики, перейдя от нерегулярной партизанской войны к неизбирательным нападениям.

В технологическом плане эта тенденция к инновациям особенно ярко проявляется в отношении Интернета и социальных сетей, которые оказались чрезвычайно ценными для террористов. Интернет и социальные сети, а также, как следствие, другие экосистемы, такие как платформа онлайн-игр, стали мощными инструментами для террористических групп, которые радикализируют, вдохновляют и подстрекают к насилию; берут на себя ответственность за нападения; вербуют; собирают и переводят средства; покупают и передают оружие; и предоставляют своим членам учебные пособия или инструменты. Например, в 2019 году стрельба в Крайстчерче в Новой Зеландии транслировалась злоумышленником в прямом эфире на Facebook. Хотя видео было снято несколько минут спустя, нападение транслировалось по всему миру, усиливая его воздействие и последствия для жертв.

Масштабы этого растущего явления можно увидеть из таких усилий, как День действий Европола по обращению. В рамках Дня действий по обращению к 2020 году Европол и 17 стран выявили и оценили на предмет удаления целых 1906 URL-адресов, ссылающихся на террористический контент на 180 платформах и веб-сайтах всего за один день. В течение двух лет сам Facebook удалил более 26 миллионов единиц контента от таких групп, как Исламское государство Ирак и Левант (ИГИЛ) и Аль-Каида, и за первые три месяца 2020 года он удалил около 4,7 миллиона единиц контента, связанного с «организованной ненавистью», в том числе увеличение более чем на 3 миллиона единиц контента по сравнению с последним кварталом 2019 года.

Злоупотребление Интернетом и социальными сетями также является областью, в которой способность террористических групп адаптироваться, в частности, к вызовам, совершенно очевидна. В ответ на усилия платформ социальных сетей и правоохранительных органов по уничтожению

террористического контента в Интернете произошло несколько изменений в том, как террористы используют Интернет и социальные сети, от зашифрованной связи до других довольно инновационных методов. Например, в попытке избежать обнаружения, недавнее видео, содержащее террористический контент, загруженное в Facebook, включало 30-секундное представление новостного канала France 24, прежде чем началось настоящее пропагандистское видео продолжительностью 49 минут. Также примечательно, что в мае 2020 года «Хайят Тахрир аш-Шам» – бывший фронт «Ан-Нусра» для народа Леванта – призвал своих членов и группы боевиков в Сирии прекратить использование таких платформ, как Telegram, Facebook Messenger и Viber, и вместо этого использовать другие зашифрованные приложения, такие как Talk, Riot, Signal и Wire. Действительно, внедрение сквозного шифрования на таких платформах вызвало значительную озабоченность у политиков и специалистов по борьбе с терроризмом в связи с тем, что оно позволяет террористам «скрываться» и безопасно общаться, тем самым избегая обнаружения. Многочисленные расследования и контртеррористические операции указывают на использование шифрования как лицами, связанными с ИГИЛ, так и лицами, связанными с «Аль-Каидой». Хотя технология, безусловно, не была исключительной движущей силой значительного развития терроризма, она сыграла в нем важную роль. Недавняя история изобилует примерами, демонстрирующими все более изощренное использование различных технологий террористическими и насильственными экстремистскими группами. Во многих отношениях это не должно вызывать удивления. Террористы, как и каждый отдельный человек, в конце концов, являются «детьми своего времени». Как коллектив, они полагаются на доступные им инструменты и используют их, как это сделал бы любой обычный человек. И действительно, все технологии, аналоговые и цифровые, развиваются до такой степени, что злоумышленники могут использовать их для совершения преступлений.

В широком смысле взаимодействие технологий и терроризма проявляется тремя основными способами. Во-первых, террористы полагаются на технологии в качестве оружия для совершения нападений. На самом деле характер террористических нападений значительно изменился с течением времени в связи с технологическими разработками. Арсеналы террористов значительно расширились – от использования ножей и пистолетов до угона самолетов и других нападений с использованием транспортных средств, причем некоторые группы даже демонстрируют степень намерения приобрести и использовать химические, биологические или радиоактивные материалы. Внедрение автоматической винтовки, возможно, является одной из наиболее значительных адаптаций к технологическому развитию. Благодаря своей низкой стоимости и смертоносности автоматическая винтовка стала излюбленным оружием террористических групп во многих частях мира. Во-вторых, технологические достижения в области транспорта и логистики изменили возможности террористических и преступных групп в целом, позволив им увеличить скорость, охват и масштабы своих операций и сделать их глобальными, а не локальными угрозами. Наконец, развитие информационно-коммуникационных технологий позволило террористическим группам и отдельным лицам быстрее и скрытнее общаться на все больших расстояниях и распространять вирусные видео и информацию, способствующие более быстрому и масштабному терроризму. При этом они смогли как повысить эффективность и результативность своих атак, так и охватить потенциальных новобранцев. Мобильные устройства связи, Интернет и, в последнее время, социальные сети и темная сеть являются ведущими примерами этого.

Недавние примеры использования террористами технологий включают в себя целый ряд передовых устройств. Например, устройства глобальной системы определения местоположения (GPS), мобильные телефоны и Интернет использовались исполнителями терактов в Мумбаи в 2008 году для планирования, координации и выполнения своей миссии. Хотя

в современных условиях это, возможно, уже не кажется особенно новаторским, в то время это ознаменовало инновационное использование новейших технологических достижений. Совсем недавно виртуальные активы на основе блокчейна, такие как «Биткоин», а также мобильный банкинг и краудфандинг, использовались террористами в целях сбора средств или для перемещения средств, в то время как темная сеть служит рынком для материалов, оружия и поддельных документов.

Однако имеющиеся данные свидетельствуют о том, что при использовании технологий террористы-одиночки, в частности, стремятся использовать общедоступные технологии для связи, оружия и транспортных целей. Предпочтительным представляется оборудование, требующее низкого уровня технической оснащенности, которое можно приобрести в магазинах «сделай сам». В таких формах «низкотехнологичного терроризма» террористы, особенно одиночки, ищут способы превратить повседневные инструменты и транспортные средства, такие как кухонные ножи, легковые и грузовые автомобили, в оружие.

Несмотря на это, с каждым днем передовые технологии, когда-то ограниченные специализированными сообществами, становятся все более доступными для широкой публики. Ярким примером является то, что, в то время как десять лет назад террористическая группа, маневрирующая флотом или «роем» беспилотных летательных аппаратов, несущих взрывоопасную полезную нагрузку, считалась бы нереалистичной, сегодня такой сценарий является реальной угрозой.

Это технологическое расширение ИИ, возможно, может привести к тому, что правоохранительные органы, подразделения по борьбе с терроризмом и другие силы безопасности могут быть «застигнуты врасплох» инновационными террористическими группами и отдельными лицами, которые выявили новые и непредвиденные пути и средства, используя доступные и коммерческие технологии в злонамеренных целях.

Учитывая это и размышляя о последних тенденциях, разработках и потенциале в области ИИ, включая компьютерное зрение, NLP и так далее, вопрос, следовательно, заключается в том, станет ли возможно ИИ еще одним инструментом в инструментарии терроризма.

IV. КЛАССИФИКАЦИЯ ТИПОВ УГРОЗ ИИ

ИИ может создавать множество новых проблем в различных контекстах для отдельных лиц, организаций и государств. Эти проблемы возникают на разных этапах жизненного цикла ИИ от проектирования до развертывания и могут быть вызваны как преднамеренными, так и непреднамеренными действиями.

Главной из проблем, связанных с использованием ИИ законными субъектами, является вполне реальный и серьезный потенциал этой технологии для нарушения прав человека. Когда технология ИИ не используется должным образом, это может угрожать, например, правам на частную жизнь, равенству, включая гендерное равенство, и недискриминации. Нарушение прав может быть результатом неоправданного или непропорционального использования ИИ, или оно может быть непреднамеренным, например, путем использования неосознанно искаженных данных для обучения алгоритмам машинного обучения, что приводит к несправедливым решениям, дискриминирующим отдельных лиц, группы или сообщества по запрещенным основаниям.

Термин «злонамеренное использование ИИ» обычно применяется к действиям, которые намеренно приводят к вредным последствиям. В 2018 году группа выдающихся авторов из различных дисциплин и организаций, включая Институт будущего человечества Оксфордского университета, Центр изучения экзистенциального риска Кембриджского университета, Фонд электронных границ и Центр новой американской безопасности, изучила злонамеренное использование ИИ государствами, преступниками и террористами. В их докладе, озаглавленном «Вредоносное использование искусственного интеллекта: прогнозирование, предотвращение

и смягчение последствий», был отмечен быстрый рост вредоносного использования технологии в течение ближайшего десятилетия. Авторы считают, что злонамеренное использование ИИ создает угрозы с точки зрения кибербезопасности, физической безопасности и политической безопасности.

Киберугрозы: Киберугрозы вызывают все большую озабоченность, учитывая присущие киберпространству уязвимости и асимметричный характер угроз, создаваемых кибератаками. С точки зрения терроризма, угрозы включают фишинг, злоумышленников, вымогателей и DDoS-атаки, а также порчу веб-сайтов. Кроме того, растет озабоченность по поводу неправомерного использования террористами информационных и коммуникационных технологий, особенно Интернета и социальных сетей, для совершения, подстрекательства, вербовки, финансирования или планирования террористических актов. Как будет подробно объяснено в следующих главах, террористы могут использовать системы ИИ, например, для повышения эффективности обычных кибератак или для подрыва безопасности информации путем нарушения ее конфиденциальности или нарушения ее целостности и доступности.

Физические угрозы: За последнее десятилетие повседневная жизнь становится все более взаимосвязанной благодаря технологиям. Эта взаимосвязанность нашла отражение в появлении концепции Интернета вещей – экосистемы подключенных цифровых устройств и физических объектов, которые передают данные через Интернет. В этом взаимосвязанном мире беспилотные летательные аппараты начали осуществлять поставки, и автономные транспортные средства уже выходят на дороги. В то же время с интеграцией этих технологий и подключенных устройств в повседневную жизнь возникают новые проблемы для людей и инфраструктуры. Взаимосвязанность и все большая автономность устройств и роботов в умных городах или в домашних условиях расширяют возможности и масштабы возможных атак.

Политические угрозы: С развитием информационно-коммуникационных технологий и глобальной известностью социальных сетей то, как, когда и почему люди общаются и находят источники новостей, неизбежно претерпевает беспрецедентные изменения. Эту трансформацию можно наблюдать во всем мире, и она повлияла на результаты выборов, способствовала народным протестам и предоставила людям возможность осуществлять свои основные права. В то же время известность социальных сетей в равной степени может сделать людей уязвимыми для манипуляций с помощью недостоверной информации и дезинформации, а также расширила возможности как государственных, так и частных организаций по проведению операций профилирования и наблюдения. Интеграция ИИ в это уравнение, например, за счет распространения глубоких затуханий, значительно усилит природу этой угрозы.

Как отметили авторы отчета за 2018 год, эти категории не обязательно являются взаимоисключающими. Например, взлом с использованием ИИ может быть направлен на киберфизические системы, приводящие к физическому ущербу, а физические или цифровые атаки могут быть осуществлены в политических целях. Более того, «политический» – это сложная классификация, особенно в контексте терроризма, для которого политическая мотивация часто очень тесно связана с общим пониманием концепции терроризма, наряду с социальными, идеологическими, религиозными и экономическими факторами.

В этой связи для целей настоящего доклада злонамеренное использование ИИ в террористических целях рассмотрит два основных типа угроз, а именно киберугрозы и физические угрозы, а также добавит к обсуждению другие соответствующие действия, связанные с действиями террористических групп и отдельных лиц, включая методы финансирования, стратегии пропаганды и дезинформации, и другие оперативные тактики.

V. ФАКТ ИЛИ НАУЧНАЯ ФАНТАСТИКА?

Рассмотрев некоторые категории угроз, создаваемых злонамеренным использованием ИИ, в этой главе будет рассмотрен вопрос о том, существует ли какое-либо достоверное содержание таких угроз или злонамеренное использование ИИ в террористических целях является немногим более чем научной фантастикой.

С самого начала важно уточнить, что на сегодняшний день не было выявлено четких доказательств фактического использования ИИ террористическими организациями. Фактически, в своем последнем докладе Группа по мониторингу ИГИЛ/«Аль-Каиды» отметила, что «несмотря на сохраняющуюся озабоченность государств-членов по поводу злоупотребления террористами технологиями, особенно в области финансов, вооружений и социальных сетей, ни ИГИЛ, ни «Аль-Каида», по оценкам, не добились значительного прогресса в этом отношении в конце 2020 года».

Однако в этом есть важные предостережения. ИИ, как уже было замечено, во многом уже является частью повседневной жизни и используется многими людьми, часто без их ведома. Например, NLP является основой интеллектуальных помощников, таких как Siri от Apple и Alexa от Amazon, и используется для исправления опечаток в текстовых сообщениях, электронных письмах и документах Word. Распознавание лиц используется для разблокировки смартфонов, а распознавание объектов помогает классифицировать изображения и улучшать результаты поиска Google. В этой связи приведенное выше заявление не предполагает исключения возможности того, что террористические группы и отдельные лица использовали ИИ косвенно? например, пассивно или даже невольно, как описано выше. Скорее, это подразумевает, что ИИ не использовался напрямую, например, специально для улучшения или усиления атаки.

Отсутствие доказательств прямого использования ИИ в терроризме также не следует истолковывать как указание на то, что террористы равнодушны или не заинтересованы в технологии. Хотя конкретных доказательств

заинтересованности или намерения террористов использовать ИИ обнаружено не было, разумно предположить, что эти группы и отдельные лица осведомлены об этой технологии, которую многие так часто хвалили за ее революционный потенциал. Например, примечательно, что в 2016 году видео, по-видимому, подготовленное ИГИЛ в Сирии, показало, как группа экспериментирует с рудиментарной версией самоуправляемого автомобиля, который в данном случае управлялся дистанционно. В автомобиле, о котором идет речь, были установлены манекены, чтобы обмануть наблюдателей, заставив их думать, что за рулем был человек. Считается, что у ИГИЛ также были планы попытаться воспроизвести тепловую сигнатуру человека в попытке еще больше обмануть системы безопасности, заставив их поверить, что кто-то действительно находится внутри транспортного средства. Вскоре после этого главный научный сотрудник F-Secure указал, что есть доказательства того, что ИГИЛ действительно работает над разработкой самоуправляемых автомобилей для использования вместо террористов-смертников, а в 2018 году британские прокуроры выявили, что двое сторонников ИГИЛ планировали использовать автомобиль без водителя для совершения террористических атак.

Совсем недавно, в марте 2020 года, сторонник ИГИЛ распространил видео о Rocket.Chat – децентрализованная платформа социальных сетей, которая использовалась ИГИЛ для распространения террористического контента и облегчения онлайн-сотрудничества и координации объясняет, как можно использовать программное обеспечение для распознавания лиц. В рассматриваемом видео подразумевалось, что распознавание лиц может идентифицировать людей на основе их черт лица, даже если они пытались скрыть свою личность, используя маскировку лица или цифровое размытие лица. В видео далее утверждалось, что эта возможность, безусловно, поможет властям в пресечении террористических заговоров и задержании преступников. Хотя нынешние возможности этой технологии, возможно, были преувеличены в видео, признание ее существования и тот факт, что видео было быстро

распространено по нескольким другим каналам, подтверждают, что террористические группы осведомлены о потенциале ИИ и следят за его тенденциями и развитием, по крайней мере, на поверхностном уровне.

Хотя не было замечено, чтобы террористические группы напрямую использовали ИИ, имеются значительные доказательства использования этими группами технологий, связанных с ИИ. Это наблюдается, в частности, при эксплуатации беспилотных летательных аппаратов, также известных как «дроны». Беспилотные летательные аппараты считаются технологией, связанной с ИИ, для целей настоящего отчета, поскольку, даже если они управляются вручную, они могут обладать различной степенью автономности. Например, беспилотные летательные аппараты уже могут быть оснащены системой стабилизации полета с поддержкой Глобальной навигационной спутниковой системы (GNSS) и функциями «чувствовать и избегать», а ИИ может быть использован для обеспечения еще большей степени автономии.

Использование такой технологии террористическими группами, а также другими негосударственными субъектами не является чем-то новым. Было замечено, что такие группы экспериментировали с беспилотными летательными аппаратами или дистанционно управляемыми летательными аппаратами в течение нескольких лет, начиная с неиспользованных планов Аум Синрике – японского культа, стоявшего за атакой зарина в токийском метро в 1995 году.

Характер использования беспилотных летательных аппаратов такими группами был разнообразен и включает в себя фактические попытки нападений, нарушения, наблюдение и пропаганду. Кроме того, было также высказано предположение, что беспилотные летательные аппараты могут использоваться для выполнения задач разведки, наблюдения и мониторинга целей, протоколов безопасности и моделей поведения; повышения точности непрямого огня; сбора видеоматериалов для использования в пропагандистских материалах; нарушения деятельности правоохранительных органов;

нарушения, вмешательства или парализации ключевых инфраструктур, воздушного движения и экономических активов; контрабанда незаконных товаров через границы или в чувствительные районы; запугивание и преследование; и разжигание паники в СМИ.

Примечательно, что есть доказательства того, что ИГИЛ использует беспилотные летательные аппараты примерно с 2016 года. Сообщается, что ИГИЛ даже создало подразделение «Беспилотных летательных аппаратов моджахедов», которое отвечает за разработку и использование беспилотных летательных аппаратов. Как полагают, впервые применив эту технологию, члены ИГИЛ развернули беспилотные летательные аппараты, начиненные взрывчаткой, во время нападений на севере Ирака, убив двух курдских бойцов пешмерга и ранив двух военнослужащих французских сил спецопераций. В 2017 году ИГИЛ хвасталось успехом своих инициатив в области беспилотных летательных аппаратов, утверждая, что их атаки беспилотников убили или ранили 39 солдат за одну неделю. Террористическая группа также распространила онлайн-руководство для своих сторонников по использованию беспилотных летательных аппаратов и выпустила пропагандистские материалы, призывающие к атакам с использованием беспилотных летательных аппаратов.

Известно также, что другие негосударственные субъекты использовали беспилотные летательные аппараты. Следует упомянуть две громкие атаки беспилотников: покушение на президента Венесуэлы Николаса Мадуро в августе 2018 года и нападения в сентябре 2019 года на нефтеперерабатывающие предприятия Saudi Aramco в Абкаике и Хураисе в Саудовской Аравии. Оба инцидента были связаны с беспилотными летательными аппаратами со взрывоопасной полезной нагрузкой. Последнее особенно примечательно тем, что в нем участвовало до 25 беспилотных летательных аппаратов.

Ключевыми факторами, обусловливающими растущий интерес к использованию этой технологии во вредоносных целях, являются

коммерческая доступность, доступность и удобство беспилотных летательных аппаратов в сочетании с проблемами противодействия их использованию. Потенциальный драматический эффект использования беспилотных летательных аппаратов в ходе террористической атаки также является еще одним фактором, который следует учитывать при попытке понять их привлекательность для террористических групп и отдельных лиц.

Соответственно, возросла озабоченность по поводу использования беспилотных летательных аппаратов террористическими группами и другими негосударственными субъектами, в частности с точки зрения возможного использования роев. Настоятельно призывая государства-члены предпринять более активные коллективные усилия для предотвращения приобретения террористами оружия, Совет Безопасности Организации Объединенных Наций в Резолюции 2370 (2017 год) решительно осудил поток беспилотных летательных аппаратов в ИГИЛ, Аль-Каиду, их филиалы и связанные с ними группы и между ними, незаконные вооруженные формирования и преступники. Глобальный форум по борьбе с терроризмом также признал, что беспилотные летательные аппараты вызывают растущую озабоченность, и в этой связи опубликовал в 2019 году Берлинский меморандум о передовой практике противодействия террористическому использованию беспилотных летательных систем. Меморандум содержит рекомендации по определению, разработке и уточнению политики, практики, руководящих принципов, положений, программ и подходов для противодействия использованию беспилотных летательных аппаратов террористами.

Несмотря на это, нынешнее использование технологий беспилотных летательных аппаратов террористическими организациями остается редкостью, носит довольно сложный характер и в значительной степени зависит от контроля со стороны человека. Хотя дроны могут использовать ИИ для повышения автономности, на данном этапе имеется ограниченное количество доказательств того, что какой-либо террорист или другой

негосударственный субъект использовал или пытался использовать дроны с поддержкой ИИ.

VI. ТЕРРОРИЗМ С ПОДДЕРЖКОЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ЗАЗЕРКАЛЬЕ

В предыдущих главах указывалось, что террористические группы и отдельные лица неоднократно демонстрировали способность внедрять и адаптироваться к новым появляющимся технологиям, таким как GPS, мобильные телефоны и, в последнее время, беспилотные летательные аппараты. Действительно, понимание и признание того, что терроризм является развивающейся угрозой, жизненно важно для обеспечения способности международного сообщества предотвращать терроризм и бороться с ним. Недостаток воображения может иметь смертельные последствия.

Имея это в виду, в этой главе мы экстраполируем некоторые потенциальные угрозы, связанные с терроризмом и ИИ, которые могут быть на горизонте или только за его пределами, представив подборку потенциальных вредоносных применений ИИ террористическими организациями. Эти вредоносные виды использования вдохновлены тенденциями и событиями в области ИИ, существующими методами работы террористических групп и отдельных лиц и известными в настоящее время преступными видами использования ИИ.

Список потенциальных вредоносных видов использования ИИ, включенный в эту главу, не является исчерпывающим резюме того, как террористические организации могут использовать ИИ, и никоим образом не предназначен для указания вероятности возникновения любого такого сценария. Вместо этого он направлен на стимулирование размышлений и информирование о том, как террористические группы и отдельные лица могут продолжать внедрять инновации с использованием технологий ИИ, тем самым накапливая знания и улучшая понимание проблемы национальными и международными организациями, ответственными за борьбу с терроризмом.

В отсутствие доказательств только с помощью предположений можно обеспечить надлежащий уровень готовности.

Эти вредоносные виды использования были охарактеризованы и сгруппированы в соответствии с их целями, а именно: расширение кибернетических возможностей, обеспечение возможностей для физических атак, содействие финансированию терроризма, распространение пропаганды и дезинформации и другие оперативные тактики. Однако некоторые из представленных ниже вредоносных видов использования могут иметь двойную цель или функцию. Например, программы-вымогатели могут быть частью кибератаки, а также способствовать финансированию терроризма. По этой причине классификация, используемая в этой главе, должна быть интерпретирована плавно.

Наконец, прежде чем продолжить рассмотрение этих потенциальных вредоносных применений, следует отметить, что, хотя внедрение ИИ, вероятно, расширит определенные возможности злоумышленников, национальные органы власти и частные организации, которым поручено обеспечивать безопасность платформ или систем от атак, не находятся в застое. Такие организации в равной степени развиваются и адаптируются к последним технологическим тенденциям, разработкам и прорывам. Таким образом, хотя ИИ может усиливать существующие угрозы или представлять новые угрозы с точки зрения терроризма, важно иметь в виду, что он также улучшит или предоставит новые возможности для предотвращения или смягчения потенциальных угроз. Это особенно относится к кибербезопасности, где ИИ уже играет значительную роль.

1. Расширение кибернетических возможностей

A. Атаки с отказом в обслуживании

Атаки типа «отказ в обслуживании» (DOS) или распределенный отказ в обслуживании (DDoS) были одними из самых популярных кибератак на протяжении десятилетий. Конечная цель этих атак состоит в том,

чтобы сделать компьютерную систему, подключенную к Интернету, временно недоступной для ее пользователей, полностью исчерпав ее память путем многократных повторных запросов на подключение. При DDoS-атаках злоумышленники используют более одной, а часто и тысячи машин, так называемых «ботнетов», для направления запросов в целевую систему.

Считается, что в период с конца 2016 года по начало 2017 года ИГИЛ запустило свою первую в истории успешную серию DDoS-атак после обсуждения среди своих членов возможности проведения таких атак на Темном веб-форуме ИГИЛ высшего уровня. Эти атаки использовали инструмент DDoS под названием «Пушка Халифата» и были нацелены, в первую очередь, на военную, экономическую и образовательную инфраструктуру, четко демонстрируя серьезность этой угрозы. С тех пор хакерский отдел ИГИЛ также взял на себя ответственность за аналогичные атаки, нарушающие работу онлайн-сервисов.

Часть того, что делает DOS- или DDoS-атаки привлекательными для киберпреступников, террористов и других злоумышленников, заключается в том, что их можно запускать с минимальными усилиями, а их производительность относительно проста. Для запуска такой атаки злоумышленнику не требуется нацеливаться на конкретные уязвимости – как правило, достаточно того факта, что целевая система подключена к Интернету. Однако машинное обучение готово вывести легкость и простоту DOS- или DDoS-атак на следующий уровень за счет автоматизации процессов, которые традиционно выполняются злоумышленником. Например, алгоритмы машинного обучения могут быть использованы для управления ботнетами, стоящими за атакой, или для выявления уязвимых систем с помощью сложной сетевой разведки.

Потенциал использования машинного обучения в DDoS-атаках уже используется злоумышленниками. Например, в 2018 году TaskRabbit – онлайн-рынок для внештатных работников стал объектом DDoS-атаки, проведенной хакером с использованием ботнета, управляемого программным

обеспечением ИИ. Эта атака затронула 3,75 миллиона пользователей веб-сайта, которые пострадали от значительного нарушения данных.

Интересно, что в 2019 году Link сообщил, что почти половина DDoS-атак в настоящее время осуществляется с использованием облачных сервисов, таких как Amazon Web Services, Microsoft Azure и Google Cloud. Используя вычислительные мощности, предоставляемые такими сервисами, вредоносные виртуальные машины могут быть созданы с использованием машинного обучения, которые затем используются как часть ботнета для запуска DdoS-атаки.

B. Вредоносное ПО

Вредоносное ПО, или вредоносное программное обеспечение, относится к широкому спектру программного обеспечения, которое проникает в компьютерную систему или сеть, выводит ее из строя и наносит вред, использует или нарушает работу цели. Некоторыми примерами вредоносных программ являются шпионские программы, программы-вымогатели, вирусы, «троянские кони» и рекламное ПО. Вредоносное ПО уже давно используется вандалами, мошенниками, шантажистами и другими преступниками, а также является очевидным инструментом для использования террористическими группами и отдельными лицами. Вредоносное ПО может использоваться, например, для обеспечения доступа злоумышленников к веб-сайту, серверу или сети для получения кредитной карты или другой конфиденциальной информации или нанесения ущерба кибер-инфраструктуре государственных или частных учреждений.

Достижения в области ИИ, и особенно в области машинного обучения, находят огромное применение в борьбе с угрозами кибербезопасности, такими как вредоносное ПО, и позволяют специалистам анализировать данные прошлых атак и использовать их для обнаружения аномалий и отражения потенциальных угроз.

Однако в то же время ИИ также может быть использован разработчиками вредоносных программ. Например, ИИ может быть использован для автоматизации процессов атак, повышения эффективности вредоносных атак или даже создания совершенно новых форм вредоносных программ. Гипотетически его можно было бы даже использовать для написания кода для совершенно новых форм вредоносных программ. Фактически, киберпреступники уже использовали ИИ для создания полиморфных вредоносных программ – типа интеллектуальных вредоносных программ, которые адаптируются и изменяются, чтобы избежать обнаружения, и ИИ можно было бы дополнительно использовать для улучшения этого типа вредоносных программ, увеличивая скорость, с которой они могут адаптироваться.

Также следует отметить, что ИИ может сыграть важную роль в расширении и даже автоматизации распространения вредоносных программ. Например, фишинговые кампании являются одним из основных способов распространения вредоносных программ. В недавнем эксперименте с использованием ИИ, получившем название «SNAP_R», фишинговые твиты были доставлены 819 пользователям со скоростью 6,75 твита в минуту, при этом 275 были успешными. Человеческий аналог в эксперименте отправлял твиты 129 пользователям со скоростью 1,075 в минуту, при этом только 49 были успешными. Используя машинное обучение, те, кто планирует атаку, могут также сканировать социальные сети, чтобы определить уязвимые цели для фишинговой кампании. Они также могут использовать алгоритмы машинного обучения для анализа электронных писем и ответов, полученных в ходе предыдущих фишинговых атак, для создания более сложного контента, который кажется более аутентичным и, следовательно, может избежать обнаружения спам-фильтрами и лучше обмануть жертв в установке вредоносного ПО.

Еще одним все более используемым способом доставки вредоносных программ являются атаки с использованием языка структурированных запросов

(SQL). Атаки с использованием SQL-инъекций также могут быть облегчены ИИ. Например, инструмент DeepHack с поддержкой ИИ учится взламывать веб-приложения с помощью нейронной сети. Подобные инструменты можно использовать для создания полностью работоспособных автоматизированных систем взлома, которые могли бы функционировать и доставлять вредоносные программы даже без предварительного знания целевой системы.

Хотя в исследовании 2019 года Malwarebytes сообщалось, что в то время еще не было реальных доказательств наличия вредоносных программ с поддержкой ИИ, стоит отметить, что исследователи IBM представили новую вредоносную программу, которую они разработали, известную как «DeepLocker», на конференции Black Hat в США в 2018 году. Вредоносная программа DeepLocker была разработана, чтобы точно продемонстрировать, как ИИ может усиливать атаки вредоносных программ. DeepLocker маскируется под программное обеспечение для видеоконференций и скрывается, пока не идентифицирует свою предполагаемую жертву с помощью распознавания лица и голоса, а затем развертывает свою полезную нагрузку. Подобные инструменты в руках террористических групп, безусловно, усилили бы серьезность угрозы кибертерроризма.

C. Программы-вымогатели

Вымогатели неоднократно признавались одной из главных угроз кибербезопасности во всем мире. Подмножество вредоносных программ, вымогателей – это вредоносное программное обеспечение, которое шифрует файлы жертв и требует выплаты выкупа за расшифровку файлов. Угроза атак вымогателей усиливается тем фактом, что вредоносное ПО может легко распространиться на тысячи устройств благодаря своей функции самовосстановления. Примером этого стала атака с целью выкупа WannaCry в 2017 году, которая затронула более 200 000 компьютеров в 150 странах. В 2019 году было подсчитано, что к 2021 году каждые 11 секунд будет происходить атака вымогателей с совокупным годовым оборотом примерно

в 20 миллиардов долларов. Совсем недавно больницы в Соединенных Штатах сообщили об увеличении числа атак вымогателей на 71% в период с сентября по октябрь 2020 года, угрожая инфраструктуре, и без того сильно напряженной из-за пандемии COVID-19.

Интеграция ИИ в программы-вымогатели может значительно усилить последствия этих атак. Модели машинного обучения могут быть использованы для расширения существующей экосистемы программ-вымогателей путем создания новых типов атак или усиления эффектов существующих с помощью интеллектуальных методов таргетинга. Алгоритмы машинного обучения также могут быть использованы для повышения эффективности фишинговой кампании по доставке программ-вымогателей, как описано выше. Используя ИИ для совершения сложных атак вымогателей, и без того прибыльный метод атаки может стать значительно более выгодным. Такие нападения, в свою очередь, могут быть использованы для получения дохода, поддерживающего инфраструктуру или деятельность террористических групп и отдельных лиц.

Напоминая о склонности террористических и насильственных экстремистских групп к похищению людей с целью получения выкупа, эффективных и прибыльных атак с использованием ИИ, по-видимому, естественным образом вписываются в их репертуар как форма «похищения с целью выкупа 2.0».

В то же время, как основной целью вымогателей традиционно было вымогательство денег у жертв, атака NotPetya 2017 года продемонстрировала, что атаки также могут использоваться в деструктивных или разрушительных целях. В ходе атаки NotPetya программа-вымогатель была изменена таким образом, что невозможно было отменить шифрование и вернуть систему в состояние, предшествовавшее атаке. В этой связи атака вымогателей с поддержкой ИИ может быть использована террористическими группами и отдельными лицами в других деструктивных целях, а не только в целях сбора средств.

D. Угадывание пароля

Пароли являются первой линией защиты от взлома и необходимы во всех стратегиях киберзащиты, от крупных компаний до домашних хозяйств. Получение пароля для доступа к защищенным веб-сайтам может позволить злоумышленнику проникнуть в системы или сети, например, для нарушения работы основных служб, создания сбоев, кражи ценных данных или информации, манипулирования данными или процессами, или установки вредоносного программного обеспечения. Сторонники террористических групп, таких как ИГИЛ, имеют давнюю историю взлома веб-сайтов и аккаунтов в социальных сетях с целью порчи и распространения пропагандистских материалов.

В целях повышения безопасности платформы и веб-сайты приняли многочисленные меры для защиты от угадывания пароля, в том числе требуют более длинных паролей, содержащих не менее восьми символов или комбинацию буквенно-цифровых и прописных и строчных символов. Тем не менее, люди склонны следовать определенным шаблонам при выборе паролей, таким как сочетание имен, фамилий и дат рождения. Они также склонны использовать простые и предсказуемые пароли и повторно использовать пароли в нескольких службах. Это значительно облегчает работу хакера.

Целые базы данных паролей, украденных с разных платформ, можно найти в Интернете, чтобы хакеры могли их изучить и позже использовать в своих попытках взломать веб-сайты. Avast, например, сообщил, что он выявил 30 160 455 237 украденных паролей в Интернете. Инструменты для подбора паролей, такие как «Джон Потрошитель», используют эти базы данных для подбора паролей, но они требуют обширной работы по ручному кодированию для создания плана атаки.

Однако достижения в области ИИ могут быть использованы для значительного ускорения, улучшения и автоматизации процесса подбора пароля. Злоумышленники могут обучать нейронные сети с помощью

этих огромных онлайновых баз данных паролей, которые, в свою очередь, могут генерировать более сложные варианты паролей, чем люди когда-либо могли себе представить. Затем эти нейронные сети могут выполнять несколько попыток подряд, пока не будет найдено решение, тем самым устраняя необходимость в непосредственном участии хакера. В исследовании 2017 года исследователи ввели десятки миллионов просочившихся паролей в нейронную сеть, которой было поручено генерировать новые пароли. Затем эти пароли были сопоставлены с просочившимися паролями с таких сайтов, как LinkedIn, чтобы измерить, насколько успешно нейронная сеть будет взламывать пароли пользователей. Исследование показало, что они смогли взломать 27% паролей в наборе LinkedIn. Последующее исследование показало, что ИИ может угадать пароль, определяя какие клавиши вводятся, на основе движений плеч, анализируемых во время видеозвонков. Результаты исследования показали, что рассматриваемое программное обеспечение ИИ имело тревожный показатель точности от 75% до 93%.

Исследования также показали, что сложная генерация паролей может быть выполнена с использованием GAN, которые анализируют большой набор паролей и генерируют варианты, аналогичные оригинальным примерам, что означает, что он способен заранее генерировать миллиарды угаданных паролей, позволяя более целенаправленно и эффективно угадывать пароли.

В то время как в таких разработках повышенное внимание уделяется наличию уникальных и надежных паролей, а также развертыванию двухфакторной или многофакторной аутентификации, например, с помощью мобильного устройства, в качестве дополнительного уровня защиты, важно помнить, что даже последнее не обеспечивает полной защиты, поскольку оно имеет свои собственные уязвимости, особенно с точки зрения социальной инженерии – еще одной области, которую, как будет описано ниже, машинное обучение также должно улучшить.

E. Взлом КАПЧИ

КАПЧА (полностью автоматизированный публичный тест Тьюринга для различения компьютеров и людей) – еще одна важная мера безопасности, предназначенная для защиты сетей и веб-сайтов от атак. Как следует из названия, КАПЧА предназначена для того, чтобы отличать реальных пользователей от спам-роботов, позволяя людям получать доступ к роботам и блокировать их. Веб-сайты используют КАПЧУ, поскольку автоматический доступ нечеловеческих лиц к учетным записям электронной почты может, например, привести к увеличению количества спам-сообщений электронной почты, а «блог-спамеры» могут извлечь выгоду из искусственно завышенного количества кликов, чтобы получить экономические преимущества. Система работает, применяя аутентификацию «запрос-ответ», чтобы понять, поступает ли запрос на доступ от человека или компьютера.

Попытки взломать системы КАПЧИ относятся к ранним дням ее внедрения, но достижения в области машинного обучения позволили методам взлома систем КАПЧИ стать более сложными. В 2013 году стартап в области ИИ заявил, что им удалось победить системы КАПЧИ с помощью программного обеспечения, имитирующего мозг, с вероятностью успеха более 90%, не требуя больших наборов данных для обучения системы или больших вычислительных мощностей. Алгоритм был обучен распознавать цифры и буквы и показал особую эффективность на КАПЧАХ, состоящих из букв, которые выглядят так, как будто они сделаны из отпечатков пальцев. С тех пор растет интерес к машинному обучению и технологиям глубокого обучения для взлома систем КАПЧИ.

Преодоление систем КАПЧИ может в значительной степени позволить террористическим группам и отдельным лицам осуществлять кибератаки. Например, это позволило бы распространять автоматизированные и крупномасштабные спам-письма, содержащие вредоносное ПО, террористический контент или другие подрывные или пропагандистские материалы.

F. Шифрование и дешифрование

В обществе, где основные черты повседневной жизни становятся все более цифровыми, шифрование имеет решающее значение для государственных учреждений, предприятий и широкой общественности для обеспечения конфиденциальности, целостности и доступности их коммуникаций и хранящейся информации. Шифрование можно понимать как процесс преобразования данных, таких как сообщения или фрагменты информации, таким образом, чтобы предотвратить несанкционированный доступ. Дешифрование, в свою очередь, представляет собой процесс возврата зашифрованных данных на начальную стадию.

Как мощный и практичный инструмент защиты от несанкционированного доступа, шифрование также используется теми, у кого более гнусные намерения, включая преступников и террористов, поскольку оно позволяет им безопасно общаться и обмениваться информацией, сохраняя при этом свою анонимность. Дешифрование одинаково привлекательно для таких групп или отдельных лиц, поскольку оно может позволить им, например, получить доступ к конфиденциальной информации.

В одном примечательном случае в 2012 году, гражданин Франции был приговорен к пяти годам тюремного заключения по делу, в котором суду были представлены копии зашифрованных электронных писем, которыми обменивались члены террористических организаций. Утверждалось, что террористическая организация использовала программное обеспечение для шифрования под названием «Секреты моджахедов» для облегчения тайных онлайн-коммуникаций между ее членами. Было также замечено, что некоторые террористические организации воспользовались таким программным обеспечением, как Camouflage и WinZip, для маскировки распространяемой и передаваемой информации с помощью стеганографии и шифрования.

На базе ИИ в настоящее время изучаются средства шифрования. В 2016 году исследователи из Google Brain успешно обучили две нейронные сети общаться друг с другом, не позволяя третьей нейронной сети

перехватывать их сообщения. Исследование показало, что первым двум нейронным сетям удалось автономно создать свою собственную форму отправки зашифрованных сообщений туда и обратно и по очереди расшифровывать эти сообщения. Интересно, что исследователи из Колумбийского университета также разработали в 2018 году метод глубокого обучения, который эффективно позволял людям встраивать конфиденциальную информацию в, казалось бы, обычный текст. Таким образом, такая информация, как текст, изображения или QR-коды быстрого ответа, может быть скрыта от невооруженного глаза на самом видном месте.

С развитием ИИ методы шифрования и дешифрования могут стать еще более мощными. Опираясь на сложные методы шифрования с использованием ИИ, члены террористических организаций смогут общаться между собой с большей легкостью и без нарушения целостности информации. Методы дешифрования с использованием ИИ, в свою очередь, позволят террористическим организациям более легко получить доступ к конфиденциальным зашифрованным разведданным, передаваемым контртеррористическими подразделениями.

2. Включение физических атак

А. Автономные транспортные средства

Транспортные средства, особенно легковые автомобили, фургоны и грузовики, уже давно используются в террористических актах. Существует бесчисленное множество громких примеров их использования. Транспортные средства использовались, например, при преднамеренных атаках на таран, как это было видно во время нападения на Рождественский рынок в Берлине в декабре 2016 года и во время нападения в Барселоне в августе 2017 года. Транспортные средства также использовались при взрывах автомобилей, таких как взрыв машины скорой помощи в Кабуле в 2018 году, в результате которого погибло 103 человека и 235 получили ранения.

Одним из наиболее известных применений ИИ являются автономные транспортные средства, также называемые самоуправляемыми или беспилотными автомобилями. Многие считают автономные транспортные средства более безопасным, удобным и эффективным средством передвижения для нашего будущего. По сути, ИИ, встроенный в бортовой компьютер транспортного средства, использует методы глубокого обучения для имитации процессов принятия решений водителем при управлении действиями транспортного средства, рулевого управления, ускорения, торможения и т.д. Компании, такие как Tesla и Google, уже давно выступают за практическое применение этой технологии, возглавляя усилия в области исследований, тестирования и разработки автономных автомобилей. В последние годы бесчисленное множество крупных автомобильных компаний присоединились к ним в их усилиях по выпуску самоуправляемых автомобилей на дороги. В ноябре 2019 года Waymo – дочерняя компания Alphabet Inc, материнской компании Google, – достигла важной вехи, запустив автономную службу такси в Финиксе штата Аризона в Соединенных Штатах, в которой не был задействован резервный водитель безопасности.

С быстрым развитием технологий в сочетании со значительными коммерческими инвестициями в индустрию автономных транспортных средств и достижением многочисленных вех в решении правовых и политических проблем становится неизбежным, что ИИ действительно в конечном итоге изменит опыт вождения, хотя до сих пор точно неизвестно, когда это произойдет.

Учитывая обширную историю терроризма и транспортных средств, повышение автономности автомобилей вполне может стать благоприятным событием для террористических групп, это позволяет им эффективно проводить один из своих наиболее традиционных видов атак удаленно, без необходимости для последователя жертвовать своей жизнью или рисковать быть задержанным. Помимо содействия атакам с помощью полностью автономных самодельных взрывных устройств на транспортных средствах,

также было высказано предположение, что самоуправляемые автомобили могут быть использованы для того, чтобы вызвать серьезные аварии, перекрыть дороги или вызвать самоходную бойню. Несмотря на это, есть основания полагать, что функции безопасности, позволяющие им обнаруживать и избегать таких ситуаций, как столкновение с пешеходами, включение аварийной системы или перевод транспортного средства на альтернативный курс, помешали бы террористическим заговорам использовать такие транспортные средства таким образом. Действительно, как было описано выше, уже произошли некоторые события, связанные с самоуправляемыми автомобилями и терроризмом, включая элементарные эксперименты и проверки в отношении планов сторонников ИГИЛ, которые не осуществились.

Уместно отметить, что термин «транспортные средства» не обязательно подразумевает только колесные транспортные средства, но также включает в себя наземные транспортные средства, такие как подводные лодки, и летательные аппараты, беспилотные летательные аппараты, обычно называемые «дронами». Как отмечалось ранее, беспилотные летательные аппараты в основном управляются дистанционно и обладают ограниченной степенью автономности, но ИИ в равной степени предоставляет дронам возможность стать более или даже полностью автономными. Исследователи, изучающие применение ИИ в беспилотных летательных аппаратах, смогли разработать автономные системы управления для роев дронов, позволяющие им перемещаться и даже выполнять акробатические маневры, такие как бочки и сальто, без вмешательства человека-контроллера на земле. И здесь технические достижения открывают двери для множества автономных беспилотных летательных аппаратов. С технической точки зрения можно утверждать, что разработка автономных беспилотных летательных аппаратов или даже подводных аппаратов в ближайшем будущем может быть еще более достижимой, чем автомобили без водителя, учитывая меньшее количество переменных, которые должны учитывать программисты беспилотных

летательных аппаратов, и более упрощенные правовые рамки, применимые к беспилотным летательным аппаратам.

B. Беспилотные летательные аппараты с распознаванием лиц

За последние несколько лет внедрение технологии распознавания лиц резко возросло, чему способствовало быстрое совершенствование машинного обучения. Его коммерциализация создала новые возможности, от улучшения аутентификации для доступа к электронным устройствам до ускорения посадки в самолет и контроля безопасности в аэропортах. В дальнейшем внедрение распознавания лиц может охватить новые сервисы и в конечном итоге даже стать предпочтительным средством аутентификации для доступа к сервисам.

В 2017 году Институт будущего жизни, некоммерческий научно-исследовательский институт и информационно-пропагандистская организация, базирующаяся в Соединенных Штатах, опубликовал видео под названием «Убойные роботы», в котором рой микро-дронов, загруженных несколькими граммами взрывчатки, использует распознавание лиц для идентификации и атаки на свои цели в стиле камикадзе. Технология распознавания лиц позволила контроллеру запрограммировать беспилотный летательный аппарат на автономное получение, идентификацию и захват выбранной цели путем сопоставления изображений, собранных дроном, с изображениями, загруженными во встроенную базу данных распознавания лиц. Несмотря на высокую драматизацию, видео быстро стало вирусным, набрав до трех миллионов просмотров в Интернете и превратив возможную комбинацию этих технологий в горячую тему. К счастью, эта технология не существует в «готовом» формате, хотя это не совсем новое понятие и не просто научная фантастика. Некоторые коммерческие продукты для беспилотных летательных аппаратов уже включают ограниченные возможности распознавания лиц, хотя это ограничено конкретными функциями, такими как разблокировка возможностей полета и включение режимов «следуй за мной». В настоящее время беспилотные летательные аппараты не включают технологию

распознавания лиц для идентификации и нацеливания на людей во время полета. В связи с этим использование распознавания лиц в беспилотных летательных аппаратах гораздо более ограничено.

Несколько правоохранительных органов по всему миру уже начали экспериментировать с сочетанием этих технологий, например, для оказания помощи в поиске пропавших без вести и уязвимых лиц или для выявления интересующих лиц в местах массового скопления людей. Способность находить, отслеживать и идентифицировать цели таким автоматизированным способом, естественно, привлекательна для правоохранительных органов, но ее использование вызвало обеспокоенность по поводу массового наблюдения и нарушений прав человека, особенно с точки зрения права на частную жизнь. В свете нескольких противоречивых событий, связанных с использованием распознавания лиц правоохранительными органами, будущее этой технологии ИИ остается неопределенным.

Злонамеренное использование беспилотных летательных аппаратов террористическими группами для нападений можно считать растущей, хотя еще и не серьезной угрозой. Интеграция технологии распознавания лиц, безусловно, изменила бы правила игры в этом отношении, значительно повысив уровень угрозы со стороны беспилотных летательных аппаратов и обеспечив возможность очень целенаправленных атак. Хотя технология не является легкодоступной, люди, обладающие необходимыми ноу-хау, могли бы разработать возможности «робота-бойни», объединив различные элементы самостоятельно.

C. Генетически нацеленное биологическое оружие

Пандемия COVID-19 имела широкий спектр пагубных последствий, от гибели отдельных людей до масштабного глобального экономического спада. В июле 2020 года Генеральный секретарь Организации Объединенных Наций Антониу Гутерриш отметил, что «пандемия также выявила уязвимость к новым и возникающим формам терроризма, таким как злоупотребление

цифровыми технологиями, кибератаки и биотерроризм». Действительно, появляющиеся новые технологии, особенно биотехнология в сочетании с ИИ, могут предоставить возможность для разработки новых смертоносных штаммов патогенов, специально предназначенных для определенных генетических групп, хотя технические препятствия для этого были бы существенными. В своем докладе о деятельности системы Организации Объединенных Наций по осуществлению Глобальной контртеррористической стратегии Организации Объединенных Наций Генеральный секретарь, кроме того, особо выделил синтетическую биологию в качестве примера новой и развивающейся технологии, которая может представлять опасность с точки зрения терроризма.

Развитие технологий генетического секвенирования позволило исследователям из различных областей обрабатывать больше генетических данных и извлекать больше генетической информации. Хотя эти разработки способствуют научному развитию и могут значительно улучшить качество нашей жизни, они вызывают проблемы безопасности. Применяя модели машинного обучения, исследователи могут еще больше продвинуть свои методы генетической диагностики и терапии.

Большая часть собранных генетических материалов хранится в генетических базах данных или биобанках и распространяется среди соответствующих исследователей. Другими словами, собранный генетический материал, а также извлеченная из него информация становятся все более доступными для сообщества заинтересованных сторон, занимающихся исследованиями.

Несмотря на преимущества этой открытой научной модели, снижение или даже устранение барьеров для доступа и использования генетических материалов и полученной информации может привести к нежелательным последствиям. Если злоумышленники получат доступ к этим генетическим данным, становится все более возможным использовать их для обучения моделей машинного обучения с целью создания опасных патогенов.

Если идентифицируемые генетические маркеры, например, однонуклеотидные полиморфизмы, могут быть надежно идентифицированы для дифференциации этнических групп, теоретически было бы возможно ориентироваться на лиц определенной этнической принадлежности. Однако важно отметить, что генетические знания, предназначенные для таких конкретных групп, до сих пор остаются недоступными для исследователей биотехнологии и что для таких вредоносных инициатив потребуются передовые технические навыки и специализированное оборудование.

3. Предоставление средств для финансирования терроризма

А. Звуковые глубокие подделки

Помимо повышения эффективности робозвонков – масштабных незапрошенных автоматических звонков, используемых для доставки предварительно записанных сообщений, часто злоумышленными компаниями, организованными преступными группами и отдельными мошенниками, – машинное обучение может сыграть значительную роль во вредоносных телефонных схемах. В частности, введение «глубоко подделанного» аудиоконтента может быть использовано для убеждения людей в том, что они общаются с человеком, которого они знают. Как будет описано более подробно ниже, глубокие подделки предполагают использование методов ИИ для манипулирования или создания визуального и аудиоконтента, который людям или даже технологическим решениям трудно сразу отличить от подлинных. Чтобы создать звук глубокой подделки, механизмы машинного обучения обучаются с помощью конференц-звонков, YouTube, обновлений в социальных сетях и даже выступлений TED, копируя голосовые шаблоны некоторых целевых пользователей, а затем создавая новые аудиозаписи с теми же характеристиками голоса.

Именно этот метод был использован в 2019 году, когда генеральному директору британской фирмы поступил звонок от того, кто, по его мнению, был исполнительным директором материнской компании его фирмы,

в котором его попросили срочно отправить 244 000 долларов венгерскому поставщику. Позже стало очевидно, что звонивший использовал программное обеспечение на основе ИИ, чтобы имитировать голос исполнительного директора. Та же тактика была использована в июле 2020 года в попытке обмануть технологическую компанию, базирующуюся в Соединенных Штатах.

Если эти вредоносные схемы окажутся прибыльным предприятием, террористические группы, возможно, попытаются использовать их для сбора средств у людей, обманывая или угрожая им. Помимо использования этих схем для финансовых возможностей, такие группы могут в равной степени использовать их для шпионажа и получения информации, выдавая себя за лиц, находящихся в критическом положении, или обманывая людей, находящихся в критическом положении, с помощью встроенных систем роботизации глубокой подделки.

B. Криптоторговля

В 2009 году группа или частное лицо, известное только как Сатоши Накамото, опубликовала «Белую книгу» об одноранговой электронной платежной системе, известной как Биткоин. В этой статье были заложены основы децентрализованной конвертируемой виртуальной валюты, защищенной криптографией, что делает практически невозможным подделку или двойные расходы. Вскоре после выхода белой книги блок биткойнов был «добыт» Накамото, вызвав бурю интереса и инвестиций в цифровые активы. Вскоре начали появляться новые формы виртуальных активов или криптовалют, как их также часто называют, такие как Litecoin, Ripple, Ethereum, Monero, Libra, Dogecoin, вдохновленный мемами, и многие другие.

В силу своей природы криптовалюты нашли широкое применение во всем мире, и даже ЮНИСЕФ начал получать, хранить и распространять пожертвования в виртуальном формате в 2019 году. В то же время их природа обеспечивает криптовалютам анонимность, что сделало их привлекательным

средством для злоумышленников, например, для незаконной продажи наркотиков, огнестрельного оружия и взрывчатых веществ, контрабанды людей, отмывания денег и содействия киберпреступности.

В дополнение к их использованию в качестве валюты, криптовалюты также стали популярным активом для торговли в результате их высокой рыночной изменчивости, создав целое поколение крипто-миллионеров и миллиардеров за удивительно короткий промежуток времени. Именно в этом конкретном контексте ИИ может сыграть важную роль в отношении криптовалют, сделав рыночные спекуляции вокруг этой виртуальной валюты ценным средством сбора средств, а не просто обращением к сочувствующим за пожертвованиями.

Например, на известных подпольных форумах, таких как «blackhatworld.com» обсуждалась разработка и использование ботов на базе ИИ, предназначенных для торговли криптовалютами. Как и в других приложениях машинного обучения, такая система будет опираться на обучение систем машинного обучения историческим данным, чтобы получать более точные и сложные прогнозы для более прибыльной торговли криптовалютами. На этих форумах также были выявлены другие формы использования ИИ, такие как сканирование сотен криптовалют, чтобы найти закономерности для оптимизации торговли криптовалютами, и использование ИИ для создания роботов для торговли криптовалютами. Несколько групп в мире торговли и бирж уже некоторое время разрабатывают роботов для торговли акциями с ИИ, но без особого успеха, но тот факт, что многие подпольные блоги ссылаются на эту тему, тем не менее, делает уместным упомянуть об этом. Помимо использования ИИ для манипулирования криптовалютным пространством с целью получения финансовой прибыли, террористы могут использовать ИИ для облегчения кражи криптовалют из «горячих кошельков», или для облегчения более анонимных транзакций в блокчейне. Обеспечение большей анонимности торговых практик снижает общий риск их разоблачения и потери средств.

Хотя систематическое использование криптовалют террористическими группами и отдельными лицами еще не было замечено, растет озабоченность по поводу использования криптовалют террористическими организациями. Даже если документированные примеры ограничены, есть несколько примечательных примеров. Например, следователи во время взрывов в Шри-Ланке в 2019 году, в результате которых погибло более 250 человек, заметили, что количество транзакций в биткойн-кошельках, используемых ИГИЛ для сбора средств, заметно увеличилось до взрывов, что привело к убеждению, что эти биткойны сыграли определенную роль в финансировании атак. Аналогичные подозрения существуют в отношении парижских нападений ИГИЛ в 2015 году, хотя доказательства, подтверждающие эти подозрения, отсутствуют. В результате крупного прорыва в начале 2020 года власти Соединенных Штатов изъяли более 1 миллиона долларов США в криптовалютах со счетов, связанных с ИГИЛ и «Аль-Каидой». Также следует отметить, что Целевая группа по финансовым мероприятиям отметила возросшее злоупотребление онлайн-финансовыми услугами и виртуальными активами для перемещения и сокрытия незаконных средств во время пандемии COVID-19, описывая это как возникающий риск отмывания денег и финансирования терроризма. В свете этих событий следует также рассмотреть возможность использования террористическими группами криптоторговли с использованием ИИ в целях сбора средств, хотя изменчивость рынка, безусловно, может снизить привлекательность такой тактики в более широком масштабе.

4. Распространение пропаганды и дезинформации

А. Глубокие подделки и другой манипулируемый контент

Термин «глубокие подделки» относится к типу поддельного аудио и/или визуального контента, который был обработан или сгенерирован с использованием GAN. В результате трудностей, которые они представляют как для людей, так и для машин, чтобы отличить настоящее от подделки,

подделки, возможно, стали одним из наиболее заметных злоупотреблений ИИ сегодня и привлекли значительное внимание средств массовой информации.

Глубокие подделки и технологии, стоящие за ними, могут стать мощным оружием в современных войнах за дезинформацию. Более того, в сочетании с охватом и скоростью Интернета, социальных сетей и приложений для обмена сообщениями, глубокие подделки могут быстро охватить миллионы людей за чрезвычайно короткий промежуток времени. В этой связи фейки представляют значительный потенциал для целого ряда злонамеренных и преступных целей, которые включают: разрушение имиджа и доверия к личности; преследование или унижение людей в Интернете, в том числе с помощью сексуальных фейков; совершение шантажа, вымогательства и мошенничества; разрушение финансовых рынков; и разжигание социальных волнений и политической поляризации.

Использование глубоких подделок в целях дезинформации, скорее всего, подорвет доверие людей к традиционно авторитетным СМИ. Наводненные все более и более генерируемыми ИИ фальшивыми новостями, основанными на фанатичном тексте, поддельных видео и множестве теорий заговора, люди могут чувствовать, что онлайн-информации, включая видео, просто нельзя доверять, что приводит к феномену, называемому «информационным апокалипсисом» или «апатией реальности». С ростом поддельного контента, дезинформации мир становится свидетелем «распада правды», и, хотя многие действующие лица играют определенную роль в этом процессе, террористы, безусловно, могут способствовать и использовать его в своих собственных целях. Действительно, дезинформация сама по себе не является самым разрушительным аспектом глубоких подделок, скорее это идея о том, что любая информация может быть поддельной. Кроме того, трудности с аутентификацией видео позволят опровергнуть любую компрометирующую информацию, поскольку любой аудиовизуальный контент может быть сфабрикован. В результате, даже если такой видеоконтент на самом деле не был

скомпрометирован, он может быть заявлен как подделка, позволяющая отдельным лицам уклоняться от ответственности за свои действия.

В настоящее время фейки в подавляющем большинстве используются для создания порнографического контента, сочетая лица знаменитостей женского пола с телами порнографических актеров. Несмотря на это, фейки могут серьезно повлиять на демократию и национальную безопасность. Учитывая, что социальные сети стали одним из основных источников информации для общественности, фейки представляют значительную угрозу с точки зрения распространения дезинформации, поскольку информация потребляется и воспроизводится быстро, при этом пользователи тратят мало времени, если вообще тратят, на аутентификацию контента. Хотя видео с фейками, как правило, имеют довольно короткий срок службы в Интернете, они могут вызвать мгновенную панику и замешательство, особенно когда они становятся вирусными. Действительно, неспособности отдельных лиц отличить поддельный контент и путаницы в вопросе о том, является ли видео глубокой подделкой или нет, может быть даже достаточно, чтобы создать серьезные проблемы.

Учитывая негативные последствия фейков, вполне возможно, что террористические группы или отдельные лица могут попытаться использовать технологию, лежащую в основе фейков, для проведения кампаний дезинформации в социальных сетях с целью манипулирования общественным мнением или подрыва доверия людей к государственным институтам.

Такая технология также может быть использована в качестве эффективного инструмента пропаганды, радикализации или в качестве призыва к действию. Например, это может быть достигнуто за счет создания «глубоко сфабрикованного» контента, в котором целевой политический деятель делает оскорбительные замечания в адрес конкретного сообщества в попытке усилить возмущение внутри него и увеличить число сочувствующих.

В дополнение к созданию аудиовизуальных глубоких подделок, ИИ также может использоваться для создания индивидуальных повествований

о радикализации. Новые передовые методы в области NLP, в том числе широко разрекламированный GPT-3,179 OpenAI, вызвали обеспокоенность в связи с потенциальным использованием технологии в микропрофилировании и микро-таргетинге, создании автоматического текста для целей вербовки или распространения настраиваемых поддельных новостей и теорий заговора, связанных с терроризмом, например, утверждения ИГИЛ и «Аль-Каиды» о том, что пандемия COVID-19 является «Божьим гневом на Запад». Использование сайтов поддельных новостных СМИ с использованием ИИ может оказаться вредным, учитывая растущие тенденции онлайн-читателей делиться статьями, основанными на названии, или быстро «бегло читать» статью без проведения надлежащей проверки по существу на рассматриваемом веб-сайте(-ах). Таким образом, остается вероятность того, что террористические организации однажды смогут распространять системы ИИ, которые могли бы автоматически читать заголовки реальных новостей и создавать усеченные, поддельные сообщения для распространения в социальных сетях и других каналах в поддержку своего дела.

Наконец, ИИ может быть использован в майнинге для легко вербуемых или легко радикализируемых мужчин и женщин, позволяя целенаправленно распространять террористический контент или сообщения. В этом случае террористы могли бы использовать ИИ в качестве «алгоритмических усилителей» и «рекомендателей» для распространения пропаганды, например, направляя целевые сообщения лицам, которые неоднократно искали насильственный контент в Интернете или транслировали фильмы, изображающие отчужденных и разгневанных антигероев.

5. Другая оперативная тактика

А. Наблюдение

Значительные достижения в области компьютерного зрения – методы получения, обработки, анализа и извлечения информации из цифровых изображений или видео – обусловленные достижениями в области машинного

обучения, возможно, стали одним из важнейших последних достижений в области ИИ. Глубокое обучение произвело революцию в обработке изображений и видео, в частности в распознавании объектов, позволив машинам проводить распознавание лиц и распознавать выражения лиц. Помимо горячо оспариваемой области распознавания лиц, разработки в области компьютерного зрения также позволили улучшить обнаружение человеческого тела, идентификацию личности, распознавание атрибутов, распознавание поведения человека и распознавание движений тела (походки). Глубокое обучение также улучшило обнаружение, распознавание и отслеживание объектов, в том числе, например, идентификация и повторная идентификация транспортного средства и распознавание номерных знаков. В то же время эти достижения позволили существенно снизить частоту ошибок при неправильной идентификации.

Правоохранительные органы, будучи сообществом, которое уже давно использует широкий спектр технологий наблюдения, таких как замкнутое телевидение (CCTV), камеры, надеваемые на тело («камеры для тела»), и патрульные беспилотные летательные аппараты, быстро оценили потенциал компьютерного зрения с поддержкой глубокого обучения для облегчения идентификации жертв, преступников или других заинтересованных лиц. В последние годы наблюдается значительный рост интереса правоохранительных органов к технологиям наблюдения на основе ИИ. Глобальный индекс наблюдения за ИИ, составленный Фондом Карнеги за международный мир, показал, что 75 из 176 проанализированных стран активно используют технологии ИИ для целей наблюдения, в том числе в платформах «умный город»/«безопасный город», системах распознавания лиц и интеллектуальной полиции, демонстрируя, что внедрение систем наблюдения с использованием ИИ быстро растет во всем мире. Пандемия COVID-19 также сыграла значительную роль с точки зрения повышения интереса к технологиям наблюдения на основе ИИ, с несколькими национальными органами власти, демонстрирующими противоречивый потенциал технологии для поддержки

их усилий по отслеживанию цифровых контактов или для содействия обеспечению соблюдения карантинных мер.

Однако, перевернув этот вариант использования с ног на голову, становится возможным вредоносное использование технологий наблюдения на основе ИИ. Особенно в случае крупномасштабных террористических нападений, для планирования и подготовки часто требуются длительные периоды наблюдения. Террористические группы ведут наблюдение как за местами, так и за людьми, чтобы идентифицировать и обнаружить цель, определить ее пригодность для нападения и выявить слабые места, которые могут быть использованы для облегчения нападения. Традиционно это делается пешком, в припаркованном автомобиле или онлайн через социальные сети и может длиться недели, месяцы или даже годы. Достижения в области возможностей наблюдения с использованием ИИ теоретически могли бы устранить значительную часть трудоемких аспектов наблюдения. С помощью технологий террористы смогут, например, контролировать места и отслеживать перемещения людей, идентифицировать целевых лиц и активы и оценивать меры физической безопасности в целевом местоположении автоматически и удаленно.

B. Поддельные онлайн-личности и выдача себя за человека на платформах социальных сетей

Интернет по своей сути обеспечивает определенную степень анонимности пользователям. Это был один из факторов, который позволил использовать некоторые из самых низменных и вредных видов использования Интернета, включая онлайн-троллинг, киберзапугивание, уход за детьми и сексуальную эксплуатацию. По оценкам, на Facebook насчитывается более 750 миллионов поддельных аккаунтов, которые используются для активного распространения заранее определенного и скомпрометированного контента в Интернете. Facebook признал масштабы этой проблемы, указав, что только в 2019 году было удалено 2,9 миллиарда поддельных аккаунтов.

Генеральный секретарь Организации Объединенных Наций Антониу Гутерриш в сентябре 2019 года отметил, что использование социальных сетей и темной сети для координации атак, распространения пропаганды и вербовки новых последователей стало новым рубежом терроризма. Поскольку основной целью террористических организаций в целях вербовки являются молодые люди в возрасте от 17 до 27 лет, эффективное использование социальных сетей становится еще более важным для террористических организаций, учитывая популярность таких платформ в этих возрастных группах. В прошлом использование ИГИЛ платформ социальных сетей способствовало беспрецедентному росту числа иностранных боевиков-террористов, направляющихся в зоны конфликтов. Кроме того, использование платформ социальных сетей также позволило террористическим организациям совершать нападения, выявлять потенциальных новобранцев, распространять пропаганду, распространять учебные материалы, заниматься незаконной торговлей и собирать средства. Поскольку террористические организации уже используют платформы социальных сетей с такой эффективностью, применение ИИ неизбежно только еще больше повысит их успешность.

На самом деле, достижения в области ИИ обещают привнести в это явление совершенно новое измерение. GANs, технология, лежащая в основе глубоких затуханий, особенно эффективна при синтезе высокореалистичных поддельных изображений лиц. Например, веб-сайт «ThisPersonDoesNotExist.com» использует GANs для создания нового и полностью сфабрикованного изображения человеческого лица каждый раз, когда страница открывается или обновляется.

Потенциал для злонамеренного использования такой технологии уже был замечен. В 2019 году в аккаунте LinkedIn под именем Кэти Джонс была использована фотография профиля, сгенерированная ИИ. Молодой специалист в возрасте 30 лет, профиль Кэти указал, что она работала в вашингтонском аналитическом центре и была связана с рядом правительственных чиновников Соединенных Штатов. Эксперты, изучившие профиль Кэти, отметили

его как вымышленный, придя к выводу, что поддельный профиль, скорее всего, был попыткой заманить интересующих лиц и собрать у них информацию, возможно, в рамках операции по сбору разведывательной информации.

Более того, на криминальных форумах растет число созданных ИИ поддельных аккаунтов и чат-ботов для платформ социальных сетей. Исследования показали, что эти поддельные аккаунты и боты становятся все более изощренными и могут выдавать себя за обычных пользователей соответствующих платформ социальных сетей, что позволяет им избежать пометки пользователями или обнаружения и запрета платформами. Эти поддельные учетные записи и боты используются для нескольких целей, таких как увеличение просмотров, подписчиков или «лайков» определенных страниц или контента.

Террористические организации могут извлечь выгоду из таких разработок на базе ИИ для повышения эффективности использования ими платформ социальных сетей. Созданные ИИ поддельные учетные записи и боты, которые могут выдавать себя за обычных пользователей, могут помочь террористическим организациям с большей легкостью распространять свои сообщения на платформах социальных сетей и с меньшим риском того, что реальные люди будут запрещены, или способствовать усилиям по социальной инженерии в попытке получить нужную информацию или поддержать усилия по радикализации.

C. Измененные паспорта

Неправильное получение, изменение или подделка проездных документов имеет важное значение для современных террористических групп. Фальшивые документы регулярно используются террористами, например, для облегчения международных поездок – как это было в случае с несколькими угонщиками 11 сентября. Они также часто используются в качестве удостоверения личности для других административных целей. Например, лица, стоявшие за терактами в Париже в 2015 году, использовали поддельные

паспорта для получения кредита до совершения терактов. Использование поддельных паспортов в террористических целях настолько широко распространено, что следователи даже полагали, что террористические организации, такие как «Аль-Каида», имеют своих собственных специализированных членов в различных странах, единственной задачей которых является предоставление другим членам организации паспортов и других соответствующих документов по запросу. В последнее время считается, что ИГИЛ «индустриализировало» производство поддельных паспортов.

Вскоре на первый план может выйти опасный и новый метод создания поддельных паспортов на основе ИИ, который можно назвать «измененными» паспортами. Используя метод Моргана (морфинг через генеративные состязательные сети), было замечено, что преступники могут создавать фотографии паспортов, которые могут быть сопоставлены более чем с одним человеком. Другими словами, измененные паспорта относятся к одному паспорту, который может использоваться двумя или более лицами. Используя это, злоумышленники могут обмануть как человеческие, так и машинные системы распознавания, легко нарушая традиционную безопасность границ. Для решения некоторых проблем безопасности, связанных с измененными паспортами, власти в некоторых странах начали принимать дополнительные меры, такие как обязывание физических лиц фотографировать паспорта в паспортных столах, а не предоставлять свои собственные – возможно, поддельные – фотографии.

Пока неизвестно, окажутся ли эти дополнительные меры достаточными, но уже ясно, что непроверенные, измененные паспорта могут значительно повысить способность террористов перемещаться незамеченными через пограничный контроль и проверки безопасности в аэропортах или даже просто в общественных местах.

D. Социальная инженерия в Интернете

Социальная инженерия – это хорошо зарекомендовавший себя вектор атаки, который опирается на человеческое взаимодействие для использования слабых мест, часто включая манипуляции. Он часто используется преступниками и другими злоумышленниками в мошенничестве для получения денег или конфиденциальной информации или для убеждения жертв сделать что-то, чего они в противном случае не сделали бы. Этот вектор атаки может быть применен как онлайн, в основном через социальные сети, так и офлайн, лично.

Чат-боты – одно из наиболее заметных применений ИИ в современном обществе. По мере развития ИИ боты, вероятно, будут играть все большую роль в онлайн-обмане, в том числе с помощью схем социальной инженерии.

Излишне говорить, что террористические организации используют тактику социальной инженерии в Интернете, в первую очередь для того, чтобы помочь им выявлять и вербовать новых членов и сочувствующих. Действительно, эти группы уже имеют значительный опыт в использовании ботов. После парижских атак 2015 года активистская группа Anonymous запустила онлайн-кампанию против ИГИЛ, в ходе которой она заявила, что удалила в Интернете до 25 000 ботов ИГИЛ.

В настоящее время чат-боты преуспевают в очень узких контекстах с повторяющимися элементами, такими как поддержка электронной коммерции и обслуживание клиентов. Благодаря достижениям в области NLP боты могут со временем учиться на основе своего взаимодействия с людьми, что позволяет им реагировать так, чтобы больше походить на человека. По мере того как способность отличать бота от человека становится все более сложной, возрастает потенциал использования ботов в атаках социальной инженерии.

В то же время успех тактики социальной инженерии зависит от их убедительности, и в этой связи получение подробной и точной информации о цели играет существенную роль. ИИ здесь тоже может сыграть свою роль. Например, на онлайн-форумах изучаются новые инструменты обнаружения учетных записей с использованием ИИ, использующие алгоритмы

распознавания лиц, которые позволят пользователю сопоставлять несколько отдельных учетных записей одного и того же человека на разных платформах социальных сетей, даже если изображение профиля не совпадает. С помощью этой технологии злоумышленник может быстро идентифицировать несколько профилей своей цели в социальных сетях. Анализируя эти профили, злоумышленники могут затем получить более полное представление об этом человеке и собрать необходимую информацию, чтобы лучше манипулировать этим человеком и, например, заставить его или ее делиться конфиденциальной информацией либо путем обмана или принуждения.

VII. РАСКРЫТИЕ ТЕРРОРИСТИЧЕСКОГО ИСПОЛЬЗОВАНИЯ ИИ

Вредоносное использование ИИ – это очень новая и еще не до конца изученная область. Потенциальное воздействие использования ИИ в террористических целях также еще предстоит оценить. Соответственно, правоохранительным органам, силам безопасности и органам по борьбе с терроризмом, а также директивным органам, промышленности и научным кругам может быть трудно смириться со злонамеренным использованием ИИ. Следовательно, трудно провести тщательную и обоснованную оценку риска.

Чтобы помочь преодолеть эти трудности, была разработана серия вымышленных сценариев. Эти сценарии описаны ниже с целью помочь читателям представить, как ИИ может быть интегрирован в образ действий вымышленных террористических групп. Вероятность такого сценария, по мнению участников Совещания Группы экспертов КТЦООН/ЮНОКТ–ЮНИКРИ, дополнительно указывается после каждого сценария.

Сценарий 1:

Проблемы пандемии – правительство Лантия и вакцина получают смертельный удар в результате сложной кибератаки

После периода экономического спада в Республике Лантия, террористическая группировка приобрела известность. Группа, известная как

«Искупители», предприняла несколько кибер- и физических атак на правительство и его институты в попытке ослабить и свергнуть его. Известно также, что группа сотрудничает с несколькими группами единомышленников по всему региону, которым они предоставили свои обширные кибер-возможности для достижения своих общих целей. Эти возможности включают создание приложения для социальных сетей с сквозным пользовательским шифрованием, известного как «Хаб», которое позволяет как обмениваться информацией между этими группами, так и распространять пропаганду среди общественности, чтобы повысить привлекательность Искупителей и привлечь новых участников.

Сейчас, в разгар глобальной пандемии, Республика Лантия изо всех сил пытается запустить свою программу вакцинации, чтобы оправиться от вспышки и защитить своих граждан от вируса. С начала пандемии более 3% ее населения было инфицировано, при этом уровень смертности на 3,4% выше, чем в большинстве стран. В эти первые дни программы вакцинации компания Республики Лантия обеспечила 40 000 доз вакцины FuturePharm в неделю. В эти трудные времена все внимание приковано к осуществлению правительственной программы вакцинации. Осознавая это, Искупители решают воспользоваться этими обстоятельствами и начинают планировать новую атаку, чтобы нанести смертельный удар по авторитету правительства в целом.

Опираясь на свою обширную сеть сочувствующих, Искупителям удается получить доступ к системе видеонаблюдения Республики Лантия, управляемой Отделом биометрии Национальной полиции. В течение нескольких часов после доступа к системе и отслеживания перемещений лиц, работающих в Национальной больнице Лантии, Искупители определяют ключевых сотрудников больницы на основе их перемещений в административное крыло и из него. Используя программное обеспечение для распознавания лиц, они могут идентифицировать себя, используя скриншоты лиц с записей камер видеонаблюдения. Перекрестные ссылки на имена идентифицированных лиц

с профилями пользователей сайта профессиональной сети «con-nected.com», Искупители выбирают подходящую цель в больнице – г-жа Элисон Эппл, одна из старших руководителей программы больницы по развертыванию программы вакцинации.

Следующей ночью Искупители начинают свою масштабную кибератаку, нацеленную на мисс Эппл в качестве точки входа. Они начинают с запуска атаки на нее с помощью ИИ-пароля, используя нейронную сеть, которая была обучена использованию онлайн-баз данных украденных паролей, полученных в темной сети. После включения нейронная сеть генерирует высококачественные догадки о паролях и в конечном итоге получает доступ к официальной учетной записи г-жи Эппл в больничной сети. Оказавшись внутри, Искупители ищут документацию, связанную с программой вакцинации. Вскоре они обнаруживают, что эти важные документы были зашифрованы для защиты их целостности. В ответ Искупители развертывают инструмент дешифрования на базе ИИ, который разблокирует функции безопасности документов, раскрывая основные данные и информацию, касающиеся программы вакцинации, включая основной узел хранения вакцины в больнице и информацию о протоколах и системах для ее хранения. Имея доступ к больничной сети, группа нацеливается на систему охлаждения вакцины, повышая температуру в морозильных камерах выше рекомендуемых минус 40 градусов Цельсия в течение пяти часов. При хранении вне температурных требований, необходимых для сохранения ее целостности, активные компоненты нейтрализуются, и эффективность вакцины снижается с 95% до всего лишь 5% без каких-либо изменений в ее внешнем виде. Сильные знания группы в области компьютерных наук позволяют им также отключать датчики температуры и систему оповещения, используемую для оповещения персонала больницы о любых изменениях температуры. Сделав это, группа очищает записи перед выходом из системы, не оставляя никаких свидетельств о каком-либо вмешательстве. К тому времени, когда персонал больницы вернется на работу на следующее утро, все морозильные камеры вернутся

к работе при рекомендуемой температуре хранения. Не подозревая о вмешательстве Искупителя, персонал больницы продолжает доставлять вакцину.

После нескольких недель вакцинации основные средства массовой информации начинают сообщать о растущем числе случаев, когда люди заражаются вирусом, а некоторые даже умирают, несмотря на то, что были полностью вакцинированы. По мере того, как вокруг этих сообщений развивается безумие и растет озабоченность по поводу вакцины, Искупители выпустили фейковый аудиоклип на сайте премьер-министра г-жи Кристины Кабальеро, которая была стойким сторонником и публичным лицом реакции правительства на вирус. В фальшивом звонке, мисс Кабальеро сообщает членам своей команды кабинета министров, что вакцина не работает и что все это было частью тщательно продуманной уловки для сбора генетического материала у граждан с целью усиления контроля правительства над населением. Глубокая подделка была создан Искупителями с помощью приложения, доступного для смартфонов, и нескольких аудиозаписей публичных заявлений премьер-министра. Хотя г-жа Кабальеро незамедлительно отрицает подлинность аудиоклипа, он быстро распространяется по сети, вызывая общественное возмущение и вынуждая ее уйти в отставку. Хотя ее место занимает заместитель премьер-министра, доверие к правительству падает до небывало низкого уровня, и без сильного руководства г-жи Кабальеро правительство постепенно начинает рушиться в результате внутренних конфликтов, что заставляет общественность призывать к проведению всеобщих выборов. В то же время аналитики рынка сообщают, что «сотни пользователей в минуту» присоединились к Хабу после выпуска аудиоклипа.

Сценарий 2:

Негде спрятаться – рой дронов убивает известного активиста

Солнечный полдень в Нью-Вайнленде нарушается, когда флот из пяти беспилотных летательных аппаратов проносится через переполненную центральную площадь города. Интерес толпы к необычному зрелищу, находящемуся всего в нескольких метрах от их голов, быстро переходит в панику и замешательство, когда небольшой взрыв внезапно сотрясает площадь. Поспешив на место происшествия, сотрудники полиции обнаруживают, что один человек погиб в результате взрыва, а несколько других получили серьезные травмы в результате их близости к месту взрыва. Погибший мужчина позже опознан как мистер Бенджамин Браун.

Браун был откровенным членом своего сообщества, который начал получать значительное внимание средств массовой информации за высказывания мнений в местных СМИ и публичные выступления, в которых он выступал с резкими и язвительными замечаниями, подрывающими идеологию террористической группы, известной как «Избранные». Со временем страсть и сила его заявлений способствовали тому, что он стал всемирно признанной фигурой, и недавно он даже выступил с докладом на TED, в котором он снова энергично атаковал методы и мотивы Избранных. Утром в день нападения мистер Браун выступал в местном книжном магазине на Центральной площади на мероприятии, связанном с выходом его последней книги «Избранные есть не более чем лжецы и мелкие преступники».

Избранный быстро взял на себя ответственность за нападение в видеообращении, опубликованном на канале социальных сетей, связанном с группой. В видео группа празднует смерть мистера Брауна, хвастаясь тем, что «месть найдет их врагов, где бы они ни прятались».

По мере расследования нападения власти устанавливают, что беспилотные летательные аппараты, замеченные на Центральной площади непосредственно перед нападением, сыграли центральную роль и что Избранные вооружили рой беспилотников самодельными взрывными устройствами (СВУ). Каждый из беспилотных летательных аппаратов был оснащен камерами и технологией распознавания лиц, сканирующими цель

под разными углами и, следовательно, имеющими разную перспективу его лица. Чтобы избежать ложных срабатываний, программное обеспечение автоматически сравнивало результаты приложения для распознавания лиц, установленного в каждом дроне, и выпускало взрывчатку только тогда, когда по крайней мере два дрона обнаруживали цель. С помощью этого метода точность обнаружения целей беспилотными летательными аппаратами была увеличена до 90%, гарантируя, что возможность для Избранных устранить эту занозу в своей стороне не будет упущена. Беспилотник просканировал цель, выходящую из книжного магазина, и как только личность мистера Брауна была обнаружена, беспилотники вошли в нисходящую спираль, развернув свою взрывчатую нагрузку и убив цель при взрыве.

Через несколько недель полиция завершает свое обширное расследование и арестовывает трех членов «Избранных» за их причастность к нападению. В пресс-релизе полиция указывает, что доказательства свидетельствуют о том, что беспилотные летательные аппараты были приобретены онлайн через различных коммерческих поставщиков для энтузиастов беспилотных летательных аппаратов. Они также сообщают, что Избранные использовали тот же веб-сайт для приобретения приложения для смартфонов multi-flyer controller, которое позволяло управлять парком беспилотных летательных аппаратов и идеально координировать полет дронов. Что касается программного обеспечения для распознавания лиц, полиция указала, что, хотя Избранные не имели большого опыта работы в области компьютерных наук, считалось, что группа также приобрела в Интернете коммерчески доступное программное обеспечение для распознавания лиц, выбрав наиболее подходящий вариант на основе онлайн-обзоров и описаний. Само программное обеспечение прилагалось к инструкциям, в которых подробно описывался процесс установки. В его спецификациях также отмечалось, что для реализации программы просто требовалось несколько изображений целей – что-то легко доступное для такого общественного деятеля, как г-н Браун.

Сценарий 3:

Границ больше нет – поддельные паспорта способствуют взрыву бомбы в столице

В начале года на популярном форуме подпольного хакерского сообщества «Broke.it», начали появляться рекламные объявления от хакерской группы «Хакерство для вас» для «ИИ как услуга». Реклама на каналах форума включала широкий спектр услуг, включая создание поддельных паспортов. В объявлениях указывается, что заинтересованным клиентам необходимо только отправить фотографии лиц предполагаемых пользователей и одну фотографию местного паспорта, и после уплаты сбора хакерская группа изготовит и выдаст поддельный паспорт.

Эта услуга быстро стала бестселлером «Хакерства для вас», учитывая, что производство измененных сервисов было относительно простым и что хакерская группа взимала низкую плату за услугу. Работа и репутация хакерской группы быстро выросли во всем преступном мире, и транснациональные преступные группы все чаще используют эти поддельные паспорта, чтобы незамеченными проходить пограничный контроль и с большей легкостью осуществлять свою деятельность на международном уровне.

По мере того как популярность этих измененных паспортов продолжала расти, слухи начали распространяться и среди других злоумышленников, включая террористические и насильственные экстремистские группы. В июле «Хакерство для вас» получило запрос на поддельные паспорта от лиц, связанных с насильственной экстремистской группировкой «Бримстоун». Группа, которая физически расположена и действует за пределами Северной земли, известна своими жестокими и громкими нападениями на уязвимые цели по всему региону, в том числе в соседних Саутани, Вестландии и Истополисе. Представив плату авансом, «Хакерство для вас» принимает запрос от Бримстоуна и начинает изготавливать для них несколько поддельных паспортов.

В течение нескольких недель Бримстоун получает партию поддельных паспортов, в которых лица членов группы сочетаются с незаконно полученными изображениями лиц граждан из Терре-Норт, Саутани, Вестландии и Истополиса. Это позволяет членам группы путешествовать туда и обратно через границы незамеченными, поскольку сотрудники пограничного контроля, как правило, быстро проверяют имя, идентификационный номер и фотографию путешественника. Первоначально Бримстоун использует эту возможность для содействия некоторым из своих незаконных действий, которые финансируют группу, включая похищение людей и выкуп, незаконную добычу полезных ископаемых, вымогательство, а также производство и распространение наркотиков.

Однако вскоре они понимают, что эти паспорта обладают еще большим потенциалом. После нескольких недель обсуждений Бримстоун останавливается на своем следующем громком нападении: серии последовательных взрывов на ключевых объектах в столице Вестландии, включая станции метро, общественную площадь, спортивное сооружение, больницу и Верховный суд города. Бримстоун считает, что в условиях неразберихи, которая возникнет в результате последовательных атак, нападавшие смогут быстро и тихо пересечь границу, которая находится всего в 100 километрах к востоку от столицы, и вернуться на Север Земли незамеченными, используя свои новые поддельные паспорта. Уверенный в том, что они смогут успешно избежать захвата, Бримстоун решает продолжить выполнение плана, остановившись на середине октября для атаки.

VIII. ОЦЕНКА УГРОЗЫ

Рассмотрев текущее положение дел с точки зрения использования ИИ террористами и выявив несколько гипотетических, но мыслимых примеров, демонстрирующих, как террористы могли бы использовать эту технологию, остается один важный вопрос: есть ли основания для беспокойства в отношении террористических групп или отдельных лиц, непосредственно

использующих ИИ способами, аналогичными описанным в вымышленных сценариях, описанных в предыдущей главе?

Прежде чем обратиться к этому вопросу, разумно отметить, как полагает Ван дер Вир, что в дискуссиях об использовании технологий террористами существуют «ставки и повестки дня». Она отмечает, что консультанты и другие частные организации могут быть заинтересованы в поддержании паникерского повествования о проблемах, по которым они продают свои услуги. Аудиториям, не являющимся экспертами, участвующим в дебатах, следовательно, может быть трудно провести различие между предвзятыми или подверженными влиянию повествованиями и устойчивыми или нейтральными утверждениями, особенно когда эти дебаты сосредоточены на сугубо технических вопросах.

Принимая это во внимание, в данной главе предпринимается попытка объективно поразмыслить над вышеупомянутым вопросом, проанализировав уровень угрозы террористического использования ИИ в попытке прийти к какому-либо выводу. Термин «угроза» обычно понимается как сочетание намерения и возможностей. Оба термина будут рассмотрены в следующих разделах.

А. Намерение

Учитывая характер терроризма, трудно установить намерения каких-либо террористических групп или отдельных лиц. Тем не менее, для оценки намерения террористов использовать ИИ есть смысл рассмотреть пригодность этой технологии для терроризма. В своем анализе того, как открытые технологические инновации вооружают террористов завтрашнего дня, Кронин перечисляет характеристики, которые, по ее мнению, негосударственные субъекты ищут в инновационном оружии. Кронин считает, что инновационное оружие должно быть доступным, дешевым, простым в использовании, транспортабельным, скрытым и эффективным – характеристики, которыми ИИ не обязательно обладает. Реальность такова, что ИИ не совершенен.

Вопреки его частому представлению в популярной культуре и средствах массовой информации, ИИ не является серебряной пулей. Он может потерпеть неудачу, и очень часто это действительно происходит. По данным VentureBeat 87% проектов в области науки о данных никогда не доводятся до производства. TechRepublic сообщает, что 56% глобальных руководителей не ожидают какой-либо отдачи от инвестиций в течение 3-5 лет. Успешная разработка и внедрение ИИ эффективным и надежным способом требует значительного времени, денег и усилий. Как предполагает Хоффман, есть веские причины для того, чтобы террористические группы более века придерживались двух основных систем оружия – огнестрельного оружия и взрывчатых веществ: они эффективны и надежны.

С другой стороны, Кронин также отмечает, что инновационное оружие должно быть полезным в широком спектре контекстов, чтобы быть привлекательным для террористов. Оно должно быть частью кластера технологий, которые могут усилить их воздействие, иметь символический резонанс и могут быть использованы в неожиданных целях. В отличие от предыдущего набора характеристик, можно утверждать, что ИИ во многом соответствует этому описанию и подтверждает возможность того, что террористы заинтересованы в этой технологии.

Несмотря на этот анализ, как уже отмечалось, появились некоторые ранние признаки интереса со стороны террористических групп или отдельных лиц к ИИ и связанным с ним технологиям. Беспилотные летательные аппараты, например, все чаще интегрируются в методы работы таких групп, как ИГИЛ. Более того, еще раз размышляя над обширной историей того, как такие группы внедряли инновации и новые технологии в прошлом, разумно рассмотреть возможность того, что террористические организации в какой-то степени намерены исследовать или стремиться понять, как ИИ может быть использован в злонамеренных целях.

B. Возможности

Способность террористических групп или отдельных лиц разрабатывать или внедрять ИИ вполне может быть аспектом «сделать или сломать» в этом анализе.

Нельзя отрицать, что возможности ИИ быстро растут по всему миру, и технологии ИИ, а также средства для разработки и внедрения этих технологий, могут быть приобретены на коммерческой основе, а некоторые даже с открытым исходным кодом. Например, TensorFlow, библиотека с открытым исходным кодом для крупномасштабного машинного обучения и численных вычислений, позволяет пользователям легко создавать нейронную сеть с простым обнаружением объектов или даже модель распознавания лиц без необходимости сложных навыков или компьютеров. Github – еще одна платформа с открытым исходным кодом, которая может снизить порог использования и доступа, увеличивая возможность злоумышленников, таких как террористы, использовать ИИ. Тем не менее, одной доступности технологии недостаточно, если не существует возможностей, необходимых для ее использования.

Изучая уровень технических возможностей, эксперты склонны предполагать, что террористические группы, такие как ИГИЛ, не проводили эффективных и сложных кибератак и атак на основе технологий, потому что у них нет необходимых возможностей или финансирования или они просто недостаточно организованы для этого. Даже если создание ИГИЛ Единого Кибер-халифата является тревожным событием, тем не менее, считается, что группа находится в зачаточном состоянии. На самом деле, группа использует методы, используемые так называемыми «детишками-сценаристами» – низкоквалифицированные хакеры, которые используют сценарии или программы, разработанные другими, для проведения своих атак, на самом деле, не понимая, как они работают. Несмотря на это, исследователи Flashpoint предположили, что «готовность адаптироваться и развиваться, чтобы быть более эффективными и получать больше поддержки, указывает на то, что, хотя эти участники все еще неискушенны, их способность

учиться, поворачиваться и реорганизовываться представляет растущую угрозу». Даже если такие группы, как Объединенный кибер-халифат, в настоящее время могут не обладать техническими возможностями, необходимыми в их рядах, действия таких групп, вероятно, поразят воображение других и со временем могут стимулировать следующее поколение более способных кибертеррористов.

Вместо того, чтобы иметь собственную команду экспертов или собственные технические возможности для проведения более сложных кибератак и теоретического запуска атаки с использованием ИИ, террористические группы и отдельные лица могут в качестве альтернативы использовать возможности из других источников. Например, было замечено, что в целях кибертерроризма некоторые организации, вдохновляемые «Аль-Каидой»/ИГИЛ, объединили свои силы даже с группами, которые не идентифицируются с их повесткой дня. В свете развивающейся и многогранной связи между организованной преступностью и терроризмом и появлением модели «преступление как услуга», в соответствии с которой инструменты торговли киберпреступностью продаются за денежную стоимость, для таких низкоквалифицированных террористических групп может оказаться возможным просто приобрести готовые или изготовленные на заказ алгоритмы «с полки», готовые к использованию, или воспользоваться услугами таких систем. В качестве примера потенциала этой модели «преступление как услуга», в ноябре 2020 года активистка за цифровые права, как сообщается, приобрела доступ к московской системе распознавания лиц за 16 000 рублей (примерно 200 долларов США) по объявлению, размещенному в Telegram. Вскоре после оплаты этого сбора активистка смогла получить подробный отчет о своих перемещениях, зарегистрированных в системе распознавания лиц за предыдущие месяцы. В этом смысле террористическим организациям необязательно быть способными самостоятельно разрабатывать такие технологии, но они могут осуществлять атаки из внешних источников через черный рынок для «хакеров по найму» или других гнусных преступных групп,

обеспечивая большую прямую корреляцию между криминальной доступностью и террористическими возможностями.

Кроме того, всегда существует риск того, что уже разработанные сложные технологии окажутся в чужих руках. В связи с растущим интересом к беспилотным летательным аппаратам и их использованию в зонах конфликтов, а также к разработке и развертыванию все более автономных систем вооружения в боевых условиях, существует опасение, что такое оружие может быть захвачено или незаконно приобретено или приобретено негосударственными субъектами, такими как террористические группы. Возможность этого на самом деле является одним из аргументов, часто используемых экспертами, призывающими к запрету на разработку автономных систем оружия.

В конечном счете, хотя может показаться, что таким группам, как ИГИЛ, не хватает возможностей для самостоятельного проектирования, разработки и внедрения ИИ, нельзя исключать возможность того, что такие группы или отдельные лица приобретут возможности для развертывания этих технологий. Разумно отметить, что исторически значительные достижения в плане возможностей происходили в течение относительно коротких промежутков времени. Показательно, что ИГИЛ потребовалось менее года, чтобы успешно использовать беспилотные летательные аппараты в своих операциях после того, как они проявили первоначальный интерес к использованию этой технологии в качестве части своего репертуара. Даже если на данный момент наиболее актуальными технологиями являются те, которые имеют низкие барьеры для входа, злоумышленники, скорее всего, со временем будут наращивать свои навыки для более продвинутых атак.

C. Причины для беспокойства?

В 2004 году Комиссия Соединенных Штатов по расследованию событий 11 сентября опубликовала свой доклад о событиях, приведших к террористическим актам 11 сентября 2001 года в Соединенных Штатах.

В этом докладе Комиссия подчеркнула опасность провалов воображения и зашла так далеко, что поощряла институционализацию воображения при оценке террористических угроз в будущем. Размышляя об этих трудно изученных уроках, разумно рассмотреть угрозу террористического использования ИИ как возможность. Даже если оценки террористических намерений или возможностей в настоящее время не являются полностью окончательными, в интересах того, чтобы не быть застигнутыми врасплох, целесообразно проявлять осторожность в отношении предыдущей оценки намерений и возможностей.

Как уже неоднократно отмечалось и затрагивалось в настоящем докладе, технологии играют определенную роль в формировании форм терроризма. Учитывая быструю интеграцию ИИ в повседневную жизнь, можно сказать, что больше не может оставаться низкой вероятность того, что террористические группы и отдельные лица не будут использовать технологии на основе ИИ в не слишком отдаленном будущем – будь то одно или несколько злонамеренных применений, описанных в этом отчете, или каким-либо другим, все еще невообразимым способом. В этой связи не следует упускать из виду прогресс и развитие ИИ и растущий интерес террористических групп и отдельных лиц к этим и связанным с ними технологиям.

Как бы то ни было, есть и другая сторона медали, которая заслуживает рассмотрения. Энди Патель, исследователь из F-Secure, предположил, что современным системам ИИ больше следует опасаться людей, чем людям следует опасаться ИИ. В этой связи он отмечает, что террористические группы и отдельные лица с большей вероятностью будут злоупотреблять системами ИИ, а не использовать их как часть своих атак.

Соответственно, есть смысл отметить одно последнее различие, прежде чем завершить это рассмотрение пересечения ИИ и терроризма: различие между использованием и злоупотреблением ИИ. В то время как злонамеренное использование ИИ касается злоумышленников, использующих ИИ, например,

для повышения эффективности атаки, злоупотребление ИИ касается атак, направленных на функционирование или функциональность ИИ, путем манипулирования ими с помощью физических и/или кибер-возможностей. Такое использование/злоупотребление динамикой можно рассматривать в отношении других технологий, включая, например, виртуальные активы. Хотя такие активы, безусловно, используются для содействия киберпреступности, криптоактивы и предприятия все чаще становятся мишенью для хакеров и мошенников. Злоупотребление ИИ, по сути, повлечет за собой такие ситуации, как террористическая группа, провоцирующая атаку на систему ИИ или пытающаяся помешать такой системе. По мере того как ИИ все больше интегрируется в системы как в государственном, так и в частном секторе, возникают новые уязвимости, особенно когда такие системы встроены в критически важную инфраструктуру. Недавняя попытка хакера отравить водоочистную станцию во Флориде демонстрирует масштабы, которые традиционная кибератака на критическую инфраструктуру может оказать на все население города.

Хотя сфера возможностей злоупотребления ИИ довольно широка, возможно несколько сценариев. Одной из таких возможностей является взлом технологии ИИ, используемой национальными властями или организациями, утечка информации, которая затем может быть использована в террористических целях. По мере того как общество становится все более зависимым от данных, а конфиденциальные данные собираются как правительствами, так и частными субъектами, вероятность компрометации и повреждения данных возрастает пропорционально.

Другая одна очень заметная возможность – взлом автономных транспортных средств. Еще в начале 2000-х годов потенциал для взлома автомобилей был очевиден, когда исследователи продемонстрировали способность взломать Ford Escape и отключить его тормоза в 2013 году и остановить Jeep Cherokee посреди автомагистрали между штатами США в 2015 году. По мере того, как ИИ продолжает проникать в автомобильную

промышленность, а автомобили становятся все более автономными и подключенными к ИИ, возможности злоумышленников взломать одну или несколько из сотен миллионов строк кода, которые входят в программы управления этих транспортных средств, значительно возрастают.

Все еще находясь в сфере автономных транспортных средств, дальнейшее злоупотребление ИИ может включать злоупотребление системами распознавания изображений. Как отмечалось, модели машинного обучения, на которые полагаются автономные транспортные средства, зависят от точности получаемой ими информации. Если эта информация будет скомпрометирована, то же самое произойдет и с самим транспортным средством. В начале 2020 года хакеры обманули систему автопилота в двух разных моделях Tesla, заставив ее разгоняться до 85 миль в час вместо 35 миль в час, наклеив ленту на знак ограничения скорости. Аналогичным образом, разместив небольшие наклейки на дороге, исследователям также удалось вытолкнуть другую Tesla на полосу встречного движения. Вредоносный потенциал террористических групп или отдельных лиц для создания хаоса с помощью такого рода злоупотреблений очевиден.

Аналогичные методы также могут быть использованы в связи с нападением, чтобы привести людей в целевые районы или задержать прибытие сил безопасности и/или экстренных служб на место после нападения, тем самым усилив его последствия. Одно недавнее исследование показало, что даже относительно небольшого взлома самоуправляемых автомобилей будет достаточно, чтобы вызвать столкновения и затор. Исследование показало, что, взломав 10-20% транспортных средств в час пик на Манхэттене, можно было бы сделать половину города практически недоступной.

Еще одним злоупотреблением, заслуживающим упоминания, является возможность вмешательства злоумышленников в службы или приложения, использующие ИИ, путем изменения параметров, используемых системой, или «отравления» наборов данных, используемых для обучения системы, путем предоставления им неверных данных. При этом злоумышленники могут

успешно направить систему ИИ в желаемом направлении или, например, генерировать ошибочные или предвзятые результаты. Например, в 2016 году новый чат-бот машинного обучения Microsoft, известный как «Tay», был преждевременно закрыт после того, как он начал публиковать подстрекательские и оскорбительные твиты вскоре после своего выпуска. Функция машинного обучения чат-бота была злонамеренно нацелена, причем Tay намеренно использовал расистские, женоненавистнические и антисемитские выражения скоординированным образом, чтобы повлиять на то, как чат-бот будет публично озвучивать себя в Twitter. Еще один простой, но эффективный пример потенциального вмешательства в правильное функционирование 55 систем на основе ИИ произошел в феврале 2020 года, когда немецкий художник обманул Google Maps, заставив поверить, что трафик на улицах Берлина был выше, чем на самом деле, путем подачи неверных данных в модели машинного обучения Google Map. Художнику удалось это сделать, имея при себе 99 мобильных телефонов, когда он шел по улицам, Google Maps неправильно понимал и оценивал это как представление людей в их автомобилях, в результате чего система работала неправильно. И здесь снова проявляется вредоносный потенциал. Такие уловки или целенаправленная эксплуатация могут быть мощными инструментами для создания хаоса и путаницы при злонамеренном использовании. Например, в городских районах, где люди все больше зависят от таких картографических приложений для создания своих маршрутов, террористы, создающие поддельные данные о пробках на дорогах, могут привести толпы людей в определенные районы перед совершением своих нападений или еще раз предотвратить раннее прибытие сил безопасности и/или экстренных служб к месту их нападений.

Следовательно, при рассмотрении вопроса о злонамеренном использовании ИИ в террористических целях также важно учитывать другую сторону медали: злонамеренное злоупотребление ИИ. В отличие от злонамеренного использования ИИ террористами, угроза злоупотреблений,

возможно, в большей степени соответствует существующим возможностям террористических групп и отдельных лиц и может быть чрезвычайно эффективной в расширении существующих методов нападения и содействии «терроризму как театру действий».

IX. ОТ ОЦЕНОК К ДЕЙСТВИЯМ

Хотя использование ИИ в террористических целях, безусловно, не является развитой угрозой, терроризм далек от застоя. В настоящее время технические возможности террористических групп и отдельных лиц по внедрению таких технологий, как ИИ, могут считаться низкими, но важно не недооценивать их намерение воспользоваться последними технологическими тенденциями, а также их расширяющиеся возможности для этого. По мере того как ИИ и связанные с ним технологии становятся все более доступными для общественности, те, кто отвечает за борьбу с терроризмом, должны быть на шаг впереди. В то же время, даже если терроризм, связанный с ИИ, может и не представлять непосредственной угрозы, крайне важно сохранять бдительность в отношении потенциального злоупотребления системами ИИ террористическими группами и отдельными лицами. Это все более тревожный аспект, учитывая темпы интеграции ИИ в процессы как в государственном, так и в частном секторе, включая важнейшую инфраструктуру.

В связи с этим для органов по борьбе с терроризмом и правоохранительных органов, а также для директивных органов, промышленности и научных кругов предлагаются следующие рекомендации для рассмотрения в будущем и для руководства последующими действиями по наращиванию потенциала для подготовки к возможному будущему терроризма с использованием ИИ. Эти рекомендации были составлены и классифицированы на основе отзывов, полученных от участников Совещания Группы экспертов КТЦООН/ЮНОКТ-ЮНИКРИ. Порядок рекомендаций не следует толковать как указание на какой-либо конкретный приоритет.

Дальнейшие исследования

– Следует отслеживать эволюцию внедрения ИИ террористическими группами и отдельными лицами.

– Следует провести дополнительные консультации в рамках исследовательского сообщества на основе этого отчета, чтобы получить дополнительные доказательства и обратную связь, с тем чтобы определить приоритеты будущих исследований.

– Следует дополнительно оценить потенциальную угрозу кибератак террористических групп или отдельных лиц на системы ИИ или на целостность данных, используемых в системах ИИ, особенно в контексте критической инфраструктуры.

– Правовые аспекты, связанные со злонамеренным использованием или злоупотреблением ИИ, должны быть рассмотрены и проанализированы.

– Следует продолжить изучение конвергенции ИИ с другими технологическими достижениями, включая биотехнологии, интерфейс мозг-компьютер, а также извлечение и обработку данных.

Сотрудничество с участием многих заинтересованных сторон

– Круг заинтересованных сторон, участвующих в обсуждениях, касающихся использования ИИ в террористических целях, должен быть расширен до всех уровней и всех регионов.

– Следует поощрять и поддерживать диалог и сотрудничество между техническими и нетехническими экспертами.

Необходимо тесно взаимодействовать с исследовательским сообществом ИИ в повышении осведомленности о возможном вредоносном использовании разрабатываемых технологий.

Знания и осведомленность в исследовательском сообществе должны формироваться с самых ранних стадий технологического развития,

ориентируясь, например, на студенческое сообщество и исследователей, ищущих гранты.

– Следует развивать грамотность политиков в области технологий, включая потенциальное злонамеренное использование и злоупотребления.

Следует проявлять осторожность, чтобы поощрять осторожность, избегая при этом чрезмерного раздувания уровня угрозы и характера сценариев угроз.

Наращивание потенциала

– Необходимо расширить возможности всех заинтересованных сторон по выявлению и реагированию на угрозу злонамеренного использования ИИ и злоупотреблений им в террористических целях.

– Следует организовать мероприятия по упорядочению сотрудничества и координации и обмену опытом между заинтересованными сторонами.

Политика и руководящие указания

– Государствам и организациям следует рассмотреть и разработать четкие стратегии и практические руководящие принципы реагирования на нападения с использованием ИИ чтобы обеспечить надлежащие и адекватные ответные меры на такие нападения, которые соответствуют ценностям, закрепленным в Уставе Организации Объединенных Наций, Всеобщей декларации прав человека и нормах и стандартах международного права.

– Следует изучить процессы регулирования и сертификации для обеспечения защиты систем ИИ от недобросовестного использования и обеспечения подотчетности в случае их неправильного использования.

Использование ИИ в борьбе с терроризмом

– Следует изучить использование ИИ и связанных с ним новейших технологий для противодействия террористическим угрозам с использованием ИИ, в частности для противодействия террористической радикализации и распространения позитивных повествований.

– Необходимо провести всеобъемлющее и углубленное картирование взаимосвязи с поддержкой ИИ и борьбой с терроризмом.

– Права человека должны быть в центре любого такого использования ИИ для борьбы с терроризмом, включая противодействие злонамеренному использованию и злоупотреблению ИИ в террористических целях.

UNITED NATIONS
OFFICE OF COUNTER-TERRORISM
UN Counter-Terrorism Centre (UNCCT)

unicri
United Nations
Interregional Crime and Justice
Research Institute

ПРОТИВОДЕЙСТВИЕ ТЕРРОРИЗМУ ОНЛАЙН С ПОМОЩЬЮ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Обзор для правоохранительных и контртеррористических органов в Южной Азии и Юго-Восточной Азии

Перевод с английского совместного доклада ЮНИКРИ и Контртеррористического центра ООН

Отказ от ответственности

Мнения, выводы, заключения и рекомендации, изложенные в настоящем документе, не обязательно отражают мнения Объединенных Наций, правительства Японии или любых других участвующих национальных, региональных или глобальных организаций. Более того, ссылка на какой-либо конкретный инструмент или приложение в настоящем докладе не должна рассматриваться как одобрение со стороны КТООН, ЮНИКРИ или самой Организации Объединенных Наций.

Используемые обозначения и материалы, представленные в этой публикации, не подразумевают выражения какого-либо мнения со стороны Секретариата Организации Объединенных Наций относительно правового статуса какой-либо страны, территории, города или района ее властей или относительно делимитации ее границ.

Благодарности

Настоящий доклад является результатом совместной исследовательской инициативы по борьбе с терроризмом в эпоху искусственного интеллекта Группы кибербезопасности и новых технологий Контртеррористического центра Организации Объединенных Наций (КТЦООН) Управления Организации Объединенных Наций по борьбе с терроризмом (ЮНОКТ) и Межрегионального научно-исследовательского института Организации Объединенных Наций по вопросам преступности и правосудия (ЮНИКРИ) через его Центр искусственного интеллекта и робототехники. Совместная исследовательская инициатива финансировалась за счет щедрых взносов Японии.

Предисловие

Искусственный интеллект (ИИ) может оказать и уже оказывает глубокое влияние на наше общество – от здравоохранения, сельского хозяйства и промышленности до финансовых услуг и образования. Однако, как заявил Генеральный секретарь Организации Объединенных Наций Антониу Гутерриш в своей Стратегии по новым технологиям на 2018 год «хотя эти технологии имеют большие перспективы, они не свободны от рисков, а некоторые вызывают беспокойство и даже страх. Они могут быть использованы в злонамеренных целях или иметь непреднамеренные негативные последствия». ИИ воплощает эту двойственность, возможно, больше, чем любая другая появляющаяся сегодня технология. Хотя это может привести к улучшению во многих секторах, оно также может препятствовать осуществлению прав человека и основных свобод – в частности, прав на неприкосновенность частной жизни, свободу мысли и выражения мнений и недискриминацию. Таким образом, любое исследование использования технологий с поддержкой ИИ всегда должно идти рука об руку с усилиями по предотвращению потенциальных нарушений прав человека.
В этом контексте мы наблюдали, как многие международные и региональные организации, национальные органы власти и организации гражданского

общества работают над инициативами, направленными на внедрение этических принципов, касающихся использования ИИ, а также появление протоправовых рамок.

Эта двойственность наиболее очевидно распространена в Интернете, где рост террористической активности является растущей проблемой, которая становится почти синонимом современного терроризма. Учтите, что в рамках Дня действий по обращению к 2020 году Европол и 17 государств-членов выявили и оценили на предмет удаления до 1906 URL-адресов, ссылающихся на террористический контент на 180 платформах и веб-сайтах за один день. Facebook указал, что в течение двух лет он удалил более 26 миллионов единиц контента от таких групп, как Исламское государство Ирак и Левант (ИГИЛ) и «Аль-Каида». Интернет и социальные сети оказываются мощными инструментами в руках таких групп, позволяя им общаться, распространять свои сообщения, собирать средства, вербовать сторонников, вдохновлять и координировать атаки, а также нацеливаться на уязвимых людей.

В Глобальной контртеррористической стратегии Организации Объединенных Наций (A/RES/60/288) государства-члены приняли решение сотрудничать с Организацией Объединенных Наций с должным учетом конфиденциальности, уважения прав человека и в соответствии с другими обязательствами по международному праву, изучить пути координации усилий на международном и региональном уровнях по противодействию терроризму во всех его формах и проявлениях в Интернете и использовать Интернет в качестве инструмента противодействия распространению терроризма. В то же время в Стратегии признается, что государствам-членам может потребоваться помощь для выполнения этих обязательств.

В настоящем докладе – продукте партнерства между Контртеррористическим центром Организации Объединенных Наций в Управлении Организации Объединенных Наций по борьбе с терроризмом и Межрегиональным научно-исследовательским институтом Организации Объединенных Наций по вопросам преступности и правосудия через его Центр

искусственного интеллекта и робототехники – мы стремимся изучить, как ИИ может быть использован для борьбы с угрозой терроризма в Интернете.

Признавая угрозу терроризма, растущие темпы цифровизации и растущее число молодых, уязвимых и онлайновых групп населения в Южной и Юго-Восточной Азии, настоящий доклад содержит рекомендации для правоохранительных и контртеррористических учреждений в Южной и Юго-Восточной Азии по потенциальному применению ИИ для борьбы с терроризмом в Интернете, а также по правам человека, техническим и политическим проблемам, которые им необходимо будет рассмотреть и решить, если они решат это сделать.

Наша работа на этом не заканчивается. Решение проблем, выявленных в этом докладе, и раскрытие потенциала использования ИИ для борьбы с терроризмом потребует дальнейшего углубленного анализа. Наши отделения готовы поддержать государства-члены и других партнеров по борьбе с терроризмом в целях предотвращения всех форм его проявления, а также изучения новаторских подходов в соблюдении прав человека.

Владимир Воронков
Заместитель Генерального секретаря
Управления ООН по борьбе
с терроризмом
Исполнительный директор
Контртеррористического центра ООН

Антония Мари Де Мео
Директор Межрегионального
научно-исследовательского института
ООН по вопросам преступности
и правосудия

ОСНОВНЫЕ ПОЛОЖЕНИЯ

В последние годы интеграция цифровых технологий в повседневную жизнь в Южной и Юго-Восточной Азии растет необычайными темпами, при этом использование социальных сетей преимущественно молодым населением регионов превышает среднемировой показатель. Хотя эта тенденция открывает широкий спектр возможностей для развития, свободы выражения мнений, участия в политической жизни и гражданских действий, она также увеличивает риск того, что потенциально уязвимая молодежь может подвергнуться воздействию террористического онлайн-контента, создаваемого террористическими и экстремистскими группами в Интернете. Кроме того, учитывая устоявшееся присутствие террористов и насильственных в Южной и Юго-Восточной Азии, правоохранительным органам и контртеррористическим учреждениям в этих регионах все чаще приходится приспосабливаться к изменениям в преступной и террористической деятельности, а также к тому, как проводятся расследования этой деятельности.

ИИ уделяется значительное внимание во всем мире как инструменту, который может обрабатывать огромные объемы данных и обнаруживать закономерности и корреляции в данных, невидимых человеческому глазу, что может повысить эффективность анализа сложной информации. Как технология общего назначения, преимущества ИИ также могут быть использованы в области борьбы с терроризмом. В свете этого среди правоохранительных органов и контртеррористических ведомств во всем мире растет интерес к изучению того, как можно раскрыть преобразующий потенциал ИИ.

Учитывая вышеупомянутые тенденции и события, настоящий доклад служит введением в использование ИИ для борьбы с терроризмом в Интернете для правоохранительных и контртеррористических учреждений в регионах Южной и Юго-Восточной Азии. Настоящий отчет носит ознакомительный характер в связи с ограниченным объемом общедоступной информации

о степени технологической готовности правоохранительных и контртеррористических органов в этих регионах, что, как считается, может свидетельствовать об ограниченном опыте использования этой технологии. В этой связи в докладе дается широкая оценка различных вариантов использования ИИ, демонстрируются возможности технологии, а также устраняются проблемы. Отчет призван послужить первоначальным отображением ИИ, контекстуализируя возможные варианты использования технологии, которые теоретически могут быть развернуты в регионах, в то же время сопоставляя это с ключевыми проблемами, которые власти должны преодолеть, чтобы обеспечить ответственное использование ИИ и соблюдение прав человека. Учитывая его вводный характер, этот доклад ни в коем случае не предназначен для того, чтобы быть исчерпывающим обзором применения ИИ для борьбы с терроризмом в Интернете.

Доклад состоит из пяти глав. В первой главе дается общее введение в контекст терроризма, использования Интернета в Южной и Юго-Восточной Азии и ИИ. Во второй главе представлены и объясняются некоторые ключевые термины, технологии и процессы, имеющие отношение к данному отчету с технической точки зрения. В третьей главе показаны области применения ИИ в контексте противодействия использованию террористами Интернета и социальных сетей, с акцентом на шесть выявленных случаев использования, а именно:

1) прогнозная аналитика террористической деятельности;

2) выявление красных флагов радикализации;

3) выявление ложной информации и дезинформации, распространяемой террористами в стратегических целях;

4) автоматическая модерация и удаление контента;

5) противодействие террористическим и насильственным экстремистским агитационным рассказам;

6) управление большими требованиями к анализу данных.

В четвертой главе рассматриваются проблемы, которые правоохранительные органы и контртеррористические учреждения должны быть готовы решать при изучении технологии, в частности конкретные политические и правовые проблемы, а также технические вопросы. Доклад завершается пятой и заключительной главой, в которой содержатся рекомендации высокого уровня для правоохранительных органов и контртеррористических учреждений в Южной и Юго-Восточной Азии, которые следует принять во внимание, чтобы помочь им справиться с проблемами, описанными с точки зрения использования ИИ для борьбы с терроризмом в Интернете.

I. ВВЕДЕНИЕ

Южная и Юго-Восточная Азия, как и многие другие регионы мира, борются с угрозой терроризма и насильственного экстремизма. Это включает как местные организованные воинствующие экстремистские группы, такие как «Джемаа Исламия», так и группы, ориентированные на международных союзников, такие как «Исламское государство Ирака и Леванта» (ИГИЛ, также известное как ДАИШ) и «Аль-Каида», в которую входят местные аффилированные группы, такие как группа Абу Сайяфа.

Эти регионы стали важными областями сосредоточения внимания террористических и насильственных экстремистских групп с точки зрения вербовки. На пике своего развития в 2015 году более 30 000 иностранных боевиков-террористов из более чем 100 государств, как считалось, присоединились к ИГИЛ. Из этого числа более 1500 человек только из Южной и Юго-Восточной Азии, как полагают, прибыли на территорию, контролируемую ИГИЛ. К июлю 2017 года, когда ИГИЛ начало терять значительную часть своей территории, в регионах Южной и Юго-Восточной Азии наблюдалось значительное число иностранных боевиков, возвращающихся в свои страны, а также значительное число иностранных боевиков, родом не из этих регионов, перебирающихся в Южную

и Юго-Восточную Азию вместо возвращения в свои родные страны. Радикализация представляет растущую угрозу в регионах. Например, Министерство внутренних дел и законодательства Сингапура недавно указало, что сроки набора персонала были сокращены примерно с двадцати двух до девяти месяцев. В условиях терроризма в Юго-Восточной Азии также заметно возросло число женщин, участвующих в терроризме. Считается, что это увеличение числа женщин, участвующих в терроризме, связано с более широкими тенденциями все более самостоятельных террористических нападений, совершаемых террористами-одиночками или группами. Пандемия COVID-19 также оказала влияние на явление, связанное с радикализацией и вербовкой, со многими государствами-членами, в том числе из Южной и Юго-Восточной Азии, которые выражают озабоченность по поводу радикализации в контексте большого числа людей, подключенных к Интернету в течение длительных периодов времени.

Присутствие террористов и насильственных экстремистов в Южной и Юго-Восточной Азии, однако, не является чем-то новым, поскольку каждый из этих регионов имеет свой собственный опыт борьбы с различными формами национального, регионального и международного насильственного экстремизма и накопил большой опыт в борьбе с терроризмом. Взрыв во Всемирном торговом центре Коломбо в октябре 1997 года, взрывы на Бали в октябре 2002 года, взрыв Супер-парома 14 в Манильском заливе в феврале 2004 года и теракты в Мумбаи в ноябре 2008 года – все это свидетельствует о тех испытаниях, с которыми столкнулись регионы.

Еще одной глобальной тенденцией, с которой регионы Южной и Юго-Восточной Азии столкнулись в последние годы, является «оцифровка». Действительно, интеграция цифровых технологий в повседневную жизнь в Южной и Юго-Восточной Азии – это то, что растет необычайными темпами. Хотя единого фактора не существует, ключевым фактором, который часто признается, является большой процент молодежи во всех регионах. Примечательно, что более 70,2% населения Южной и Юго-Восточной Азии

моложе 40 лет. Это молодое население исключительно активно в Интернете: «более 55% активно пользуются социальными сетями, что на 13% больше, чем в среднем по миру». Как и в случае с молодыми поколениями по всему миру, многие из них являются так называемыми «цифровыми уроженцами» – людьми, родившимися или выросшими в цифровую эпоху и обладающими высоким уровнем знакомства с компьютерами, Интернетом и цифровыми технологиями с раннего возраста – и, таким образом, имеют более высокое признание услуг, связанных с Интернетом, и являются восторженными пользователями социальных сетей. В соответствии с этим Ассоциация государств Юго-Восточной Азии (АСЕАН), что характерно, является самым быстрорастущим интернет-рынком в мире, где 125 000 новых пользователей ежедневно подключаются к Интернету. Сообщалось, что почти 60% глобальных пользователей социальных сетей в 2020 году находились в Азии. Пандемия COVID-19 в равной степени сыграла свою роль в ускорении процесса оцифровки в регионах, молодежь в Южной и Юго-Восточной Азии расширяет свое цифровое присутствие в течение 2020 года и более чем на 70% верит в то, что их более широкое использование социальных сетей продлится и после пандемии. По данным респондентов Опроса молодежи АСЕАН 2020, проведенного Всемирным экономическим форумом, использование социальных сетей выросло больше всего по сравнению с другими онлайн-сервисами.

Естественно, эти разработки открывают широкий спектр возможностей при условии их надлежащего использования. Интернет и социальные сети неоднократно демонстрировали свой благотворный потенциал в Южной и Юго-Восточной Азии, например, в качестве ускорителя активности на низовом уровне. Исследования, проведенные в Юго-Восточной Азии за последнее десятилетие, продемонстрировали положительную корреляцию между использованием социальных сетей, участием в политической жизни и гражданскими действиями как в демократических, так и в авторитарных системах. К сожалению, однако, преимущества Интернета и социальных сетей, которые поддерживают движения гражданского общества, также делают

их привлекательными для участников со злым умыслом и создают множество проблем для властей в Южной и Юго-Восточной Азии, а также во всем мире.

Террористы и воинствующие экстремисты во всем мире адаптировались к новым цифровым парадигмам 21 века, научившись использовать информационные и коммуникационные технологии, в частности онлайн-пространства и множество интерактивных приложений и платформ социальных сетей, для достижения своих целей – например, для распространения ненавистной идеологии и пропаганды, вербовки новых членов, организации финансовой поддержки и оперативной тактики и управления поддерживающими онлайн-сообществами. Использование таких технологий в Южной и Юго-Восточной Азии аналогично использованию в других частях мира, при этом социальные сети и сильно локализованный контент, адаптированный к местным жалобам и доступный на местных языках, играют особенно важную роль в радикализации и вербовке. Например, по словам бывшего Министра внутренних дел Малайзии Ахмада Захида Хамиди, социальные сети ответственны примерно за 17% вербовки ИГИЛ в стране. Аналогичным образом, в Сингапуре из 21 гражданина, задержанного за деятельность, связанную с терроризмом, в соответствии с Законом о внутренней безопасности в период с 2015 по 2018 год, 19 были радикализированы пропагандой ИГИЛ в Интернете, в то время как два других радикализируются другим онлайн-контентом, поощряющим участие в сирийском конфликте. Актуальность таких информационно-коммуникационных технологий в этих регионах в последние годы также прослеживается в национальных ответных мерах. Например, в Индонезии Министерство связи и информационных технологий обратилось к зашифрованному приложению для обмена сообщениями Telegram с просьбой создать специализированную группу модераторов, знакомых с индонезийскими языками, для конкретной модерации террористического контента, распространяемого в Индонезии.

В дополнение к необходимости понимания расширяющегося ландшафта угроз за пределами физической области, правоохранительные органы и контртеррористические учреждения проходят испытания и сталкиваются с необходимостью проведения обширных и сложных расследований в условиях все большего объема данных, которые выходят за рамки их традиционных областей знаний. Крупные дела могут потребовать нескольких лет работы для поиска и перекрестной проверки соответствующей информации по делу, а это означает, что найти одну ключевую информацию или выделить наиболее важные зацепки для целей расследования никогда не было так сложно. Таким образом, 22 правоохранительных и контртеррористических учреждения по всему миру вынуждены идти в ногу с цифровыми преобразованиями.

Столкнувшись с реальностью, что неспособность идти в ногу может привести к неспособности воспрепятствовать террористическому заговору и привести к гибели людей, растет интерес к изучению инструментов, методов или процессов для заполнения пробелов в оперативной деятельности и потенциале правоохранительных и контртеррористических учреждений в борьбе с терроризмом в Интернете. Одной областью, которая вызывает значительный интерес во всем мире как со стороны организаций государственного, так и частного секторов, сталкивающихся с аналогичными «информационными перегрузками», является ИИ. Как будет объяснено в следующей главе, ИИ – это область компьютерных наук, направленная на разработку компьютерных систем, способных выполнять задачи, которые обычно требуют человеческого интеллекта, такие как визуальное восприятие, распознавание речи, перевод между языками, принятие решений и решение проблем. Большая часть привлекательности ИИ заключается в его способности анализировать огромные объемы данных – также называемых «большими данными» – быстрее и с большей легкостью, чем это может сделать человек-аналитик или даже команда аналитиков, и при этом обнаруживать закономерности и корреляции, невидимые человеческому глазу. Более того, ИИ

может экстраполировать вероятные результаты данного сценария на основе имеющихся данных.

Долгое время считавшийся не более чем научной фантастикой, ИИ уже используется в государственном и частном секторах для целого ряда полезных целей. Например, ИИ сыграл определенную роль в содействии значительному ускорению разработки вакцин на основе рибонуклеиновой кислоты-мессенджера (мРНК), таких как вакцины, которые в настоящее время используются для сдерживания пандемии COVID-19 и используются для содействия заключению мирных соглашений в раздираемой войной Ливии и Йемене. Генеральный секретарь Организации Объединенных Наций Антониу Гутерриш указал, что при надлежащем использовании и закреплении ценностей и обязательств, определенных Уставом Организации Объединенных Наций и Всеобщей декларацией прав человека, ИИ может сыграть определенную роль в выполнении Повестки дня в области устойчивого развития на период до 2030 года, способствуя искоренению нищеты, защите планеты и обеспечению мира и процветания для всех.

ИИ может стать мощным инструментом в борьбе с терроризмом, позволяя правоохранительным органам и контртеррористическим учреждениям реализовать потенциал, изменяющий правила игры, повышая эффективность, расширяя существующие возможности и позволяя им справляться с огромным увеличением объема данных. ИИ может оказывать поддержку правоохранительным и контртеррористическим учреждениям, например, путем автоматического выполнения повторяющихся задач для уменьшения рабочей нагрузки; оказания помощи аналитикам в прогнозировании будущих террористических сценариев для четко определенных, узких условий; выявления подозрительных финансовых операций, которые могут свидетельствовать о финансировании терроризма; а также мониторинг интернет-пространств на предмет террористической деятельности в масштабах и скорости, превышающих традиционно доступные человеческие возможности.

Однако волнение по поводу потенциала социального прогресса с помощью ИИ сдерживается растущей обеспокоенностью по поводу возможных неблагоприятных последствий и непреднамеренных последствий, которые могут возникнуть в результате внедрения этой технологии. В результате ИИ в настоящее время является предметом широких дискуссий среди технологов, специалистов по этике и политиков по всему миру. В условиях, когда борьба с терроризмом – и особенно упреждающие формы борьбы с терроризмом – уже находится на переднем крае дискуссий о защите прав человека, разработка и внедрение ИИ вызывает в этих контекстах острые проблемы в области прав человека.

Тем не менее, с точки зрения безопасности, необходимость в том, чтобы правоохранительные органы и контртеррористические учреждения адаптировались к цифровой трансформации, безусловно, существует. Можно даже сказать, что это особенно актуально для Южной и Юго-Восточной Азии, учитывая возросшие темпы цифровизации и растущее присутствие молодых, потенциально уязвимых элементов местного населения в Интернете, а также установившееся присутствие террористов и насильственных экстремистов в регионах. Однако уместно отметить, что имеется ограниченная общедоступная информация о степени технической готовности правоохранительных и контртеррористических учреждений в Южной и Юго-Восточной Азии или о любых конкретных возможностях, которые могут быть доступны или разрабатываются. Учитывая относительно зарождающееся состояние использования ИИ в целях борьбы с терроризмом, это, вероятно, свидетельствует об ограниченных знаниях или опыте использования этой технологии в этих регионах.

Недавнее исследование, проведенное ЮНИКРИ и Интерполом на Третьем ежегодном Глобальном совещании по ИИ для правоохранительных органов, подтвердило общее зачаточное состояние использования ИИ в правоохранительных органах в целом. Из 50 представителей правоохранительных органов по всему миру 50% считали, что уровень знаний

и опыта в области ИИ в их организации был «зачаточным», 30% считали его «промежуточным» и только 20% считали его «продвинутым».

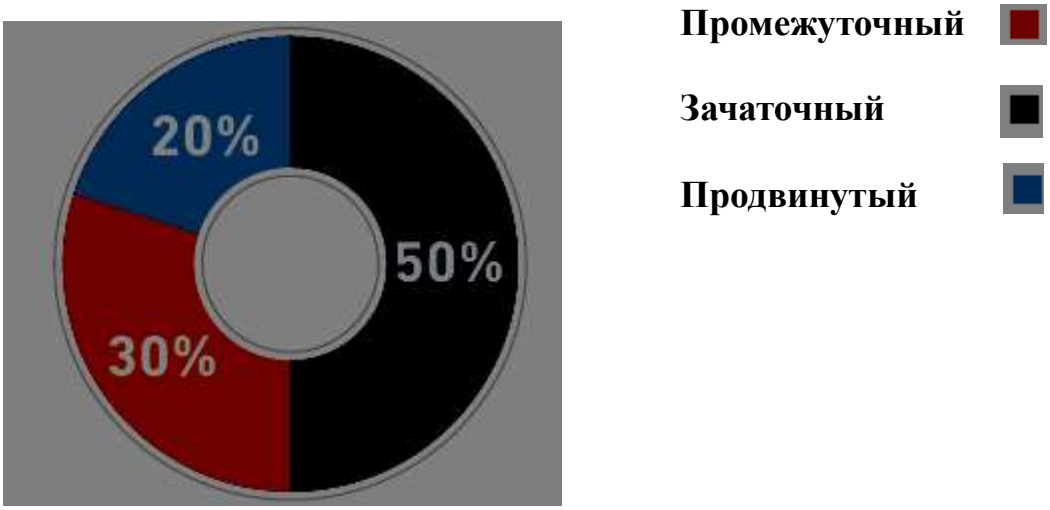

Рисунок 1: Опрос ИНТЕРПОЛА-ЮНИКРИ по самооценке уровня знаний и опыта ИИ в правоохранительных органах

На этом фоне настоящий доклад призван послужить введением для правоохранительных органов и контртеррористических учреждений в Южной и Юго-Восточной Азии по применению ИИ в контексте борьбы с терроризмом в Интернете. В отчете дается широкая оценка различных вариантов использования, демонстрируются возможности, предоставляемые этой технологией, а также устраняются проблемы. Отчет призван служить отображением ИИ, контекстуализируя возможные варианты использования технологии, которые теоретически могут быть развернуты в регионах, в то же время сопоставляя это с ключевыми проблемами, которые власти должны преодолеть, чтобы обеспечить ответственное использование ИИ и соблюдение прав человека. Хотя доклад специально предназначен для правоохранительных и контртеррористических учреждений в Южной и Юго-Восточной Азии, его охват и структура также делают его полезным ресурсом для правоохранительных и контртеррористических учреждений во всем мире.

При подготовке настоящего доклада Контртеррористический центр Организации Объединенных Наций (ККООН) Управления Организации Объединенных Наций по борьбе с терроризмом (ЮНОКТ) и Межрегиональный научно-исследовательский институт Организации Объединенных Наций по вопросам преступности и правосудия (ЮНИКРИ) опирались в основном на кабинетные исследования и информацию из открытых источников, такую как статьи, отчеты (включая сообщения СМИ), и провели частично закрытые интервью с межсекторальными экспертами из научно-исследовательских институтов, международные организации по безопасности и неправительственные организации. Совещание группы экспертов по использованию ИИ для борьбы с использованием Интернета и социальных сетей террористами, с акцентом на Южную и Юго-Восточную Азию, было фактически организовано ЮНОКТ и ЮНИКРИ 18 марта 2021 года, чтобы дополнить выводы, сделанные на основе анализа информации из открытых источников и проведенных интервью, и собрать конкретную информацию, в частности из целевых регионов. Учитывая деликатный характер вопросов безопасности, несколько собеседников анонимно делились информацией, и поэтому ссылки не всегда возможны.

Важно также подчеркнуть, что ссылка на какой-либо конкретный инструмент или приложение в этом докладе не должна рассматриваться как одобрение со стороны КТЦООН/ЮНОКТ, UNICRI или самой Организации Объединенных Наций. Инструменты и приложения, упомянутые в этом отчете, включены исключительно для демонстрации потенциального применения ИИ. ООН и ЮНИКРИ признают проблемы, связанные с разработкой и внедрением любых таких технологий с поддержкой ИИ, которые обязательно включают в себя те, которые упомянуты в этом докладе.

II. КЛЮЧЕВЫЕ КОНЦЕПЦИИ, ТЕХНОЛОГИИ И ПРОЦЕССЫ

Для того чтобы правоохранительные и контртеррористические органы могли более точно оценить, как ИИ может быть использован для борьбы

с терроризмом в Интернете, важно начать с установления основополагающего понимания самой технологии. В этой главе дается краткий технический обзор ключевых концепций, технологий и процессов.

1. Искусственный интеллект

Быстро развивающаяся область, ИИ все больше затрагивает многие сферы нашей жизни. ИИ уже широко используется для предложения фильмов и телевизионных шоу на потоковых платформах и для предоставления рекомендаций по онлайн-покупкам. Он курирует и заполняет новостные ленты в социальных сетях и разблокирует мобильные телефоны с помощью распознавания лиц. Несмотря на уровень интеграции ИИ в общество и частоту популярного использования этого термина, универсального определения «ИИ» не существует. Однако этот термин обычно понимается как описание дисциплины, связанной с разработкой технологических инструментов, реализующих человеческие качества, такие как планирование, обучение, рассуждение и анализ. В публичных дебатах этот термин часто используется взаимозаменяемо с «машинным обучением» и «глубоким обучением», что неточно с технической точки зрения. В то время как ИИ описывает общую область, машинное обучение и глубокое обучение являются подполями, описывающими конкретные типы ИИ. Таким образом, система ИИ может, например, включать датчики, которые фиксируют окружающую среду, плюс алгоритм машинного обучения для выполнения определенной задачи в соответствии с полученными данными. Оба этих отдельных подполя более подробно описаны ниже.

ИИ также можно классифицировать как «узкий» или «общий». Системы ИИ, существующие сегодня в нашем мире, состоят из так называемых узких приложений ИИ, то есть моделей ИИ, которые запрограммированы на достижение одной конкретной цели, такой как поиск наилучшего пути между А и В или сопоставление похожих изображений. Эти программы не могут быть применены за пределами их варианта использования

или при небольших изменениях в среде. Например, если бы на шахматной доске было 9 линий вместо 8, модель ИИ сразу же не смогла бы играть. Другими словами, алгоритмы ИИ – мастера улавливать закономерности, но они пока не могут понять и приспособиться к меняющемуся миру. Общий ИИ или искусственный общий интеллект могли бы это сделать, но пока это существует только в научной фантастике. Искусственный общий интеллект не будет обучаться для определенной цели, но его интеллект скорее будет более похож на человеческий, в том числе в анализе, планировании, общении и рассуждениях. Концепция искусственного суперинтеллекта идет еще дальше, поскольку она относится к ИИ, который превзошел бы человеческий интеллект во всех аспектах. От творчества до решения проблем сверхинтеллектуальные машины преодолеют наш интеллект как отдельных людей, так и общества в целом. Это тот тип ИИ, который вызвал довольно много философских споров, и некоторые эксперты утверждают, что он может даже представлять экзистенциальную угрозу для человечества.

ИИ часто воспринимается как современная разработка или что-то очень футуристическое, однако сама концепция ИИ на самом деле довольно старая, уходящая своими корнями в 1950-е годы. Из-за ограниченных в то время мощностей по хранению и обработке большая часть ранних надежд, связанных с ИИ, так и не материализовалась, что привело к тому, что стало известно как «Зима ИИ» – период, когда интерес общественности и инвестиции в ИИ значительно снизились. Новые технологические разработки, особенно в последнее десятилетие, позволили создать более дешевые решения для массового хранения данных и более быстрой обработки. В сочетании с «демократизацией» технологии, в результате которой ИИ становится все более доступным и может использоваться без больших инвестиций или даже при ограниченном увеличении технических знаний экспертов, а также расширении доступа к огромным объемам данных, необходимые ингредиенты для начала новой эры ИИ наконец-то на столе.

Как концепция, ИИ может вводить в заблуждение, поскольку подразумевает некоторое сходство с человеческим интеллектом или процессами обучения человека. Глубокие нейронные сети, семейство алгоритмов ИИ, на самом деле вдохновлены архитектурой человеческого мозга, с построением различных уровней процессоров, используемых для получения интересных результатов, даже с неструктурированными или немаркированными данными. Однако возможности ИИ, включая глубокие нейронные сети, смоделированные на основе человеческого мозга, сильно отличаются от человеческих возможностей. Например, даже если ИИ может делать прогнозы, он не может придать значения результатам. Например, приложение на основе ИИ для выявления рака молочной железы может очень надежно выявлять заболевание. Благодаря анализу снимков маммографии он выдает результаты с более низкой частотой ошибок, чем у рентгенологов. Однако программное обеспечение не способно понять значение такого диагноза, поскольку оно может видеть только числа интенсивностей пикселей за этим изображением. AI Alpha Go от Google может аналогичным образом вычислять лучшие ходы в сложной игре Go, но он не может объяснить, почему он выбрал определенные ходы и, следовательно, придать им смысл.

Также важно отметить, что модели ИИ могут находить закономерности и корреляции, которые не обязательно имеют причинно-следственную связь, но могут привести к желаемому результату. Например, ИИ, обученный распознавать поезда на изображениях, может, например, идентифицировать не поезда, а скорее железнодорожные пути, которые также часто появляются на изображениях, используемых для разработки модели. Подобные результаты основаны на непреднамеренных нейронных связях.

В то время как способность ИИ обнаруживать закономерности и корреляции может быть информативной и представлять непредвиденные связи, идентификация «железнодорожных путей» вместо «поездов» может быть опасной в контексте контртеррористических операций. Фактически, эта неспособность ИИ по-настоящему «понимать» и извлекать только

закономерности имеет решающее значение, когда речь заходит о приложениях ИИ в сфере борьбы с терроризмом. В то время как ошибка в алгоритме, разработанном для рекомендации фильмов для просмотра на основе профиля личной истории и предпочтений пользователей с аналогичными шаблонами, может просто привести к плохому просмотру фильма, ошибки в моделях ИИ в контртеррористических операциях могут иметь гораздо более тяжелые последствия и последствия для прав человека.

2. Данные

ИИ данных позволяет машинам учиться на собственном опыте. Модель машинного обучения может быть обучена путем обработки больших объемов данных и распознавания шаблонов в данных, шаблонов, которые используются для прогнозирования новых точек данных. Для получения точных прогнозов необходимы два основных компонента: модель и данные.

Данные можно понимать как единицы информации, собранной путем наблюдения. Для целей ИИ данные представляют собой набор значений переменных о людях или объектах, среди прочего, которые могут быть качественными (например, цвет глаз) или количественными (например, возраст). Набор данных, или база данных, представляет собой набор из нескольких единиц данных, которые измеряются и сообщаются, создавая визуализации данных, такие как графики, таблицы или изображения.

Для того чтобы иметь хорошую модель ИИ, крайне важно обеспечить как количество, так и качество данных. Вообще говоря, простые модели с большими наборами данных являются более точными и эффективными, чем сложные модели с небольшими наборами данных. С другой стороны, также бесполезно иметь много данных, если они неточны, нерепрезентативны или устарели. В этом смысле качество результата в значительной степени зависит от качества обучающих данных. Это включает в себя наличие данных, свободных от предвзятости, поскольку эта предвзятость может быть отражена в результатах.

После построения набора данных их необходимо преобразовать таким образом, чтобы модель могла их считывать. Данные могут быть «структурированными», когда они хранятся в предопределенном формате, таком как электронная таблица, или «неструктурированными», когда они состоят из множества различных типов данных, которые хранятся в их собственных форматах, таких как электронная почта или сообщение в социальных сетях. Подавляющее большинство всех полученных данных приходится на неструктурированные данные. Преобразование и очистка данных для использования в качестве входных данных для модели является наиболее трудоемким, но также и наиболее важным шагом с точки зрения обеспечения высокой производительности модели ИИ. Учитывая его природу, неструктурированные данные требуют больше работы для обработки, хотя они также могут иметь большую ценность, помогая организациям с нужными возможностями извлекать ценные идеи и возможности.

Одна из ключевых проблем, возникающих при использовании ИИ в области борьбы с терроризмом, заключается в том, что огромное количество необходимых данных не всегда доступно. Реальность терроризма такова, что инциденты не являются регулярными событиями, и случаи радикализации часто уникальны. Существует несколько баз данных с открытым исходным кодом по терроризму, которые могут быть использованы для целей алгоритмов обучения, таких как Глобальная база данных по терроризму, в которой собрана историческая информация о более чем 200 000 террористических инцидентах во всем мире с 1970 года. В то время как это очень ценные источники данных, в частности, с точки зрения прогнозирования возможных будущих типов террористических атак, целевых областей и используемых средств, для реализации приложений, описанных в настоящем докладе, потребуются более конкретные и близкие к реальному времени наборы данных, касающиеся действий отдельных террористов или подозреваемых террористов, такие как данные социальных сетей. Естественно, поскольку большая часть этих данных неструктурирована по своей природе, потребуется большая работа

с точки зрения подготовки их использования. Одним из возможных решений для преодоления отсутствия достаточного количества данных «реального мира» является использование «дополненных данных», т.е. искусственных данных, создаваемых общими сетями состязательности (GAN) для целей алгоритмов обучения. Однако необходимы дальнейшие исследования для изучения потенциала расширенных данных в области борьбы с терроризмом.

3. Машинное обучение

Машинное обучение – это подполе ИИ, которое касается алгоритмов, которые могут «учиться» на данных, т.е. постепенно повышать производительность при выполнении конкретной задачи. В отличие от других компьютерных программ, алгоритмы машинного обучения не требуют явных инструкций от людей, а извлекают шаблоны и изучают неявные правила из примеров, включенных в базу данных. Исходная база данных разделена на три группы, так что алгоритм может быть обучен с некоторыми примерами данных из обучающего набора данных, проверен на наборе данных проверки и впоследствии протестирован на никогда ранее не встречавшихся примерах из тестового набора данных.

Типы встречающихся примеров обучения включают «регрессию», при которой вывод представляет собой действительное число; «классификацию», при которой вывод представляет собой метку из конечного набора вариантов; и «ранжирование», при котором вывод упорядочивает объекты в соответствии с их релевантностью, маркировкой последовательности, автономным поведением и т.д. В зависимости от типа обучающего примера можно использовать несколько моделей, включая деревья решений, линейную и логистическую регрессию, нейронные сети и другие.

4. Глубокое обучение

Глубокое обучение – это область машинного обучения, которая имеет дело с меньшим семейством алгоритмов, известных как глубокие нейронные

сети. Это алгоритмы, которые вдохновлены человеческим мозгом и которые стремятся учиться на больших объемах данных, выполняя задачу повторно, каждый раз внося незначительные изменения в ее внутренние функции, чтобы улучшить результат. Термин «глубокое обучение» происходит от нескольких (или «глубоких») слоев нейронной сети. Достижения в области глубокого обучения являются движущей силой прогресса и исследований в области обработки изображений и видео, анализа текста и распознавания речи.

5. Порождающая состязательная сеть (GAN)

GAN состоят из двух нейронных сетей, которые конкурируют друг с другом, тем самым улучшая свои соответствующие характеристики. Например, одна нейронная сеть используется для создания поддельных лиц, а другой поручено отфильтровывать их из набора реальных. По мере совершенствования системы фильтрации улучшается и система подделки лиц. Веб-сайты, такие как https://thispersondoesnotexist.com/, которые генерируют новое вымышленное лицо при каждом обновлении, являются хорошо известными примерами использования GAN.

Помимо создания реалистичных фальшивых лиц, GAN также являются основой широко разрекламированного и горячо обсуждаемого феномена, известного как «глубокие подделки». Портфолио «глубокого обучения» и «поддельных медиа», deepfakes – это разновидность синтетических медиа, изобретенных в 2017 году. Они предполагают использование GAN для манипулирования или создания поддельного визуального и аудиоконтента, который люди или даже технологические решения не могут сразу отличить от подлинного контента. Изначально глубокие подделки использовались и до сих пор в подавляющем большинстве используются для создания порнографического контента, сочетающего лица знаменитостей женского пола с телами порнографических актеров. Однако глубокие подделки и технологии, стоящие за ними, также были определены как потенциально мощное оружие в современных войнах за дезинформацию, где люди больше не могут

полагаться на то, что они видят или слышат. Это особенно актуально при рассмотрении охвата и скорости Интернета, социальных сетей и приложений для обмена сообщениями.

Глубокие подделки представляют значительный потенциал для целого ряда вредоносных и преступных целей, которые включают в себя: уничтожение репутации и доверия к личности; преследование или унижение людей в Интернете, в том числе с помощью сексуальных подделок; совершение шантажа, вымогательства и мошенничества; нарушение финансовых рынков; разжигание социальных волнений и политической поляризации. С точки зрения терроризма, фейки представляют угрозу с точки зрения их использования в кампаниях по дезинформации в социальных сетях для манипулирования общественным мнением или подрыва доверия людей к потенциальным и действующим политическим представителям или государственным институтам. Они также могут быть эффективным инструментом пропаганды, радикализации или в качестве призыва к действию.

Интересно, что ИИ также может быть частью решения этой растущей социальной проблемы, основанной на ИИ. Например, разработчики, в том числе Facebook, Microsoft и многие другие, разработали модели ИИ, которые были обучены распознавать аудиовизуальный контент, управляемый ИИ. Однако существует мало зрелых общедоступных инструментов.

6. Обработка естественного языка

Обработка естественного языка (NLP) – это приложение для глубокого обучения, которое касается обработки и анализа больших объемов данных на естественном человеческом языке, чтобы машины могли читать, понимать и извлекать смысл из человеческих языков. Задачи в NLP часто включают распознавание речи, понимание естественного языка, генерацию естественного языка и перевод между языками. За последнее десятилетие в NLP были достигнуты значительные успехи, особенно в сочетании с ранее описанными GAN, как недавно продемонстрировала статья, написанная в соавторстве

с генератором текста GPT-3 в британской ежедневной газете The Guardian. Тип архитектуры, наиболее часто используемой в NLP, известен как Рекуррентная нейронная сеть, в которой узлы нейронной сети соединены во временной последовательности. Опираясь на внутреннюю память, которая обрабатывает последовательности входных данных, алгоритм может извлекать морфосинтаксическую и семантическую функции на основе последовательности слов.

7. Распознавание объектов

Распознавание объектов – это подкатегория компьютерного зрения, которая использует алгоритмы глубокого обучения для обработки изображений и идентификации геометрических фигур и, в конечном счете, объектов. Сложные алгоритмы, основанные на так называемых сверточных нейронных сетях, используют несколько слоев локально соединенных узлов для постепенного извлечения объектов более высокого уровня из необработанных входных данных. Если входным сигналом является изображение, то первые слои нейронной сети могут, например, идентифицировать линии и кривые, в то время как последние слои могут идентифицировать буквы или лица. Важной разновидностью распознавания объектов является распознавание лиц – биометрическая технология, способная идентифицировать интересующих лиц на изображениях или видео путем сравнения и анализа изображений, форм и пропорций их черт лица и контуров с лицами в базе данных.

8. Прогнозная аналитика

Прогнозная аналитика стремится предвидеть вероятные будущие или неизвестные события, анализируя то, что уже произошло, и, исходя из этого, экстраполируя вероятные результаты в соответствующих контекстах. Он включает в себя различные статистические методы, такие как интеллектуальный анализ данных и машинное обучение, которые анализируют

текущие и исторические факты в качестве основы для своих прогнозов. Прогностические модели фиксируют взаимосвязи между рядом переменных, чтобы позволить оценить риск, связанный с определенным набором условий. Инструменты, основанные на машинном обучении, могут представлять результаты с помощью простых диаграмм, графиков и оценок, которые указывают на вероятность событий в будущем, определяя процессы принятия решений.

9. Анализ социальных сетей

Анализ социальных сетей – это комплексный подход к пониманию и моделированию сетевых структур и поведения участников в них. Социальные сети могут быть физическими – как в сети передачи заболеваний – или цифровыми, как в сети дружбы в социальных сетях. Фундаментальным шагом для анализа социальных сетей является кодирование сетевых данных в низкоразмерные представления, обычно с использованием набора узлов для представления отдельных элементов сети и набора связей или ребер между этими узлами, которые соответствуют попарным отношениям. Интеллектуальный анализ данных и машинное обучение могут быть использованы для разработки методов сетевого представления, позволяющих составлять карты сообществ, выявлять основных участников или группы внутри сообщества и других приложений, таких как классификация, увязка прогнозов, обнаружение аномалий и кластеризация.

10. Технология сопоставления контента

В изображении и сопоставлении видео используется технология «хеширования» для сокращения ввода любой длины в фиксированную строку текста – так называемый хэш, который похож на цифровой отпечаток пальца. Затем короткую версию входных данных можно сравнить с другими файлами, чтобы найти дубликаты и предотвратить их совместное использование. Эта технология может быть использована для выявления идентичного

вредоносного контента, такого как экстремистский, террористический или порнографический контент, в режиме реального времени в больших масштабах. В то время как ИИ позволяет идентифицировать неизвестный или вредоносный контент «первого поколения», технология хэширования позволяет обнаруживать уже идентифицированный контент, так что, когда один и тот же материал передается несколько раз через несколько платформ, его можно обрабатывать и удалять быстрее. В этом смысле эта технология дополняет функциональные возможности ИИ в этой области и может быть объединена для обеспечения более эффективной модерации контента. PhotoDNA является примером этой технологии, которая изначально была разработана для выявления материалов о сексуальном насилии над детьми и в настоящее время более широко используется в отношении другого незаконного контента. В декабре 2016 года Facebook, Twitter, Google и Microsoft объявили о планах борьбы с экстремистским контентом, таким как видеоролики о вербовке террористов и изображения жестоких террористов с использованием PhotoDNA.

11. Анонимизация и псевдонимизация данных

Учитывая, что приложения ИИ, представленные в этом отчете, предполагают обработку персональных данных, такие методы, как анонимизация и псевдонимизация, являются ключевыми для защиты права на частную жизнь. Несмотря на то, что у них есть некоторые общие черты, анонимизация и псевдонимизация – это разные понятия. Анонимизация данных состоит в преобразовании персональных данных в анонимные данные, так что отдельные лица или группы лиц, которым принадлежат данные, больше не могут быть идентифицированы в данных. Анонимизация может быть достигнута различными методами, в том числе с помощью псевдонимизации. Псевдонимизация состоит в удалении или замене всех прямых идентификаторов другими уникальными идентификаторами таким образом, чтобы уникальные люди все еще были различимы в наборе данных,

но их личность невозможно отследить без доступа к дополнительной информации. Следует отметить, что анонимизированные данные по прежнему являются личными данными до тех пор, пока анонимизация не станет необратимой, поскольку при наличии соответствующих навыков или технологий данные могут быть связаны с отдельными лицами или группами.

12. Разведка с открытым исходным кодом и разведка в социальных сетях

Разведка с открытым исходным кодом (OSINT) – это метод сбора, анализа и интерпретации общедоступных данных. Источники OSINT могут варьироваться от СМИ (печатные газеты, телевидение и т.д.), Интернета (онлайн-публикации, блоги и другие сайты социальных сетей), государственных данных, профессиональных и академических публикаций, коммерческих данных или того, что иногда называют «серой литературой» (технические отчеты, патенты, информационные бюллетени и т.д.). Инструменты OSINT помогают ориентироваться, анализировать и визуализировать материал, варьируясь от поиска определенных ключевых слов до взаимодействия учетных записей.

Social media intelligence (SOCMINT) – это подкатегория OSINT, которая фокусируется на сборе разведданных в социальных сетях. В этом случае инструменты SOCMINT позволяют организациям анализировать разговоры, реагировать на социальные сигналы и синтезировать точки социальных данных в значимые тенденции и анализ.

13. Неверная информация и дезинформация

Рост феномена «фальшивых новостей» сделал неверную информацию и дезинформацию бытовыми терминами. Разница между неверной информацией и дезинформацией заключается в осознании ее неточности. Дезинформация – это ложная информация, которая распространяется

намеренно, чтобы причинить вред. А вот неверная информация, распространяется непреднамеренно. Еще один связанный с этим термин – ложная информация, которая представляет собой информацию, основанную на реальности, но стратегически используемую для причинения вреда. Примечательно, что эти явления значительно усилились во время пандемии COVID-19. Хотя ни один из этих терминов не имеет прямого отношения к области ИИ, поскольку ИИ может значительно усугубить последствия дезинформации и неверной информации или играть центральную роль в борьбе с ними.

III. ИССЛЕДОВАНИЕ ПОТЕНЦИАЛА ИИ

Приняв к сведению угрозу терроризма в Южной и Юго-Восточной Азии, рассмотрев ключевые тенденции и события, связанные с «цифровизацией» в этих регионах, и рассмотрев, что это означает с точки зрения проблем, с которыми правоохранительным органам и контртеррористическим учреждениям приходится все чаще сталкиваться, в этой главе делается попытка представить, как могут быть применены некоторые технологии ИИ, описанные в предыдущей главе.

В этой связи была определена серия из шести вариантов использования технологий с поддержкой ИИ в борьбе с терроризмом, каждый из которых будет представлен ниже в вводном формате для поддержки концептуализации применения ИИ в области противодействия терроризму в режиме онлайн. Эти варианты использования были выбраны из-за их значимости в дискуссиях среди заинтересованных сторон в сообществе ИИ в целом, а также из-за их особого потенциала для применения в борьбе с терроризмом в Интернете. Однако это не следует считать исчерпывающим резюме применения ИИ в целях борьбы с терроризмом.

Примеры конкретных инструментов, представленных в этой главе, в основном взяты из Европы и Соединенных Штатов, поскольку именно в этих регионах сосредоточена большая часть исследований и разработок

в области ИИ и борьбы с терроризмом. Прежде чем продолжить, важно еще раз подчеркнуть, что ссылка на какой-либо конкретный инструмент или приложение в этом докладе не должна рассматриваться как одобрение со стороны КТЦООН-ЮНОКТ, ЮНИКРИ или самой Организации Объединенных Наций. Инструменты и приложения, упомянутые в этом отчете, включены исключительно для демонстрации потенциального применения ИИ.

1. Прогнозная аналитика террористической деятельности

Применение прогнозной аналитики для борьбы с терроризмом можно в некотором смысле охарактеризовать как «Святой Грааль» для сил безопасности, позволяющий им преодолеть традиционно реакционный подход к терроризму и стать более активными, предвидя будущие террористические действия и вмешиваясь до того, как произойдет нападение. Для этого в модель ИИ необходимо будет вводить большое количество данных в режиме реального времени о поведении террориста или подозреваемого лица. Анализируя эти данные, такая модель потенциально могла бы, например, делать прогнозы относительно вероятной будущей деятельности этих людей. Учитывая значительный рост за последнее десятилетие объема данных о поведении людей в Интернете, особенно в социальных сетях, растет интерес к изучению того, как данные социальных сетей, собранные о поведении людей в Интернете, могут быть использованы для прогнозирования террористической деятельности.

Учитывая непредсказуемость человеческого поведения и текущее состояние технологического развития, применение алгоритмов для прогнозирования поведения на индивидуальном уровне, вероятно, будет иметь весьма ограниченную ценность. Кроме того, эксперты по правам человека и организации гражданского общества указали на ряд этических проблем, касающихся потенциальных точек входа для дискриминационных суждений и обращения. Большое количество данных об отдельном человеке,

необходимых для дальнейшего точного функционирования алгоритма, вызывает опасения по поводу возможности необоснованного массового наблюдения.

Однако прогнозная аналитика все еще может способствовать борьбе с терроризмом, но по-другому. Вместо мониторинга отдельных лиц в Интернете и прогнозирования их поведения для выявления тенденций или прогнозирования будущего поведения террористов можно было бы использовать прогностические модели, основанные на статистических данных из онлайновых источников, которые были полностью анонимизированы или, по крайней мере, псевдонимизированы для защиты конфиденциальности пользователей. Этот анализ, основанный на агрегированных данных, может быть полезен для поддержки служб безопасности и разведки, определяющих приоритетность ограниченных ресурсов в качестве оперативной поддержки, принятия стратегических решений или предоставления предупреждений компетентным органам. Приведенные ниже примеры иллюстрируют, как прогностическая аналитика позволяет получить глубокое представление о сетевой структуре террористических групп, прогнозировать фрагментацию и разрабатывать политику, направленную на сокращение числа нападений.

INSIKT Intelligence, технический стартап, активно работающий в этой области, использует различные модели машинного обучения для обнаружения потенциальных угроз в Интернете с помощью методов NLP и SNA, выполняемых на контенте с открытым исходным кодом, полученном из социальных сетей и других источников. Выводы, полученные в результате анализа текста и сети, затем используются для выявления потенциально опасного контента и возможных угроз или определения моделей взаимоотношений между отдельными лицами или организациями. Используя SNA, INSIKT оценивает активность группы пользователей в сети, определяя узлы влияния и уровни/эффективность распространения информации, например, от пропаганды через эти сети. Этот анализ с открытым исходным кодом позволяет правоохранительным органам использовать большие данные и определять приоритеты ограниченных ресурсов в отношении потенциальных

угроз. Анонимизация или псевдонимизация данных также способствует соблюдению принципов защиты данных, таких как принципы, включенные в Рамки АСЕАН по защите персональных данных или Рамки конфиденциальности Азиатско-Тихоокеанского экономического сотрудничества.

Автоматизированное моделирование террористических сетей с использованием систематически собираемых данных об организации может способствовать усилиям по борьбе с терроризмом путем определения приоритетов и наиболее эффективных стратегий «влияния» на поведение террористов. Например, исследователи применили ИИ, включая алгоритмы анализа социальных сетей, для прогнозирования фрагментации террористических групп, чтобы получить более глубокое представление о том, как и когда террористические группы, такие как ИГИЛ и «Аль-Каида», раскололись.

В одном интересном исследовании в 2013 году модели поведенческого прогноза были применены для проведения всеобъемлющей и всесторонней оценки Лашкар-и-Тайбы – группы, связанной с «Аль-Каидой», которая была ответственна за многочисленные нападения в Пакистане, Индии и Афганистане и достигла глобальной известности в результате нападений в Мумбаи в 2008 году. Основываясь на данных, касающихся идеологии, истории и других соответствующих фактов, исследователи применили «временные вероятностные» правила, чтобы определить, какие действия потребуются, чтобы сорвать кампанию Лашкар-и-Тайбы и снизить смертность группы. В основу исследования легли поведенческие модели, так называемый алгоритм обучения правилам агентов стохастического моделирования противников (SOMA). В результате исследования были выработаны политические рекомендации, которые можно было бы использовать для создания среды вокруг Лашкар-и-Тайбы, способствующей сокращению числа нападений.

Другая исследовательская инициатива, представляющая интерес, касается модели прогнозной аналитики машинного обучения, связывающей сетевую

структуру с летальностью. Алгоритм, известный как «Формирование эффективности террористической онлайн-сети» или «КАМЕНЬ», дает прогнозы о том, кто, скорее всего, преуспеет в определенной должности в данной террористической сети, если субъект будет насильственно удален с помощью вмешательства сил безопасности; как будет перестраиваться сеть, когда удаляются несколько участников; как управлять сетью, чтобы свести к минимуму «ожидаемую летальность» сети. Прогнозирование сетевых реакций на различные вмешательства полезно для служб разведки и безопасности, чтобы определить, как наиболее эффективно использовать ограниченные ресурсы, направляя их в особо перспективную область.

Эти примеры показывают, как прогностическая аналитика может функционировать в случаях, когда имеется достаточно данных для информирования о контртеррористических операциях. Онлайновые данные, в частности данные социальных сетей, теоретически могут изменить правила игры для прогнозной аналитики, предлагая совершенно новое измерение общедоступных или открытых данных о террористических организациях, их членах, а также действиях других субъектов, которые могут повлиять на их поведение. Тем не менее, как отмечалось, существуют реальные проблемы в отношении использования данных социальных сетей для прогнозирования будущего индивидуального поведения террористов, которые, вероятно, будут препятствовать применению прогностической аналитики в этом отношении. Правоохранительные органы и контртеррористические учреждения, стремящиеся изучить возможность использования прогностической аналитики таким образом, должны помнить, что полученные результаты отражают вероятности, и обязательно, не являются доказательствами для принятия мер. Несмотря на это, хотя использование прогностической аналитики для прогнозирования террористической деятельности может быть технически и этически сложным, а также практически сложным для принятия мер, прогностическая аналитика может найти применение правоохранительным органам и контртеррористическим

учреждениям для привлечения внимания следователя к конкретным закономерностям или, в зависимости от обстоятельств, отклонениям в закономерностях, которые могут возникнуть и заслуживают дальнейшего рассмотрения.

2. Выявление красных флагов радикализации

Еще один пример использования ИИ для борьбы с терроризмом в Интернете касается использования технологии на базе ИИ для выявления лиц, подверженных риску радикализации в онлайн-сообществах, для содействия надлежащему расследованию и вмешательству, что, как уже отмечалось, становится все более актуальным явлением в Интернете. Это также то, что невозможно обнаружить с помощью традиционных методов правоохранительных органов.

Хотя радикализация является сложным социальным явлением, а путь к радикализации очень личный и часто политический, методы машинного обучения, такие как NLP, могут оказать ценную поддержку правоохранительным органам и контртеррористическим учреждениям, а также, если на то пошло, соответствующим другим субъектам сообщества, таким как социальные работники. NLP можно использовать, например, для определения ключевых слов, которые могут указывать на степень радикализации учетной записи в социальных сетях или уязвимость человека к террористическим рассказам в Интернете. Также может быть полезно распознавать конкретные модели поведения отдельных лиц, такие как потребление или поиск террористического и насильственного экстремистского контента, который соответствует показателям радикальности.

Финансируемая Европейским Союзом (ЕС) Система раннего обнаружения и оповещения в режиме реального времени о террористическом контенте в Интернете (RED-Alert) является одним из примеров инструмента, направленного на выявление ранних стадий радикализации при одновременном обеспечении высоких стандартов конфиденциальности и безопасности.

RED-Alert использует NLP, SNA и сложную обработку событий для сбора, обработки, визуализации и хранения онлайн-данных, связанных с террористическими группами, включая ранние стадии радикализации на основе контента социальных сетей. Инструмент поддерживает поиск известных ключевых слов или тем в контенте, который еще не был идентифицирован как релевантный. Кроме того, инструмент включает процесс анонимизации и деанонимизации данных, который адаптируется к организационным процессам правоохранительных органов, что представляется перспективным также для других областей, связанных конфиденциальными данными. Проект RED-Alert завершился в конце 2020 года, и правоохранительные органы, участвующие в пилотировании платформы, указали, что она предлагает значительное улучшение по сравнению с инструментами, которые они используют в настоящее время. Несмотря на это, важно отметить, что платформа использовалась только на этапе тестирования, и поэтому ее работоспособность вне тестовых сред еще предстоит выяснить.

Moonshot, технологический стартап, базирующийся в Соединенном Королевстве и специализирующийся на противодействии насильственному экстремизму, является еще одним хорошим примером роли, которую ИИ может сыграть в выявлении людей, уязвимых к радикализации. Как и проект «Красная тревога», Moonshot направлен на выявление лиц, уязвимых к радикализации в Интернете, но вместо того, чтобы способствовать перехвату и расследованию правоохранительными органами и контртеррористическими агентствами, Moonshot стремится связать этих уязвимых лиц с «позитивными сообщениями». Это приложение более подробно рассматривается в разделе ниже, посвященном борьбе с террористическими рассказами.

ИИ также может помочь отслеживать глобальные сдвиги, которые могут указывать на благоприятную почву для радикализации в Интернете. Например, финансируемый правительством Германии исследовательский проект «Система мониторинга и платформа передачи радикализации» (MOTRA) в настоящее время работает над комплексным инструментом мониторинга для анализа

агрегированных данных для мониторинга важных социальных изменений. Цель состоит в том, чтобы выявить изменения в установках, которые потенциально могут служить ранним показателем преступной деятельности. Систематический мониторинг позволяет быстрее выявлять и классифицировать новые тенденции и служит основой для прогнозных заявлений, позволяющих разработать политику безопасности, основанную на фактических данных, репрессивную и превентивную. Однако разработка методологии и технологии все еще находится в стадии разработки, и, следовательно, имеется ограниченная информация. Первые результаты ожидаются от MOTRA в 2023 году.

Как показывают эти примеры, технология с поддержкой ИИ может быть полезной для поддержки аналитиков в выявлении потенциальных уязвимостей для радикализации в Интернете. Тем не менее, следует подчеркнуть, что автоматизированные оценки уязвимости к радикализации вызывают очень серьезные этические проблемы. Кроме того, следует также сказать, что технология далека от того, чтобы она могла заменить работу опытных специалистов по безопасности. Наконец, важно признать, что, даже если бы технология находилась в таком продвинутом состоянии, что ее можно было бы использовать уверенно и надежно, такие действия, как эта, в области профилактики не обязательно всегда дают основания для вмешательства правоохранительных органов.

3. Выявление ложной информации и дезинформации, распространяемой террористами в стратегических целях

Явление ложной информации и дезинформации не ново. Тем не менее, способность такого контента «поддельных новостей» охватывать широкую аудиторию при относительно низких затратах с помощью онлайн-средств беспрецедентна. Хотя фабрикация или искажение информации не обязательно являются незаконными, они, безусловно, могут быть вредными и потенциально могут способствовать распространению террористических или экстремистских нарративов в основной дискурс. Например, во время пандемии COVID-19 такие

террористы или воинствующие экстремисты создавали и распространяли вводящий в заблуждение контент в больших масштабах, используя уязвимости в экосистеме социальных сетей и манипулируя людьми с помощью рассказов о заговорах и фальшивых новостей, чтобы подорвать доверие к правительству и в то же время укрепить экстремистские рассказы негосударственных субъектов и стратегии вербовки.

Однако для того, чтобы ложная информация и дезинформация укоренились, ее необходимо сначала широко распространить в Интернете и установить контакт с уязвимыми пользователями. В то время как люди играют важную роль в распространении ложной информации и дезинформации, так называемые боты усугубляют масштабы проблемы. Сокращение от «робот», боты – это тип программного приложения, которое работает в режиме онлайн и выполняет повторяющиеся задачи. Чат-боты, разновидность ботов, могут, например, имитировать обычный разговор и по этой причине часто используются на веб-сайтах для облегчения и выполнения элементарных услуг для клиентов. Согласно одному исследованию в 2017 году, в Twitter было 23 миллиона ботов, 140 миллионов ботов на Facebook и около 27 миллионов ботов на Instagram. Такие группы, как ИГИЛ, доказали, что умеют использовать ботов в социальных сетях для автоматизации распространения своей пропаганды.

Хотя это вряд ли остановит поток ложной информации и дезинформации в целом, идентификация поддельных или бот-аккаунтов, созданных с намерением распространять поддельные новости или направлять дебаты в определенных направлениях, представляет собой возможную отправную точку для борьбы со значительным процентом ложной информации и дезинформации, распространяемой террористами. Специалисты, исследующие твиттер-ботов, предположили, что твиты, сделанные ботами, касаются очень узких тем, в то время как твиты людей, как правило, более разнообразны с точки зрения содержания. В связи с этим была выдвинута

гипотеза о том, что инструменты ИИ могут быть использованы для автоматической идентификации ботов.

Штаб-квартира правительственной связи (GCHQ), британская организация разведки и безопасности, недавно объявила, что будет использовать инструменты, поддерживаемые ИИ, для обнаружения и идентификации поддельных аккаунтов, распространяющих ложные новости. GCHQ также будет использовать технологию для автоматизации проверки фактов путем проверки достоверных источников, для обнаружения и блокирования ботнетов, а также для выявления групп интернет-троллей, известных как «фермы троллей», и других источников дезинформации.

Хотя инициатива NewsGuard не имеет прямого отношения к правоохранительным органам и контртеррористическим учреждениям, дальнейшее применение ИИ для противодействия дезинформации и дезинформации в Интернете продемонстрировано инициативой NewsGuard. Основанная в 2018 году, NewsGuard – это журналистская и технологическая компания, которая оценивает достоверность новостных и информационных веб-сайтов и отслеживает дезинформацию в Интернете. Анализ достоверности проводится журналистами и опытными редакторами. News Guard использовал записи из своего набора данных дезинформации и в сочетании с NLP и другими методами машинного обучения для обнаружения ложных новостей на разных платформах.

Аналогичным образом в Шри-Ланке исследователи выявляют и комментируют дезинформацию с помощью инструмента машинного обучения. В соответствии с предварительными результатами исследований, модель машинного обучения была обучена всего 1600 статьям, с точностью до 97% при классификации дезинформации по миллиону статей. Продолжение многоступенчатого исследования будет проводиться на английском, бенгальском и сингальском языках. Благодаря применению более простой модели машинного обучения, в отличие от нейронной сети, исследователи, о которых идет речь, стремятся получить отслеживаемые результаты без

существенного снижения точности. Хотя они и не предназначены для правоохранительных или контртеррористических целей, многообещающие результаты таких исследований могут со временем найти практическое применение в силах безопасности для противодействия использованию террористами ложной информации и дезинформации.

4. Автоматическая модерация и удаление контента

Социальные медиа-каналы и веб-страницы, на которых размещается мультимедийный контент, различными способами борются со злоупотреблением их услугами террористами. Во многом то, как они это делают, зависит от того, как террористы злоупотребляют своими платформами. Например, веб-сайт, который позволяет обмениваться большими файлами, может использовать иной подход, чем приложение для обмена сообщениями, которое позволяет осуществлять зашифрованную связь. Одной из хорошо известных реакций компаний социальных сетей на борьбу с террористическим и экстремистским контентом является «деплатформирование». Согласно определению Оксфордского словаря, деплатформирование – это «действие или практика, направленная на то, чтобы помешать кому-либо, придерживающемуся взглядов, которые считаются неприемлемыми или оскорбительными, участвовать в форуме или дебатах, особенно путем блокировки их на определенном веб-сайте». Это часто используется компаниями социальных сетей в качестве реакции на повторные нарушения условий предоставления услуг или стандартов сообщества их платформ. Другой часто используемый подход – это техника, известная как «запрет теней». Это относится к контенту, который либо полностью удален, либо его видимость значительно ограничена, без уведомления пользователя, опубликовавшего контент.

Такие инструменты и подходы, естественно, не лишены противоречий. В частности, возникла озабоченность в связи с возможностью субъективного, несопоставимого и потенциально предвзятого правоприменения со стороны

различных платформ в результате отсутствия согласованных на международном уровне определений того, что представляет собой терроризм и насильственный экстремизм. Кроме того, при ограниченной прозрачности в отношении инструментов и подходов, используемых компаниями социальных сетей, и отсутствии подробностей об их реализации также трудно реально оценить их эффективность. На самом деле, эффективность деплатформинга довольно обсуждаема, поскольку это может на самом деле увеличить количество жалоб и предоставить рассказы о виктимизации для запрещенных пользователей и сообществ. Это также может способствовать поощрению миграции таких людей с хорошо регулируемых крупных платформ со значительными ресурсами для модерации контента на менее регулируемые небольшие платформы и нишевые сервисы, возможности которых по решению таких проблем в Интернете могут быть более ограниченными. Возникающий в результате фрагментированный ландшафт может, по сути, поставить под угрозу коллективные усилия по борьбе с проблемой в целом.

Уместно отметить, что также не всегда просто пресечь террористическую деятельность, просто удалив учетную запись или ограничив видимость контента. Например, исполнители теракта в Крайстчерче в 2019 году транслировали атаку в прямом эфире – нововведение, которое создало новые проблемы для модераторов контента. Хотя Facebook успешно удалил оригинальное видео через 12 минут после окончания записи, видео стало вирусным, и в последующие 24 часа было предпринято до 1,5 миллиона попыток загрузить копии видео по всему миру. Крайстчерч недвусмысленно продемонстрировал необходимость не только удалять учетные записи и ограничивать видимость контента, но и иметь возможность работать на разных платформах, чтобы своевременно предотвращать стратегическое распространение террористического контента. После событий в Крайстчерче, Глобальный интернет-форум по борьбе с терроризмом (GIFCT) создал общую отраслевую базу данных хэшей террористической пропаганды с целью поддержки скоординированного удаления такого контента на разных

платформах при соблюдении политики конфиденциальности и хранения данных.

Автоматизированная модерация контента приобрела известность как прагматичный подход к работе с огромным количеством контента, создаваемого пользователями в Интернете, и скоростью, с которой определенный контент может стать вирусным. Частные компании используют различные формы автоматизированных решений для кураторства и модерации контента в Интернете, либо удаляя, либо понижая рейтинг контента, либо перенаправляя пользователей на другой контент. Например, Facebook полагается на машинное обучение, чтобы определить приоритетность того, какой контент необходимо просмотреть в первую очередь. Сообщений, нарушающих политику компании, помечаются либо пользователями, либо фильтрами машинного обучения, которые включают в себя все, от спама до разжигания ненависти и контента, «прославляющего насилие». С 2020 года компания решила разбираться с четкими случаями, автоматически удаляя сообщение или блокируя учетную запись. Только контент, который явно не нарушает политику компании, просматривается модератором человеческого контента. Для борьбы с терроризмом и насильственным экстремизмом Facebook использует различные инструменты, в том числе языковые модели ИИ, для понимания текста, который может пропагандировать терроризм, который часто зависит от языка и типа группы. Платформа сообщает, что человеческий опыт по-прежнему необходим для детального понимания того, как терроризм и насильственный экстремизм проявляются во всем мире. Другие популярные платформы, такие как Twitter и YouTube, также полагаются на ИИ для быстрого удаления комментариев, нарушающих правила компаний.

Модели ИИ, модерирующие контент, обучены отфильтровывать определенный контент, соответствующий определенным критериям. Однако в своей нынешней форме они страдают от присущих им ограничений. Например, модель машинного обучения, обученная находить контент одной террористической организации, может не работать для другой из-за языковых

и стилистических различий в их пропаганде. Как выразилась журналистка Массачусетского технологического института Карен Хао «алгоритм, который научился распознавать отрицание Холокоста, не может сразу определить, скажем, отрицание геноцида Рохинджа». Как отмечалось ранее в этом отчете, ИИ должен быть обучен работе с данными. Без таких данных он не сможет отфильтровывать контент. В то же время, как будет отмечено в следующей главе, ИИ сталкивается с серьезными проблемами в отношении уровней сложности в использовании языка, особенно иронии и юмора, которые могут значительно снизить эффективность автоматической модерации контента. Нынешние модели также часто обучаются основным языкам и поэтому менее надежны для языков меньшинств, таких как языки, на которых в основном говорят в регионе Южной и Юго-Восточной Азии. В связи с этим автоматическая модерация контента может или, скорее, не должна быть полностью автоматизирована. Человеческий надзор за процессами обзора и принятия решений остается необходимостью. Несмотря на ограничения, решения для автоматической модерации контента все чаще считаются незаменимыми в частном секторе в свете огромного количества контента, публикуемого в Интернете каждый день.

Естественно, учитывая характер рассматриваемой проблемы, национальные власти традиционно имели ограниченные полномочия по модерации и удалению контента. В ответ на растущую критику по поводу того, что при существующих формах саморегулирования социальные медиа-компании не в состоянии бороться с распространением такого контента, несколько стран попытались принять национальное законодательство, направленное на то, чтобы заставить компании делать больше. Например, это может быть достигнуто путем регулирования того, как быстро должен удаляться контент, а также путем установления стимулов и наказания за несоблюдение. Например, Закон о защите сети в Германии является одним из примеров национального законодательства, получившего известность в 2017 году, когда он стал одним из первых принятых таких инструментов.

Другим примечательным примером является недавно принятое постановление ЕС о борьбе с распространением террористического контента в Интернете, которое обязывает удалять террористический контент в течение одного часа после получения уведомлений об удалении.

Некоторые национальные органы власти также начали применять более «практический» подход. Например, правоохранительные органы и агентства по борьбе с терроризмом в нескольких странах, а также в рамках Европола начали пытаться самостоятельно удалять онлайн-террористический и насильственный экстремистский контент, используя механизмы пометки контента на платформах, чтобы сообщать о контенте как о нарушении условий предоставления услуг платформ. В этой связи, точно так же, как ИИ занял видное место с точки зрения того, как платформы социальных сетей автоматизируют модерацию контента, ИИ также может сыграть роль в повышении возможностей таких интернет-справочных подразделений в правоохранительных органах и контртеррористических агентствах просматривать огромное количество создаваемого контента. Примечательно, что в этой связи Министерство внутренних дел Соединенного Королевства и ASI Data Science объявили в 2018 году о разработке новой технологии, которая использует машинное обучение для анализа аудиовизуального контента в Интернете, чтобы определить, может ли он быть пропагандой ИГИЛ. По данным Министерства внутренних дел, тесты показали, что инструмент может автоматически обнаруживать такой контент с точностью 99,995%. Методология, лежащая в основе этого инструмента, не была обнародована.

5. Противодействие террористическим и насильственным экстремистским повествованиям

Хотя удаление террористического и насильственного экстремистского контента из Интернета или социальных сетей может в определенной степени быть эффективным в предотвращении распространения вредных повествований, это исключительно противоречиво и вызывает серьезные

проблемы в области прав человека. Кроме того, важно отметить, что удаление контента никоим образом не способствует устранению коренных причин терроризма и подвергает риску уязвимых лиц. Помимо простого выявления уязвимых лиц, алгоритмы NLP и машинного обучения могут играть еще более активную роль в борьбе с терроризмом в Интернете. ИИ можно использовать для анализа поведения пользователей и направления их на определенный контент, способствующий противодействию террористическим рассказам или запуску тактики таргетинга рекламы.

Moonshot со своим инновационным «Методом перенаправления», который был опробован в 2016 году с помощью Jigsaw от Google, использует автоматизированную оценку рисков и NLP для выявления уязвимых аудиторий на основе их поведения в онлайн-поиске. Например, если люди ищут определенный контент, соответствующий заранее определенным показателям, запускается реклама с положительным, дерадикализирующим контентом, и пользователи перенаправляются на рекламу и кураторские видео на канале YouTube, предназначенном для опровержения пропаганды ИГИЛ. В одном из таких видеороликов женщина на территории, контролируемой ИГИЛ, тайно записала свою жизнь, предоставив уникальное представление из первых рук о реальности жизни под властью ИГИЛ. Контент с контр-повествованием курируется в сотрудничестве с неправительственными организациями на местах, чтобы адекватно адаптировать сообщения к местным условиям. Это включает в себя неидеологический контент и контактные данные для линий помощи и индивидуальных вмешательств.

Хотя трудно измерить влияние таких подходов, как метод перенаправления, тем не менее, возможно, обнадеживает тот факт, что в ходе пилотного проекта программы целевые пользователи, которые были перенаправлены на такой контент, просмотрели более полумиллиона минут контента.

Примечательно, что Moonshot также провел ряд программ с использованием микро-таргетированной рекламы в Интернете в целях

дерадикализации, что позволило получить полезную информацию о стратегиях цифровой дерадикализации в Южной и Юго-Восточной Азии. Например, в 2020 году Moonshot провел эксперимент в Индонезии, связав уязвимых людей с психосоциальной поддержкой. Исследование показало, что пользователи, получающие психосоциальную поддержку, чаще занимались неидеологическим дерадикализирующим контентом, чем идеологическим дерадикализирующим контентом.

Лондонский институт стратегического диалога также использует инструменты рекламы в социальных сетях, основанные на ИИ, для противодействия нарративам ИГИЛ в Интернете, и в 2015 году запустил организованную кампанию по борьбе с ИГИЛ. В сотрудничестве с Сетью по борьбе с насильственным экстремизмом и при поддержке Facebook и Twitter институт нацелился на уязвимых людей, особенно подверженных риску стать мишенью пропаганды ИГИЛ.

Потенциал ИИ для того, чтобы играть определенную роль в противодействии террористическим повествованиям в Интернете, очевиден, особенно когда речь идет об охвате отдельных лиц и групп риска. Тем не менее, рассматриваемые инструменты ИИ могут быть лишь одной частью решения. ИИ может помочь соединить точки, но подлинное противодействие террористическим повествованиям в Интернете требует гораздо более тонкого понимания путей радикализации отдельных людей, которые могут позволить себе такие инструменты. Кроме того, нельзя сбрасывать со счетов важную роль организаций гражданского общества и подобных инициатив в этих процессах.

6. Управление большими требованиями к анализу данных

Анализ нападения на рождественский рынок в Берлине в 2016 году, так и взрыва на Манчестер-Арене в 2017 году свидетельствуют о том, что наборы данных следует использовать для перекрестной ссылки на информацию и проверки закономерностей для выявления соответствующих связей, поскольку в обоих случаях злоумышленники уже были в записях

местных властей в качестве объектов интереса. Несмотря на это, учитывая растущий объем и скорость сбора данных в рамках правоохранительных процессов, в частности в контексте онлайн-расследований, такой анализ часто невозможен.

Независимо от того, идет ли речь о противодействии терроризму онлайн или оффлайн, ИИ может сыграть значительную роль в расширении возможностей национальных органов власти эффективно обрабатывать большие объемы данных и при этом оптимизировать необходимый объем людских и финансовых ресурсов, выделяемых для любой конкретной ситуации. Более конкретно, ИИ может использоваться для извлечения соответствующей информации, фильтрации и сортировки данных, чтобы помочь определить приоритеты при анализе обширных наборов данных, которые могут выявить жизненно важные следственные зацепки и помочь спасти жизни.

Анализ аудиовизуального контента – это одна из задач, которая требует значительных специализированных людских ресурсов. С массовым расширением возможностей интеллектуальной видеозаписи в последние годы и в собственных возможностях наблюдения правоохранительных органов, в том числе с помощью замкнутого телевидения (CCTV) и использования камер, надеваемых на тело (или «камер для тела»), и патрульных беспилотных летательных аппаратов, произошло резкое увеличение количества видеоматериалов, требующих анализа. В контексте терроризма очень хорошо известно, что террористические группы и отдельные лица широко используют средства видео и активно обмениваются и распространяют такой контент в Интернете. Более того, при рассмотрении онлайн-расследований по борьбе с терроризмом также уместно учитывать, что, по данным CISCO, к 2021 году, по оценкам, 82% потребительского интернет-трафика будет составлять видео. В свете этого работа детективов по цифровой криминалистике огромна и растет.

Распознавание лиц, биометрическое применение распознавания объектов на базе ИИ, является одной из технологий, которая предлагает значительные перспективы с точки зрения возможности анализа видеоматериалов

для идентификации интересующих лиц. Внедрение технологии распознавания лиц резко возросло за последние несколько лет, чему способствовало быстрое совершенствование машинного обучения. Программное обеспечение для распознавания лиц требует высококачественных фотографий для справочной базы данных для идентификации целевых лиц. Несколько правоохранительных органов по всему миру уже начали экспериментировать с использованием этой технологии. Например, в 2017 и 2018 годах Федеральная полиция Германии опробовала систему видеонаблюдения с поддержкой распознавания лиц на одном из самых оживленных железнодорожных вокзалов Берлина. Заключительный отчет пилота подтвердил перспективность использования технологии для выявления соответствующих субъектов, таких как террористы или насильственные преступники, в людных общественных местах. Интерпол также управляет системой распознавания лиц, которая содержит изображения лиц, полученные из более чем 179 стран. Изображения лиц в уведомлениях и сообщениях, запрашиваемых странами-членами, ищутся и хранятся в системе распознавания лиц в соответствии с Правилами Интерпола по обработке данных. Такие инструменты, как распознавание лиц, также могут быть особенно полезны для судебных следователей, анализирующих видеодоказательства, собранные в Интернете. В то же время, однако, растущее использование технологии распознавания лиц властями по всему миру способствовало значительной негативной обратной связи со стороны правозащитных групп и организаций гражданского общества, которые выразили озабоченность по поводу потенциала этой технологии, в частности, для отражения и сдерживания ранее существовавших предубеждений в правоохранительных органах.

IV. ЧЕМ БОЛЬШЕ ВОЗМОЖНОСТЕЙ, ТЕМ СЛОЖНЕЕ ЗАДАЧА

Как показали шесть примеров использования ИИ, описанных в предыдущей главе, потенциальное применение ИИ для противодействия

угрозе терроризма в Интернете, очевидно, велико и, следовательно, заслуживает пристального рассмотрения правоохранительными и контртеррористическими органами. Несмотря на это, применение ИИ ни в коем случае не следует рассматривать как «быстрое и простое» решение, о чем говорилось на нескольких этапах в этом отчете. Хотя технология, безусловно, привлекательна, существуют широкие правовые, политические и технические проблемы, о которых все правоохранительные органы и агентства по борьбе с терроризмом должны знать заранее, а также во время внедрения технологий на основе ИИ. Хотя действия, необходимые для решения многих из этих проблем, могут в большей степени зависеть от директивных органов государств-членов или поставщика технологий, важно, чтобы правоохранительные органы и контртеррористические учреждения были осведомлены о полном спектре проблем, которые может представлять ИИ, и, при необходимости, для создания необходимых механизмов надзора.

Как и в предыдущих главах, нижеследующее не является исчерпывающим обзором проблем, с которыми может столкнуться ИИ. Скорее, он задуман как вводный обзор нескольких ключевых межсекторальных проблемных областей. Важно отметить, что каждый из вариантов использования, описанных в предыдущей главе, также будет сопряжен со своими уникальными проблемами. Соответственно, правоохранительным органам и контртеррористическим учреждениям, стремящимся изучить любую из этих проблем, потребуется дополнительно провести тщательную оценку в каждом конкретном случае, чтобы лучше понять конкретные проблемы, возникающие при каждом отдельном использовании.

1. Правовые и политические проблемы

А. Проблемы в области прав человека

Главной из ИИ в борьбе с терроризмом, является вполне реальный и серьезный потенциал для использования этих технологий в целях ущемления прав человека и основных свобод. Генеральная Ассамблея Организации

Объединенных Наций уже давно утверждает, что государства обязаны уважать и осуществлять права человека и защищать отдельных лиц от злоупотреблений со стороны негосударственных субъектов в контексте борьбы с терроризмом. Кроме того, в своей резолюции о поощрении, защите и осуществлении прав человека в Интернете Совет по правам человека подтвердил, что права человека применяются в Интернете в той же степени, что и в автономном режиме. В дополнение к воздержанию от использования ИИ якобы незаконным образом, таким как развертывание систем наблюдения с поддержкой ИИ сверх того, что необходимо и соразмерно законной цели, властям необходимо учитывать другие менее явные риски для прав человека, связанные с использованием ИИ, такие как потенциал алгоритмов машинного обучения, использующих необъективные данные для усиления предвзятости с помощью автоматизированных процессов и, следовательно, получения дискриминационных результатов.

Из широкого спектра прав человека, на которые может повлиять неправомерное использование технологий с поддержкой ИИ, право на неприкосновенность частной жизни, свободу мысли и выражения мнений и недискриминацию часто определяются как наиболее затрагиваемые права. Это вытекает из характеристик, присущих ИИ. Как уже отмечалось, разработка технологий с поддержкой ИИ требует больших объемов данных для обучения моделей. Некоторые из этих данных, скорее всего, являются личными данными. В резолюции 68/167 Генеральной Ассамблеи Организации Объединенных Наций о праве на неприкосновенность частной жизни в цифровую эпоху «незаконный или произвольный сбор персональных данных» описывается как крайне навязчивый акт, который может нарушать «права на неприкосновенность частной жизни и свободу выражения мнений и может противоречить принципам демократического общества». Кроме того, данные, вводимые в алгоритмы, часто загрязнены человеческими предубеждениями, и внедрение этих моделей может привести к усилению этих предубеждений и, следовательно, повлиять на право на недискриминацию.

Примечательно, что не все технологии с поддержкой ИИ представляют аналогичный риск для прав человека. Как отмечалось во второй и третьей главах, ИИ – это обширная область и различные типы приложений в разной степени влияют на права человека.

Права на неприкосновенность частной жизни, свободу мысли и выражения мнений и недискриминацию предусмотрены в Универсальной декларации прав человека, а также в различных международных и региональных договорах, включая широко ратифицированный Международный пакт о гражданских и политических правах и Декларацию прав человека АСЕАН. Учитывая актуальность этих прав в онлайн-пространстве, в этом подразделе основное внимание уделяется ключевым проблемам, связанным с последствиями использования технологий с поддержкой ИИ для борьбы с терроризмом в Интернете. Однако, правоохранительные и контртеррористические органы должны иметь в виду, что использование инструментов ИИ для борьбы с терроризмом в Интернете может повлиять на другие права человека. Например, на право на презумпцию невиновности и права на справедливое судебное разбирательство также потенциально сильно влияет использование доказательств, созданных ИИ, которые, учитывая непрозрачность ИИ, обвиняемым может быть трудно оспорить в суде.

Еще одно общее замечание, которое следует иметь в виду, заключается в том, что большинство прав человека не являются абсолютными и могут быть ограничены при соблюдении определенных требований. В целом, ограничения прав человека, предусмотренные Международным пактом о гражданских и политических правах, включая неприкосновенность частной жизни, свободу выражения мнений и недискриминацию, допускаются, когда такие ограничения юридически установлены законом и являются необходимыми и соразмерными для достижения законной цели.

Как описано в докладе бывшего Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение

Фрэнка Ла Ру, право на неприкосновенность частной жизни защищает «частную сферу» каждого человека, «область автономного развития, взаимодействия и свободы», где они защищены «от вмешательства государства и от чрезмерного нежелательного вмешательства других незваных лиц». Право на неприкосновенность частной жизни также подразумевает «способность отдельных лиц определять, кто владеет информацией о них и как эта информация используется». Для обеспечения права на неприкосновенность частной жизни во все более цифровом мире на региональном и национальном уровнях по всему миру были утверждены рамки конфиденциальности данных. Многие страны, в том числе в Южной и Юго-Восточной Азии, приняли законы о защите персональных данных. Как подчеркивается в Докладе Верховного комиссара Организации Объединенных Наций по правам человека о праве на неприкосновенность частной жизни в цифровую эпоху, хотя эти законы и рамки различаются по содержанию, большинство из них следуют набору общих принципов, в том числе о том, что обработка персональных данных должна быть «справедливой, законной и прозрачной», а также ограничиваться тем, что «необходимо и соразмерно законной цели». По возможности следует применять такие методы, как анонимизация данных и псевдонимизация.

Инструменты ИИ, включающие массовый сбор нецелевых персональных данных, по своей сути рискуют вторгнуться в частную жизнь отдельных лиц. Как отмечается в Справочнике ЮНОКТ и Интерпола по онлайновым контртеррористическим расследованиям, «Массовый, нецелевой и неизбирательный сбор данных вряд ли будет соответствовать требованиям необходимости и соразмерности. Аналогичным образом, хранение данных дольше, чем необходимо, может нарушать международные законы о правах человека или защите данных». По этой причине «законы, устанавливающие автоматический сбор, хранение и использование персональных данных, должны включать подробную информацию о целях, для которых собираются данные, способе их использования, о том, кто имеет доступ к данным, о целях,

для которых они могут использоваться, и о продолжительности времени, в течение которого данные могут храниться». С другой стороны, даже когда государства определяют условия, при которых эти вторжения юридически оправданы, они должны учитывать, что собранная информация может быть использована и использована не по назначению злоумышленниками.

Хотя риски ИИ для конфиденциальности часто подчеркиваются, иногда утверждается, что инструменты с поддержкой ИИ могут повысить конфиденциальность отдельных лиц. Аргумент предполагает, что автоматизированный сбор и оценка информации делает людей менее уязвимыми для анализа персональных данных человеком и приводит к более эффективным целенаправленным операциям, направленным на данные, относящиеся к подозрительным лицам. С другой стороны, встречные утверждения утверждают, что «алгоритмическое профилирование» может считаться более навязчивым, чем профилирование человека, и поэтому более опасным для прав человека. Также утверждается, что сбор массовых данных в Интернете с целью сбора разведданных может существенно усилить отношения между правительствами и гражданами, поскольку это наносит ущерб сути надежного режима. Государственное вторжение посредством надзора за онлайн-платформами превращает государства в «цифровые авторитарные государства».

Тем не менее, тип используемой технологии и, следовательно, необходимый сбор и хранение потенциально конфиденциальных данных имеют различные последствия для права на неприкосновенность частной жизни. Автоматизированные инструменты, которые помогают правоохранительным органам анализировать законно собранные данные и находить закономерности или сопоставлять лица подозреваемого с данными из открытых источников или иным образом законно собранными данными из учетных записей социальных сетей, должны отличаться от технологий, которые направлены на мониторинг социальных сетей и других онлайн-источников в режиме реального времени для выявления соответствующих зацепок

для контртеррористических операций. В то время как первый набор инструментов может соответствовать требованиям по ограничению частной жизни отдельных лиц, последние слишком вторгаются в частную жизнь в основном невинных людей, чтобы быть разрешенными в соответствии с законодательством о правах человека.

Права на свободу мысли и выражения включают как «внутреннюю» свободу безоговорочно придерживаться и изменять мысли, совесть, религию, убеждения или мнения, так и «внешнюю» свободу выражать эти мысли, совесть, религию, убеждения или мнения.

Государства могут ограничить «внешнюю» свободу выражения убеждений или претворить их в жизнь, если будут выполнены соответствующие требования. Поэтому при определенных обстоятельствах может быть разрешена модерация и удаление контента, в том числе с помощью решений ИИ. Технология борьбы с терроризмом, инициатива, выдвинутая Исполнительным директоратом Контртеррористического комитета Организации Объединенных Наций (ИДКТК), призвала директивные органы обеспечить четкое регулирование того, что является незаконным контентом и как с ним поступать, избегая удаления контента, защищенного свободой выражения мнений. В этой связи стоит отметить, что экстремисты и террористы все чаще предпочитают общаться через небольшие платформы, используя разнообразную среду онлайн-сервисов от облачных хранилищ до зашифрованных мессенджеров, чтобы избежать препятствий, связанных с ужесточением мер и удалением вредоносного контента на более крупных онлайн-платформах. Как отмечалось выше, небольшим компаниям часто не хватает финансовых и людских ресурсов, чтобы предотвратить использование их платформ злоумышленниками. Четкое регулирование того, что считается террористическим и другим вредоносным контентом и как с ним бороться, в сочетании с мероприятиями по наращиванию потенциала для небольших платформ, может поддержать усилия компаний по борьбе с этим риском террористической эксплуатации. Тем не менее, сохраняющееся отсутствие

общепринятого определения терроризма, объясненного в следующем подразделе, остается препятствием для государств, а также как для небольших, так и для крупных компаний, чтобы должным образом преодолеть противоречие между необходимостью обеспечения умеренности контента и правом на свободу выражения мнений.

Право на свободу мысли в его «внутреннем» измерении является абсолютным правом, которое не может быть ограничено или нарушено государствами ни при каких обстоятельствах. Это особенно важно отметить при рассмотрении потенциала определенных технологий, в том числе технологий с поддержкой ИИ, влиять на мысли людей. Развертывание автоматизированных приложений для противодействия террористическому использованию Интернета путем мониторинга пользовательского контента в Интернете может нарушить свободу мысли, поскольку это может спровоцировать действия, основанные на поведении людей в Интернете, которые представляют собой мысли. Инструменты с поддержкой ИИ интерпретируют ежедневные интерактивные взаимодействия и оценивают их как «внешние признаки внутренних мыслей, указывающие на то, кто представляет угрозу безопасности, чтобы позволить правоохранительным органам или службам безопасности предпринять превентивные действия, чтобы остановить превращение мысли в действие». Аналогичным образом, правоохранительные органы и контртеррористические учреждения, стремящиеся использовать технологии с поддержкой ИИ для направления пользователей, подверженных риску радикализации, на контент, противоречащий повествованию, должны учитывать возможность того, что эти технологии могут привести к незаконному вмешательству в право на свободу мысли путем манипулирования тем, как думают целевые пользователи.

Право на недискриминацию гарантирует, что ни к одному человеку не будет относиться менее благосклонно из-за того, что он обладает определенными защищенными характеристиками, такими как раса, пол,

этническое происхождение или религия. Дифференцированное обращение может быть оправдано, если оно преследует законную цель, которая должна быть обоснована и достигнута соразмерными средствами. Поэтому меры по борьбе с терроризмом, направленные в Интернете против отдельных лиц на основе их защищенных характеристик, могут нарушать право на недискриминацию. Это особенно верно для инструментов ИИ, отслеживающих индивидуальное поведение в Интернете, проверяя индикаторы, которые могли бы выступать в качестве прокси для защищенных характеристик. На самом деле следы защищенных характеристик часто скрыты. Более того, сохраняющаяся проблема предвзятости в ИИ, более подробно описанная ниже, часто влияет на право на недискриминацию, например, из-за непропорциональной ориентации на лиц, принадлежащих к определенным обездоленным группам. Примеры из других областей, помимо сбора конфиденциальной оперативной информации, неоднократно демонстрировали, как системы с поддержкой ИИ могут дискриминировать уязвимые группы. Нет никаких оснований полагать, что системы правоохранительных органов не будут страдать от тех же недостатков. Использование ИИ в государственных органах часто оправдывается повышением эффективности, однако это не может оправдать неравное обращение.

B. Допустимость доказательств, полученных с помощью ИИ, в суде

Хотя в принципе существует несколько случаев использования ИИ, которые могут иметь отношение к правоохранительным органам и учреждениям по борьбе с терроризмом для борьбы с онлайн-терроризмом в Интернете, практическая полезность любого такого случая использования напрямую связана с возможностью его использования для привлечения к ответственности в суде. Если действия, предпринятые на основе закономерностей и корреляций, выявленных системами ИИ, не считаются

доказательными по своей природе, польза от использования инструментов ИИ неизбежно ограничена с точки зрения конечных пользователей.

В свете технических проблем, которые будут представлены в последующих разделах, в частности непрозрачности и риска предвзятости в отношении ИИ, доказательства, полученные в результате использования ИИ, могут оказаться недостаточными с точки зрения демонстрации надежности и аутентичности – аспектов, традиционно считающихся важными для допустимости доказательств. Как и во всех формах цифровых доказательств, доказательства, созданные ИИ, могут быть изменены намеренно или непреднамеренно. Кроме того, проблемы в области прав человека, о которых говорилось в предыдущем разделе, могут повлиять на соразмерность процессов с поддержкой ИИ, используемых для сбора доказательств. Другими словами, преимущества использования инструментов ИИ в интересах безопасности и правосудия и доказательная ценность доказательств, полученных с помощью ИИ, могут не оправдывать риски для прав человека, создаваемые внедрением систем ИИ правоохранительными и контртеррористическими учреждениями.

Хотя последствия этого варьируются в зависимости от правовой системы и структуры каждой страны, при отсутствии правовой определенности и растущем объеме юридических дискуссий, развивающихся вокруг этой темы, использование инструментов ИИ для сбора доказательств, вероятно, столкнется с процедурными проблемами в судах по всему миру – по крайней мере, в обозримом будущем. Признавая это, правоохранительные органы, заинтересованные в изучении применения ИИ, призвали предоставить дополнительные рекомендации по допустимости доказательств, полученных с помощью ИИ, в суде, которые оценивают влияние и результаты конкретного использования инструментов ИИ при обеспечении уважения прав человека и верховенства закона.

Примечательно, что в известном деле COMPAS 2016 года в Соединенных Штатах, касающемся прогностической аналитической модели, используемой

судьями и сотрудниками по условно-досрочному освобождению для оценки вероятности повторного правонарушения обвиняемого по уголовному делу, Суд разрешил использовать оценку риска, сгенерированную ИИ, с определенными ограничениями, а именно, что необходимо четко сформулировать опасения относительно точности оценки риска, и оценки риска не могут быть использованы для определения порогового вопроса о том, следует ли заключать человека в тюрьму или строгости приговора.

Однако, как уже отмечалось, даже в том случае, если доказательства, основанные на ИИ, не соответствуют юридическим пороговым значениям, необходимым для использования в суде, инструменты ИИ, тем не менее, могут быть полезны для правоохранительных органов и контртеррористических учреждений, борющихся с терроризмом в Интернете, привлекая внимание следователей к конкретным закономерностям или отклонениям в закономерностях, которые могут привести к выявлению других форм допустимых доказательств.

C. Фрагментированный ландшафт определений

Хорошо известно, что общепринятого определения терроризма не существует, и это реальность, которая вряд ли изменится в ближайшем будущем. В равной степени отсутствует ясность или понимание точных процессов радикализации. Эти реалии имеют несколько серьезных последствий с точки зрения использования ИИ для борьбы с терроризмом в Интернете, препятствуя использованию технологии.

Отсутствие общего понимания того, что определяет терроризм, неизбежно приводит к отсутствию ясности в отношении того, что представляет собой террористический контент в Интернете. Поэтому специалисты, стремящиеся умерить содержание, должны учитывать различные интерпретации того, что определяет терроризм, и, конечно же, политику, которая с ним связана. Технология борьбы с терроризмом недавно подчеркнула настоятельную необходимость решения проблемы отсутствия определения

терроризма, рекомендуя разработчикам политики вносить вклад в усилия по борьбе с терроризмом в режиме онлайн, обеспечивая большую четкость определений «посредством улучшения определения».

Еще одна проблема заключается в том, что множество определений также может привести к фрагментированному сбору данных о терроризме и насильственном экстремизме в Интернете. Без фундаментальных знаний всеобъемлющим методам, основанным на эмпирических данных, наверняка не хватит точности, последовательности и сопоставимости. Кроме того, важно отметить, что радикализация или путь к терроризму очень индивидуальны и, следовательно, чрезвычайно сложны для отливки в форму, которую можно перевести в шаблоны для обработки автоматизированными моделями.

Наконец, на данном этапе важно также напомнить о постоянной озабоченности, а именно о том, что власти могут попытаться использовать национальное законодательство о терроризме для продвижения своей собственной политической повестки дня путем ограничения свободы слова правозащитников, журналистов или лиц, критикующих правительство, и это может быть отражено в том, как регулируются социальные сети. Эти проблемы можно считать острыми в некоторых частях Южной и Юго-Восточной Азии, которые имели спорную историю в отношении прав человека. События, подобные этому, вероятно, окажут сдерживающее воздействие на активность гражданского общества. Говоря о проблемах, которые могут возникнуть в подобных ситуациях, Брайан Фишман, который возглавляет усилия по борьбе с террористическими организациями и организациями, разжигающими ненависть, в Facebook, отметил, что для того, чтобы платформы социальных сетей не действовали косвенно как расширенная рука правительства посредством своей практики модерации контента, им потребуются согласованные на международном уровне списки обозначений определенных организаций или движений в качестве террористов.

D. Управление ИИ

Вопрос, который выходит далеко за рамки случаев использования в борьбе с терроризмом, представленных и обсуждаемых в этом докладе, заключается в том, как следует регулировать использование ИИ в целом, чтобы обеспечить справедливые, подотчетные и прозрачные системы ИИ. В частности, много споров возникло вокруг этичного и справедливого ИИ, направленного на устранение предвзятости или систематических искажений. Надежность таких систем – их устойчивость и безопасность – является еще одним аспектом, приобретающим все большее значение в политических дискуссиях, особенно в свете растущей интеграции ИИ в повседневную деятельность как в государственном, так и в частном секторе и последующего потенциала атак, направленных на функционирование или функциональность ИИ. Однако в настоящее время не определено универсально, что влечет за собой каждая из этих концепций с точки зрения регулирования. Тем не менее, управление ИИ обязательно повлияет на стандарты применения в борьбе с терроризмом.

Возможно, уместно отметить, что в апреле 2021 года Европейская комиссия представила предложение о регулировании, устанавливающем согласованные правила в отношении ИИ, которые, в случае их принятия Европейским парламентом и Советом ЕС, непосредственно станут жестким законом в государствах-членах ЕС и первой в истории наднациональной правовой базой по ИИ. Текущий проект примерно устанавливает, что правила применяются как к поставщикам, так и к пользователям систем ИИ, даже если они расположены за пределами ЕС, при условии, что системы или их выходные данные используются в ЕС. В этой связи, хотя проект закона об ИИ является предложением ЕС, он имеет международное значение для всех субъектов, изучающих использование ИИ. Важным выводом из сути проекта является его ориентированный на права человека подход к классификации систем ИИ по категориям в соответствии с их «неприемлемым», «высоким» или «низким риском» для прав человека. Эта классификация лежит в основе общего запрета проекта на использование правоохранительными органами распознавания лиц

в общественных местах. Несмотря на этот общий запрет, «предотвращение конкретного, существенная и неминуемая угроза жизни или физической безопасности физических лиц или террористического акта» это одно из исключений из запрета на использование технологии живого распознавания лиц в общественных местах в правоохранительных органах.

E. Отношения между государственным и частным секторами

Еще одна потенциальная проблема для правоохранительных и контртеррористических учреждений, стремящихся изучить возможности развития ИИ, касается роли частного сектора в противодействии использованию террористами Интернета и социальных сетей, хотя уместно отметить, что это проблема, которая выходит за рамки конкретной области ИИ.

В связи с постоянно растущей актуальностью онлайн-коммуникации, в том числе в плане борьбы с терроризмом, вес частного сектора значительно возрастает в связи с объемом их ресурсов и компетенций по отношению к государственным субъектам. В результате государственный сектор часто обращается к частным организациям, чтобы дополнить и поддержать их усилия по борьбе с терроризмом в Интернете. Это происходит не только потому, что любой террористический контент размещается на платформах или серверах, управляемых этими частными организациями, но и потому, что организации частного сектора обладают навыками и возможностями для онлайн-вмешательства, которых во многих отношениях просто не хватает правоохранительным органам и контртеррористическим учреждениям. Кроме того, частный сектор выполняет роль привратника, предоставляя доступ к данным, необходимым для обучения и использования алгоритмов ИИ, разработанных правоохранительными органами и контртеррористическими учреждениями. Частный сектор также, как правило, обладает более высоким потенциалом, чем государственный сектор, для разработки инновационных технологических инструментов, необходимых для борьбы с терроризмом в Интернете, и, таким образом, правоохранительным и контртеррористическим

учреждениям, возможно, потребуется сотрудничать с частным сектором и/или приобретать инструменты у него.

Отношения между государственным и частным секторами в контексте борьбы с терроризмом в Интернете не являются прямыми отчасти из-за их различного характера и целей. Например, контент, который мог бы побудить правоохранительные органы к действиям, в прошлом удалялся и удалялся частными компаниями, тем самым уничтожая важные доказательства для следователей. В одном конкретном случае компании социальных сетей даже удалили доказательства, свидетельствующие о военных преступлениях, которые могли быть использованы правоохранительными органами. Хотя можно утверждать, что предпочтительнее удалять вредоносный контент, в настоящее время такой контент не архивируется таким образом, чтобы он был доступен для расследования, если только власти не предъявят повестку в суд, судебный приказ или ордер компаниям, ответственным за платформы. Таким образом, правоохранительным органам может быть неясно, могут ли у них отсутствовать соответствующие доказательства, поскольку они не знают, могут ли такие доказательства существовать, или, если да, то как долго хранятся данные до их удаления.

Еще одной проблемой в этом контексте является технический опыт, необходимый для разработки, разработки и обслуживания приложений ИИ, который в большей степени сосредоточен в частном секторе и, если на то пошло, особенно сосредоточен в руках крупных технологических фирм, которые традиционно преуспевали в привлечении студентов и преподавателей из университетов.

В этой связи правоохранительным органам и контртеррористическим учреждениям необходимо будет бороться и налаживать более тесные отношения с частным сектором, если они хотят полностью понять использование Интернета и социальных сетей террористическими группами и отдельными лицами или получить доступ к инструментам ИИ или разработать или использовать свои собственные инструменты ИИ. Однако

следует признать, что агентства в некоторых странах Южной и Юго-Восточной Азии могут обладать ограниченными переговорными возможностями по отношению к крупным технологическим компаниям.

2. Технические проблемы при использовании инструментов ИИ

А. Ложные положительные и ложные отрицательные результаты

При оптимизации точности алгоритмов разработчики ИИ могут изменить пороговое значение, которое устанавливает классификационную метку на положительную или отрицательную. Регулируя этот порог, можно контролировать два типа ошибок: ложные срабатывания и ложные отрицания. Ложные положительные результаты могут быть поняты как случаи, когда неверно указан положительный результат, а ложные отрицательные результаты могут быть поняты как случаи, когда неверно указан отрицательный результат. Поскольку некоторая погрешность в выводе алгоритмов неизбежна и невозможно одновременно уменьшить как ложные положительные, так и ложные отрицательные результаты, необходимо выбрать, какая коррекция должна быть приоритетной. Этот выбор не является простым, поскольку как ложные отрицательные, так и ложные положительные результаты могут иметь значительные последствия. В прогностической модели, которая пытается идентифицировать террористических субъектов (рассматриваемых как положительный ярлык), уменьшение ложных отрицательных результатов подразумевает увеличение ложных положительных результатов, что приводит к принятию ошибочного определения кого-либо как террориста. Это сводит к минимуму риск того, что потенциально опасные люди пройдут через алгоритм незамеченными, но могут не избирательно обременять гражданских лиц. С другой стороны, оптимизация для ложных срабатываний увеличивает ложноотрицательные результаты. Этот подход ставит во главу угла предотвращение неверной идентификации кого-либо как террориста, но также проявляет большую терпимость к соответствующим субъектам,

ускользающим незамеченными. Соответственно, точная классификация порога может оказать существенное влияние на результаты развернутой модели ИИ.

B. Искажение данных

Справедливость в ИИ – это декларируемая цель во многих областях технической индустрии, политики, научных кругов и гражданского общества, а также один из ключевых принципов, пропагандируемых с точки зрения ответственного использования ИИ. Это подразумевает, что алгоритмические решения не оказывают дискриминационного или несправедливого воздействия на конечных пользователей – как это было в случае с вышеупомянутым алгоритмом рецидивизма COMPAS. Расследование, проведенное независимой редакцией новостей ProPublica, показало, что алгоритм, используемый судьями и сотрудниками по условно-досрочному освобождению в Соединенных Штатах для оценки вероятности повторного правонарушения обвиняемого по уголовному делу, был предвзятым в отношении определенных расовых групп. Анализ инструмента показал, что ответчики-афроамериканцы с большей вероятностью будут ошибочно оценены как подверженные более высокому риску рецидива, чем ответчики-кавказцы, т.е. среди афроамериканского сообщества было значительно больше ложноположительных результатов, в то время как ответчики-кавказцы с большей вероятностью, чем ответчики-афроамериканцы, будут ошибочно помечены как низкий риск, что означает, что уровень ложноотрицательных результатов был повторно высоким в кавказском сообществе, создавая дифференцированный подход для двух групп. Еще один громкий пример алгоритмической дискриминации, на этот раз связанный с предвзятостью по признаку пола, был выявлен в 2018 году, когда инструмент автоматического найма ИИ Amazon был закрыт после того, как было замечено, что он приводит к предвзятому отношению к женщинам. Основываясь на доминировании мужчин в технологической компании, система Amazon сама научила себя тому, что кандидаты мужского пола предпочтительнее.

Несмотря на высокое стремление, обеспечение справедливости в ИИ может быть исключительно сложным делом. Бесспорно, технология сама по себе является нейтральным статистическим и математическим процессом, но ИИ может усилить существующие предубеждения общества при обучении с использованием необъективных наборов данных, что приводит к случаям автоматизированных решений, дискриминирующих отдельных лиц, группы и сообщества по запрещенным основаниям.

В дополнение к риску дискриминации, вытекающему из данных обучения, которые отражают присущие обществу предубеждения, также было высказано предположение, что однородная технологическая среда приводит к слепым зонам при разработке программного обеспечения, также вызывая дискриминационные последствия. Это послужило причиной призыва к более разнообразному представительству в технологических компаниях.

Наконец, также важно отметить, что, хотя смещение в наборах данных может быть непреднамеренным, данными также можно сознательно манипулировать. Манипулируемые данные могут оказывать такое же воздействие, как и необъективные данные, используемые для обучения модели, поскольку они могут воспроизводить аналогичные вредные эффекты. Набор данных, который был изменен, трудно обнаружить извне, особенно для нетехнических экспертов. В области безопасности, и особенно в приложениях для борьбы с терроризмом, это слабое место, которое необходимо устранить путем строгого регулирования использования и доступа к системе, а также регулярного мониторинга системы и ее производительности.

C. Объяснимость и проблема черного ящика

Еще одним принципом, который часто подчеркивается как важный для ответственного использования ИИ, является понятие объяснимости. Тесно связанный с требованием прозрачности, объяснимость фокусируется на обеспечении того, чтобы ИИ не был так называемым «черным ящиком»

и чтобы алгоритмические решения могли быть поняты конечными пользователями в нетехнических терминах.

Системы глубокого обучения часто описываются как черные ящики, поскольку они комбинируют и рекомбинируют атрибуты многими произвольными способами. После ввода данных внутреннее поведение, которое приводит систему к выходу, может быть неясным. Другими словами, люди не могут понять, как системы глубокого обучения дают результаты. Это затрудняет отслеживание и проверку результатов, что может вызвать проблемы с точки зрения прав человека, в частности права на справедливое судебное разбирательство и надлежащую правовую процедуру для обвиняемого или отдельных лиц, а также затруднить привлечение к ответственности, что, в свою очередь, может повлиять на право на эффективное средство правовой защиты тех, чьи права были несправедливо ограничены или нарушены в результате внедрения систем ИИ. Понятие объяснимости в этой связи требует, чтобы конечные пользователи могли интерпретировать информацию, извлеченную из черного ящика, и понимать, какие элементы, используемые в модели машинного обучения, отвечали за каждый конкретный результат.

Недостаток объяснимости может быть устранен только при глубоком техническом понимании нейронной сети и при поддержке инструментов объяснимости для локальных и глобальных решений, таких как SHAP или LIME. Инструменты объяснимости могут помочь объяснить и представить в понятных терминах функции в данных, которые были наиболее важны для модели, и влияние каждой функции на любой конкретный результат.

D. Сложность контента, созданного человеком

Как уже говорилось, необходимым условием для разработки надежных инструментов ИИ является наличие доступа к точным и подробным наборам данных. Хотя многие из проблем, представленных в этом докладе, носят глобальный характер, Южная и Юго-Восточная Азия представляют особые

дополнительные соображения, учитывая большое разнообразие регионов с точки зрения языков и диалектов. В качестве примера рассмотрим, что в настоящее время в Азии в целом говорят примерно на 2300 языках. Хотя в NLP было достигнуто большое количество достижений, подавляющее большинство усилий в этой области сосредоточено на нескольких ключевых языках: английском, китайском, урду, фарси, арабском, французском и испанском – и из них английский в значительной степени предпочтителен. В отношении других так называемых языков с низким уровнем ресурсов было получено мало результатов.

Кроме того, языки, на которых говорят в Южной и Юго-Восточной Азии, – как и все языки в мире – динамичны, постоянно развиваются и адаптируются к социальным изменениям. Эта естественная динамика также создает серьезные проблемы для ИИ, поскольку системы ИИ не могут самостоятельно адаптироваться к меняющимся условиям, а скорее требуют больших объемов данных для обеспечения адаптации. В этом смысле наборы данных должны постоянно отслеживаться и обновляться по мере необходимости. Для многих менее известных языков или диалектов в регионах вероятная нехватка необходимых данных для обучения может представлять проблему.

Примером практических проблем, с которыми ИИ может столкнуться в этом контексте, недавно был случай, когда алгоритмы, разработанные для выявления и блокирования вредоносного контента на Facebook, неоднократно вводились в заблуждение крайне правой экстремистской группой в Соединенных Штатах, которая использовала зашифрованный язык для общения в Интернете и открыто делилась инструкциями по изготовлению бомб. Незнакомые с используемым кодом, алгоритмы не смогли обнаружить содержимое.

Контекст может добавить дополнительный уровень сложности, поскольку он определяет более тонкие нюансы человеческого общения, которые приводят к иронии и юмору. Обнаружение иронии или сарказма – это обманчиво сложная задача даже для людей, поскольку она варьируется от человека к человеку

и сильно зависит от культуры, а также многих других аспектов, таких как выражение лица и тон. В области анализа настроений NLP сарказм является специфической областью изучения, поскольку его нельзя классифицировать как негативное или позитивное настроение. Недавние исследования показывают, что один только сарказм может привести к снижению точности на 50% при автоматическом определении настроений. Подходы к решению этой проблемы включают добавление слоев информации для лучшего понимания взаимосвязи между говорящим и средой, таких как анализ прагматических функций, таких как смайлики, хэштеги и упоминания; использование несоответствия контекста, когда определенные функции показывают, что контекст не соответствует содержанию текста; использование пользовательских вложений, которые кодируют стилистику и индивидуальность пользователей.

В мае 2021 года Twitter запустил новую функцию предупреждения о разжигании ненависти, которая просит людей просматривать ответы с потенциально вредными или оскорбительными выражениями. Ранние тесты показали, что алгоритмы «изо всех сил пытались уловить нюансы во многих разговорах и часто не различали потенциально оскорбительные выражения, сарказм и дружеское подшучивание». Улучшения в системе подсказок включали добавление пользовательских вложений, таких как отношения пользователя и ответчика и происхождение пользователя. Пример из Шри-Ланки также продемонстрировал, как алгоритмы Facebook не смогли оценить многослойный культурный контекст. Сообщения, созданные пользователями в социальных сетях до пасхальных взрывов в Коломбо в апреле 2019 года, прошли через системы мониторинга, поскольку алгоритмы не могли идентифицировать высказывания ненависти в сообщениях из-за сложной культурной среды. Хотя технология постоянно развивается, это техническое ограничение может стать серьезным камнем преткновения для правоохранительных и контртеррористических органов, стремящихся

использовать ИИ для идентификации соответствующей информации в Интернете.

V. ПРОДВИЖЕНИЕ ВПЕРЕД С ПОМОЩЬЮ ИИ

Использование ИИ обладает значительным потенциалом для содействия борьбе с терроризмом в Интернете. ИИ может быть особенно полезен для поддержки правоохранительных органов в работе с большими объемами собранных данных путем классификации новых записей, извлечения закономерностей, выделения важной информации, событий или взаимосвязей и визуализации результатов. Это может помочь в поиске закономерностей и отношений, которые в противном случае могут остаться непризнанными, и может принести большую пользу правоохранительным органам и контртеррористическим учреждениям, чтобы переломить ход борьбы с терроризмом в Интернете. Однако существуют многочисленные политические, правовые и технические проблемы, и для правоохранительных и контртеррористических учреждений в Южной и Юго-Восточной Азии крайне важно признать эти проблемы. В этом отношении от любого агентства, изучающего или рассматривающего возможность продвижения вперед в применении ИИ, требуется значительная осмотрительность.

С учетом этого и признавая, что следует ожидать дальнейшего технического прогресса в области ИИ, для правоохранительных и контртеррористических учреждений в Южной и Юго-Восточной Азии предлагаются следующие рекомендации. Первый набор этих рекомендаций относится к конкретному региону, в то время как остальные пять носят универсальный характер и, следовательно, могут иметь одинаковое значение для правоохранительных или контртеррористических учреждений за пределами Южной и Юго-Восточной Азии, стремящихся изучить использование ИИ.

Эти рекомендации были составлены и классифицированы на основе отзывов, полученных от участников Совещания Группы экспертов ООН-ОКТ-

ЮНИКРИ. Порядок рекомендаций не следует толковать как указание на какой-либо конкретный приоритет.

Формирование регионального подхода:

– Признавая, что информация о текущих возможностях ИИ в Южной и Юго-Восточной Азии ограничена или недоступна для общественности, следует провести дальнейшие полевые исследования, чтобы понять текущие возможности и проинформировать о формировании индивидуального практического руководства по использованию ИИ для противодействия терроризму в Интернете в регионах.

– Усилия национальных органов власти должны быть направлены на каталогизацию существующих знаний в этой области на национальном уровне и во всех регионах, а также на выявление национальных экспертов в своих странах или в регионах.

– Усилия национальных органов власти должны быть направлены на разработку баз данных, содержащих законно собранные данные по конкретным регионам, для оказания помощи в разработке конкретных инструментов для Южной и Юго-Восточной Азии, и такие базы данных должны быть доступны исследователям.

– На региональном уровне следует создать форум для обмена идеями, опытом и проблемами в целях дальнейшего развития регионального корпуса знаний и опыта.

– Следует поощрять диалог и сотрудничество с организациями частного сектора, в частности с платформами социальных сетей, для содействия облегчению доступа к соответствующим учебным данным из Южной и Юго-Восточной Азии.

– Разработка приложений должна учитывать многокультурную и многоязычную реальность Южной и Юго-Восточной Азии, которая во многих отношениях отличает эти регионы от других.

Признайте ограничения ИИ:

– Правоохранительные и контртеррористические учреждения должны признать, что:

1. ИИ не совершенен и, возможно, никогда им не будет. По-прежнему существует множество технических проблем, и, хотя ИИ становится все более эффективным и точным, может потребоваться значительное количество времени, чтобы достичь уровней, требуемых как конечными пользователями, так и гражданским обществом, – если это вообще возможно достичь.

2. Не существует решения «один размер подходит всем». Инструменты ИИ должны быть адаптированы к конкретным контекстам и требованиям.

3. ИИ представляет результаты в виде вероятностных расчетов, а не безошибочных прогнозов.

4. ИИ не может в одностороннем порядке искоренить терроризм и насильственный экстремизм в Интернете. Инвестиции в ИИ должны сопровождаться усилиями по предотвращению радикализации и насильственного экстремизма в его корнях.

Уважать права человека и защищать гражданское общество:

– Следует признать потенциальное воздействие на права человека использования ИИ для борьбы с терроризмом в Интернете. Оценки воздействия на права человека должны проводиться до развертывания любых инструментов, и законность, соразмерность и необходимость их использования должны оцениваться на регулярной и постоянной основе на протяжении всего жизненного цикла инструмента ИИ.

– Необходимо разработать национальные законы и политику, определяющие и регулирующие использование инструментов ИИ для борьбы с терроризмом в Интернете, в частности, для устранения риска неправильного использования таких инструментов, например, для преследования законных общественных движений, организаций гражданского общества и журналистов, а также для сведения к минимуму риска нарушения функций.

– В отношении использования ИИ для борьбы с терроризмом в режиме онлайн следует применять многосторонний подход с регулярными циклами обратной связи, чтобы обеспечить выявление любых возможных «белых пятен» в проектировании, разработке и применении автоматизированных инструментов.

Установить технические гарантии:

– Решения, основанные на технологии с поддержкой ИИ, должны быть объяснимы. Следует использовать инструменты соблюдения прав человека и объяснимости, чтобы помочь преодолеть проблемы с «черными ящиками» и обеспечить подотчетность за любые действия или решения, основанные на системах ИИ.

– Наборы данных должны быть максимально свободными от предвзятости и максимально прозрачными для целей внешней оценки.

– Должны быть созданы надзорные механизмы, которые должны быть оснащены достаточным техническим опытом, чтобы иметь возможность понимать и надлежащим образом оценивать использование ИИ. Эти надзорные механизмы должны регулярно оценивать каждый случай использования систем ИИ, законность, соразмерность и необходимость их использования, а также качество результатов, которые они дают. Институциональные сдержки и противовесы должны основываться на прозрачной политике.

Развивать знания и наращивать потенциал:

– Правоохранительным и контртеррористическим учреждениям следует развивать свои собственные внутренние знания и технический потенциал, насколько это возможно, с тем, чтобы они могли осуществлять полный контроль над своей системой и вносить необходимые коррективы.

– Правоохранительные органы и контртеррористические учреждения должны тесно взаимодействовать с индустрией ИИ и исследовательским сообществом для расширения их знаний и понимания.

– Следует поощрять обмен опытом и проблемами между правоохранительными органами и контртеррористическими учреждениями, использующими ИИ для борьбы с терроризмом в Интернете, с тем, чтобы способствовать созданию сообщества практиков, основанного на ответственном использовании технологии.

– Следует проанализировать правовые требования, касающиеся отдельных случаев использования ИИ для борьбы с терроризмом в Интернете, особенно с точки зрения влияния ИИ на права человека.

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И АВТОНОМИЯ В РОССИИ

Перевод с английского ст. Джеффри Эдмондс, Сэмюэль Бендетт, Аня Финк, Мэри Чеснат, Дмитрий Горенбург, Майкл Кофман, Кейси Стриклин и Джулиан Уоллер

Аннотация

В этом отчете представлен всеобъемлющий обзор текущего состояния гражданского и военного ИИ в России, в котором рассматриваются все соответствующие сектора, ключевые институты и тенденции.

В частности, в докладе исследуется, как Россия применяет ИИ к своим военным возможностям.

Этот отчет является частью усилий CNA по предоставлению своевременной, точной и актуальной информации и анализа в области ИИ в России и следует за серией из более чем двадцати информационных бюллетеней, выходящих раз в две недели по той же теме. Он основан на русскоязычных материалах с открытым исходным кодом.

Документ содержит лучшее мнение CNA на момент выпуска. Это не обязательно отражает мнение спонсора.

Этот отчет был написан Отделом стратегии, политики, планов и программ CNA (SP3). SP3 обеспечивает стратегический и военно-политический анализ, основанный на региональном опыте, для поддержки лиц, принимающих решения на оперативном и политическом уровнях, в Департаменте военно-морского флота, Канцелярии Министра

обороны, объединенных командованиях комбатантов, разведывательном сообществе и внутренних учреждениях.

Отдел использует методы исследований в области социальных наук, полевые исследования, региональный опыт, основные языковые навыки, партнерские отношения по направлению, а также опыт в области политики и оперативной деятельности для поддержки старших руководителей.

CNA – некоммерческая исследовательская организация, которая служит общественным интересам, предоставляя углубленный анализ и ориентированные на результат решения, помогающие руководителям правительств выбирать наилучший курс действий при разработке политики и управлении операциями.

Резюме

Российское руководство рассматривает способность к инновациям как один из признаков великой державы и рассматривает военные инновации как важнейшее условие общей оборонной позиции России в условиях меняющейся обстановки и угрозы.

Цели российского ИИ и автономной экосистемы лучше всего поняты в контексте усилий по экономическому развитию и модернизации России и включают инициативы, направленные на повышение благосостояния российских граждан, а также условий для бизнеса и предпринимательской деятельности.

В следующем отчете подробно описана экосистема ИИ в России, где он является частью годовой работы, проводимой от имени Объединенного центра искусственного интеллекта Министерства обороны (JAIC), чтобы понять развивающуюся область ИИ и ее автономию в России. Уделяя особое внимание ИИ и автономии, в докладе также делается попытка поместить ИИ в более широкую технологическую среду в России.

Управление и правовые аспекты ИИ в России

Российское правительство создает структурную правовую и управленческую базу, необходимую для развития и конкуренции в быстрорастущей области ИИ и автономии. Оно пытается реализовать общенациональные стратегии с целями и показателями для содействия созданию среды, благоприятной для развития цифровых технологий, в частности ИИ в России.

Однако реализация этих усилий в значительной степени осуществляется правительством через государственные предприятия. И в то время как инициативы в области ИИ распространяются по всему российскому Правительству, отсутствие внимания к частным инициативам может нанести ущерб усилиям России в будущем. В то время как многие россияне надеются на преимущества большей оцифровки по всей России, существует также некоторая критика усилий правительства по расширению доступа к частным данным. Граждане России устали от бесконтрольного развития ИИ и его потенциального воздействия на общество.

Российская экосистема ИИ

Российская экосистема ИИ состоит из кластеров взаимосвязанных видов деятельности между государственными, государственно-корпоративными, военными, академическими и частными субъектами.

Однако ключевой особенностью российской экосистемы ИИ является ее лидерство со стороны государственных компаний и значительная часть федерального финансирования сектора ИИ. Эти государственные компании включают инкубаторы, спонсоров и инициативы, направленные на содействие развитию ИИ. Сильная зависимость от федерального финансирования вызывает у некоторых заинтересованных представителей в России опасения, что это подрывает инициативу, принятие технологических рисков и рост. В то время как опросы и международные рейтинги (такие как обзоры статей и рейтинги учреждений) говорят о том, что Россия отстает в области ИИ

от других, более крупных игроков, но все-таки она делает некоторые улучшения.

Академические учреждения, связанные с ИИ, подготовка кадров и образование

Россия сталкивается с нехваткой технически квалифицированных специалистов в коммерческом, промышленном и оборонном секторах, и это особенно касается области ИИ. Причины этого включают отток технологически подготовленных специалистов на высокооплачиваемую работу за рубежом, затяжные последствия распада Советского Союза и последовавшего за ним времени, а также неравномерную демографию на обширных территориях России.

Российское правительство признает эти проблемы и предпринимает шаги по их смягчению. Эти шаги включают в себя многочисленные программы, ориентированные на широкий круг демографических показателей, начиная от поощрения подготовленных технических экспертов и заканчивая обучением широких слоев населения технологиям, связанным с ИИ. Несмотря на эти шаги, слабые стороны в области образования и профессиональной подготовки, вероятно, будут в течение некоторого времени препятствовать попыткам России внедрить технологические инновации, в зависимости от того, как вступят в силу новые меры, подробно описанные в этом отчете, и сколько времени им потребуется для этого.

ИИ частного сектора в России

Технологические разработки и рост российского частного рынка ИИ обусловлены в первую очередь научно-исследовательскими разработками, поддерживаемыми государством, хотя частный спрос на ИИ-решения растет.

В целом, на частном рынке ИИ доминирует ориентация на использование достижений в области обработки естественного языка (NLP) и других форм

автоматизированного анализа данных, хотя интерес к компьютерному зрению и другим видам возможностей распознавания и прогнозирования растет.

Помимо широких автоматизированных приложений NLP для финансовых и розничных целей, наиболее важными технологиями ИИ, которые привлекли внимание частного рынка, являются программное обеспечение для распознавания лиц, безопасность объектов и периметра, беспилотные перевозки грузов и агробизнес, системы управления общественным транспортом и интеграция железнодорожной сети, автоматизированные платформы для обучения нейронных сетей и других методов ИИ, а также автоматизированный медицинский анализ.

Военный ИИ в России

Судя по высокопоставленным политическим и военным заявлениям и профессиональным военным трудам, российские эксперты в области ИИ необходимы для будущего успеха вооруженных сил России и являются ключом к ее военной мощи.

В то время как военный ИИ следовал многим из тех же тенденций в России, что и в других развитых странах военные, российское военное ведомство делает особый акцент на тех областях, на которых оно уже сосредоточено, таких как управление информацией для принятия решений и автономия.

Российские военные стратеги уделяют особое внимание установлению того, что они называют «информационным доминированием на поле боя», и технологии, улучшенные ИИ, обещают использовать преимущества данных, доступных на современном поле боя, для защиты собственных сил России и отказа в этом преимуществе противнику. При этом в российских вооруженных силах также продолжается дискуссия о конечной цели военного ИИ.

Существует распространенное мнение, что оператору необходимо оставаться в цикле принятия решений, чтобы избежать непредвиденных

последствий, как в военном, так и в этическом плане, но также и дискуссий, которые предсказывают полную автономию как неизбежную особенность будущего конфликта, частично подпитываемую интерпретациями намерений США, связанных с ИИ.

Международное сотрудничество

Несмотря на упомянутые выше проблемы, Россия стремится стать одним из ключевых лидеров мысли в области ИИ. Российские лидеры подчеркивают перспективы ИИ для жизни простых граждан, от медицинских инноваций до улучшения экономических показателей.

Однако российское руководство также подчеркивает опасность, которую ИИ может представлять в неправильных руках или с неправильными намерениями. Возможно, больше, чем кто-либо другой, российские лидеры сосредоточены на необходимости защиты традиций и внутренней стабильности своего общества, что отражает давнюю озабоченность России внешним вмешательством в российские дела.

Россия стремится к выгодному партнерству в области технологий и развития ИИ по всему миру; например, она заключила существенные соглашения с Китаем и Южной Кореей через Huawei и Samsung.

Однако Китай и Южная Корея являются скорее исключением, чем правилом. Геополитические интересы сотрудничества с Россией часто не перевешивают коммерческие выгоды, доступные в других экосистемах, таких как Соединенные Штаты и Европейский союз. Несмотря на это, мы ожидаем, что его растущие отношения с другими зрелыми технологическими обществами принесут некоторую пользу.

Аббревиатуры

ABM – противоракетная оборона

ACS – автоматизированные системы управления

AI – ИИ искусственный интеллект

APEC – АТЭС Азиатско-Тихоокеанское экономическое сотрудничество

ARF – Фонд перспективных исследований АРФ (Россия)

ASVN – военная автоматизированная система

BRICS – БРИКС Бразилия, Россия, Индия, Китай, и Южная Африка

C2 – командование и управление

CCTV – замкнутое телевидение

CCW – Конвенция ООН о конкретных видах обычного оружия

CNA – Центр военно-морских исследований

COVID – коронавирусная болезнь

DARPA – Агентство перспективных исследовательских проектов в области обороны

DOD – Министерство обороны США

ESU TZ – ЕСТУ Единая система тактического управления (Россия)

EC – Европейский Союз

EW – РЭБ радиоэлектронная борьба

FCS – Американская боевая система будущего США

FPRI – Институт исследований внешней политики

FSB – ФСБ Федеральная служба безопасности Российской Федерации

GDP – ВВП валовой внутренний продукт

GII – Глобальный индекс инноваций

GLONASS – Глобальная навигационная спутниковая система ГЛОНАСС (Россия)

GPS – Глобальное позиционирование

IADS – Интегрированная система ПВО

ICBM – МБР межконтинентальная баллистическая ракета

IHL – МГП Международное гуманитарное право

IISS – Международный институт стратегических исследований

IoT – интернет вещей Интеллектуальная собственность

ISR – ИСР разведка, наблюдение и разведка

IT – ИТ интернет-технологии

JADC2 – Министерство обороны США Объединенное командование и управление всеми областями

JAIC – Министерство обороны США Объединенный Центр искусственного интеллекта

KAIROS – Ориентированный на знания Искусственный интеллект, Рассуждения над схемами

KRUS – КРУС разведывательный, командный и коммуникационный комплекс

LAWS – ЗАКОНЫ смертоносные автономные системы вооружения

MIRT – МФТИ Московский физико-технический институт

MIT – Массачусетский технологический институт

MOD – МО РФ, Минобороны России

MSU – МГУ Московский государственный университет

NATO – Организация Североатлантического договора НАТО

NDMC – Национальный центр управления обороной (Россия)

NLP – обработка естественного языка

OECD –Организация экономического сотрудничества и развития ОЭСР

PPP – паритет покупательской способности

QS – Научно-исследовательские и опытно-конструкторские разработки

R&D – исследования и разработки

RANEPA – РАНХИГС Российская академия народного хозяйства и государственной службы при Президенте РФ

RD&T – Исследования и разработки, развитие и технологии

RF – РФ Российская Федерация

RUB – Руб. Российский рубль

S&T – научно-технический

STEM – Научно-техническая разработки и технологии STEM

T&E – технологии, инженерия, обучение и образование

ТЕРКОМ – контур местности, соответствующий времени

THE – Высшее образование

TIGER – ТИГР Технологии,

TSU – ТГУ Томский государственный университет

UAE – ОАЭ Объединенные Арабские Эмираты

UFV – БЛА беспилотный летательный аппарат

USAV – БПЛА беспилотный боевой летательный аппарат

UGV – беспилотный наземный аппарат

UN – ООН Организация Объединенных Наций

US – США

USD – Доллар

USSR – СССР Союз Советских Социалистических Республик (Советский Союз)

UUV – Беспилотный надводный аппарат беспилотный подводный аппарат

Методология и структура

Этот отчет является результатом работы Программы исследований CNA в России за прошедший год по составлению карты и пониманию экосистемы ИИ в России.

Во-первых, команда разработала и внедрила подготовку раз в две недели информационного бюллетеня, освещающего текущие разработки в области технологий, ИИ и автономии в России. В этих информационных бюллетенях также освещались различные инициативы, связанные с военным ИИ, и ключевые организации, занимающиеся ИИ. Они также сыграли решающую роль в составлении карты экосистемы ИИ в России и предоставили ключи к областям, нуждающимся в более глубоких исследованиях. Благодаря этому исследованию мы смогли понять взаимоотношения между различными организациями в государственном, частном и военном секторах. Мы собрали данные из широкого спектра русскоязычных источников, включая юридические документы, официальные заявления, информацию об отраслевой продукции, российские профессиональные военные журналы, материалы конференций

и отдельные публикации. Значение каждого источника варьировалось в разных разделах. Например, правительственный раздел в значительной степени опирался на множество доступных официальных документов, в то время как военный раздел больше полагался на российские новостные сообщения из открытых источников. Исследование должно было сбалансировать необходимость собрать как можно больше информации с признанием того, что многие источники, которые говорят и пишут об ИИ, не обязательно понимают сложную и обширную область, которая подпадает под сферу ИИ и автономии. С этой целью команда CNA работала с Центром автономии и искусственного интеллекта CNA, чтобы лучше понять некоторые технологические значения различных отчетов. Однако обратите внимание, что основное внимание в нашем отчете уделяется не техническому обзору разработок в области ИИ в России.

В первом разделе этого отчета представлен обзор, который поможет читателю понять Россию и различные показатели, по которым аналитики часто оценивают ее. Эта часть отчета уникальна тем, что в ней не рассматривается ИИ или автономия в частности, но мы считаем, что она обеспечивает необходимый контекст, который обогатит обсуждение российских технологических инноваций, ИИ и автономии. В частности, этот раздел будет наиболее полезен читателям, чей основной опыт связан с ИИ и автономией, а не конкретно с Россией.

В последующих разделах описываются усилия, предпринимаемые российским правительством для создания в России атмосферы, способствующей технологическому прогрессу. Он охватывает более широкие усилия по «оцифровке» и помещает ИИ в эти более широкие рамки. Этот раздел служит фоном и контекстом для следующих разделов. Третий раздел посвящен экосистеме ИИ в России, ее ключевым игрокам и взаимодействиям. После этого в четырех разделах рассматривается ИИ, связанный с российским образованием, частным сектором, военным

и международным сотрудничеством, чтобы придать некоторую детализацию нашему обсуждению экосистемы ИИ в России.

РОССИЙСКАЯ ВЛАСТЬ В ПЕРСПЕКТИВЕ

В этом разделе представлен взгляд на потенциал российского государства и российскую власть в международной системе, чтобы обеспечить контекст для российских инвестиций в ИИ и автономные системы.[1]

Хотя мы считаем, что все читатели могут извлечь выгоду, этот раздел будет наиболее полезен читателям, которые обращаются к теме ИИ в России и автономии от ИИ или неспециализированных международных отношений.

Читатели, которые уже обладают глубоким пониманием проблем национальной безопасности России, могут пожелать перейти непосредственно к следующему разделу. Этот фон может помочь определить ожидания относительно того, может ли Россия стать долгосрочным стратегическим соперником.

Может ли он развиваться самостоятельно или поглощать передовые технологии, произведенные другими? Находится ли эта страна в состоянии застоя, упадка или возрождения?

В этом разделе мы делаем акцент на экономических, военных, демографических и технологических аспектах России. В этой главе не ставится цель всесторонне осветить эту тему, поскольку она не является предметом настоящего доклада, но предлагается взглянуть на Россию сквозь призму исторического контекста.

Россию лучше всего представлять как относительно слабую великую державу, причем слабость означает ее положение по отношению к Соединенным Штатам и Китаю, а не абсолютное описание способности государства влиять на мировые дела. В целом, это одно из самых могущественных государств в международной системе и устойчивая держава,

[1] Части этого раздела взяты из или проинформированы Майклом Кофманом и др., Государственный потенциал России в 2030 году, Случайная статья CNA, август 2020 года.

которая исторически бросала вызов вековым тенденциям подъема или упадка. Россия обладает огромной способностью к самовосстановлению, пережив периоды возрождения, застоя, упадка или даже краха государства.[2]

Действительно, она смолаг восстановиться в течение одного поколения после гражданской войны в межвоенный период и после распада СССР в 1991 году. Россия занимала видное место в конфликтах великих держав последних трех столетий, а также в послевоенной борьбе за структурирование международного порядка.

Национальная элита страны рассматривает Россию как наследственную великую державу, имеющую право на статус; с местом за столом принятия решений в крупных международных организациях и в экстерриториальном геополитическом пространстве, где преобладают российские интересы.

Современная Россия не является ни восходящей, ни падающей державой, но лучше всего воспринимается как нация в состоянии застоя. После резкого спада после распада Советского Союза в 1991 году, по наиболее значимым показателям российская мощь и государственный потенциал возродились с 2000 года по 2014 год.

Таким образом, экономическая стагнация является относительно недавним явлением (после 2012 года) из-за структурных экономических проблем, внутриполитической окостенелости и неотложных внешних факторов, таких как мировые цены на энергоносители.

Тем не менее, российская мощь по сравнению с мощью Соединенных Штатов в ближайшей перспективе не ожидается заметного снижения.

Страна обладает значительными экономическими ресурсами, сильным человеческим капиталом, крупными и модернизированными обычными вооруженными силами и находится в союзе только с Соединенными Штатами, когда речь заходит о ее разнообразном ядерном арсенале.

---

[2] Хорошую дискуссию на эту тему можно найти в книге Стивена Коткина «Вечная геополитика России: Путин возвращается к историческому образцу». https://www.foreignaffairs.com/articles/ukraine/2016-04-18/russias-perpetual-geopolitics, Foreign Affairs 95, № 3 (2016).

Более того, полезно разделить различные ресурсы, которыми располагает государство, в качестве мер власти, по сравнению с властью «на практике» и тем, что оно может заставить другие страны делать то, чего они в противном случае не сделали бы.[3]

В этой последней категории Россия демонстрирует хорошие результаты в способности определять результаты в международных делах относительно имеющихся у нее средств.

Россия исторически была обременена отсталой и расточительной политической и экономической системой, то есть страна обладает огромным потенциалом в своих природных и людских ресурсах, но редко способна его реализовать.

Как в экономике, так и в обществе доминирует государство, которое неэффективно, коррумпировано и часто неэффективно в осуществлении стратегического планирования.

Эта непреходящая реальность была обобщена историком Василием Ключевским с комментарием: «государство толстело, но народ худел».[4]

Таким образом, страна часто боролась за достижение устойчивой модели экономического развития, не поддаваясь стагнации или не требуя принудительной мобилизации государства. На протяжении всей истории проблема передачи власти также была сложной в российской политике.[5]

Вооруженные силы

Российские вооруженные силы состоят примерно из 850 000 – 900 000 военнослужащих на действительной службе, состоящих из 400 000 контрактников, около 250 000 призывников и, возможно, 200 000 офицеров. Призывники распределены неравномерно, сосредоточены в сухопутных войсках

---

[3] Роберт А. Даль, «Концепция власти», Поведенческая наука 2, № 3 (1957), https://onlinelibrarywiley.com/doi/10.1002/bs.3830020303.

[4] Коткин, «Вечная геополитика России: Путин возвращается к историческому образцу».

[5] Томас Э. Грэм, «Источники поведения России: Длинная телеграмма Кеннана нуждается в обновлении для путинской России», Национальный интерес, август. 24, 2016, https://nationalinterest.org/feature/the-sources-russian-conduct 17462.

и воздушно-десантных войсках, в то время как контрактники и прапорщики выполняют более сложные задачи и, как ожидается, пополнят батальоны, которые создаются для участия в любом конфликте.

Российская национальная гвардия представляет собой еще одну силу численностью 180 000 человек и существуют военизированные службы безопасности, такие как пограничная служба ФСБ и береговая охрана.

Российские вооруженные силы функционально подразделяются на силы общего назначения, стратегического сдерживания (отдельные обычные и ядерные средства) и силы быстрого реагирования (высокая готовность/мобильность). Российский оборонный бюджет кажется обманчиво маленьким.

Хотя рыночные обменные курсы предполагают, что российский оборонный бюджет составляет 60 миллиардов долларов, на самом деле эта цифра в высшей степени вводит в заблуждение и, очевидно, не может учитывать размеры и масштабы вооруженных сил России.

Организации, которые сравнивают расходы на оборону, такие как ежегодный отчет IISS «Военный баланс», показывают, что российские расходы составляют ничтожные 45 миллиардов долларов, исходя из постоянных рыночных обменных курсов 2010 года, что меньше, чем в Соединенном Королевстве.

Эти утверждения, порождают очевидную проблему финансового баланса и обменного курса.

Вооруженные силы России, включая обычные и ядерные компоненты, значительно больше по размеру, имеют больший потенциал на местах и находятся в более высокой степени готовности, чем вооруженные силы Франции или Соединенного Королевства.[6]

Поскольку материальные, трудовые и различные другие затраты на ввод значительно различаются в разных странах, более подходящее сравнение

[6] Майкл Кофман и Ричард Коннолли, «Почему военные расходы России намного выше, чем принято считать (как и у Китая)», Война на скалах, 16 декабря 2019 г., https://warontherocks.com/2019/12/why-russian.

для автаркических оборонных отраслей, где торговые потоки сильно ограничены геополитической динамикой и национальными правилами, будет использовать скорректированный на импорт паритет покупательной способности (ППС).[7] Действительно, рыночные обменные курсы наиболее полезны для определения стоимости торговли, но плохо учитывают внутреннюю экономическую активность. При использовании таких мер российские военные расходы фактически составляют 150-180 миллиардов долларов США, что составляет примерно 4% российского ВВП.[8] Это консервативная оценка, учитывая, что некоторые расходы классифицированы или потрачены на гражданские организации, участвующие в ядерном предприятии военного назначения.

Хотя широко распространено мнение, что расходы США на оборону превышают расходы России в 10 раз (от 700 до 60 миллиардов долларов)[9], на самом деле это ближе к четверти, если учесть, насколько дешевле эквивалентные военные товары и услуги должны производиться и предоставляться в России при покупке в местной валюте. Гораздо большая доля российского бюджета тратится на закупки личного состава, по сравнению с западными военными. Примерно 50% оборонного бюджета России направляется на Государственную программу вооружения (1,6 трлн рублей в 2020 году). Это составляет примерно треть от общих военных расходов, примерно 55 миллиардов долларов США в пересчете на ППС, и этот показатель стабильно поддерживается в 2016-2020 годах.

Российский оборонный бюджет в значительной степени сократился, но не из-за экономических ограничений.

---

[7] Основное различие в оценках ВВП PPE и ME заключается в том, что рыночные обменные курсы хорошо оценивают размер нефтегазового сектора России, поскольку эти товары, а также активы и услуги, которые их производят, могут в гораздо большей степени – свободно продаваться. Цена на международном рынке сходится к местной цене. Однако в случае оборонных технологий почти все страны сильно ограничивают как импорт, так и экспорт. В результате рыночная биржевая цена не сходится к местной цене, а анализ, основанный на обменном курсе, не учитывает истинную стоимость инвестиций в российскую военную технику и персонал.

[8] Кофман и Коннолли, «Почему военные расходы России намного выше, чем принято считать (как и у Китая)».

[9] Например, см. Последние сравнения расходов на оборону, опубликованные в Международном институте стратегических исследований, «Военный баланс 2021» (Routledge, 2021), https://www.iiss.org/publications/the-military-balance.

Многие заказы на модернизацию и перевооружение были выполнены в 2011-2015 годах, и военно-промышленный комплекс был в целом рекапитализирован с точки зрения оборудования, технической экспертизы и т.д. Различия в паритете покупательной способности полезно учитывать при изучении показателей государственных расходов на разработку ИИ или автономных систем, особенно в тех случаях, когда системы не зависят от импортных технологий, иностранной рабочей силы или компонентов, т. е. затраты на них являются локальными в рублях.[10]

Экономика

Россия часто изображается как 11-я по величине экономика в мире, сопоставимая с Канадой, основанная на рыночных обменных курсах. Однако и здесь паритет покупательской способности (PPP) предлагает совершенно иную картину.

Россия является шестой по величине экономикой в мире и второй по величине в Европе по показателю ВВП по ППС, оцениваемому примерно в 4,3 трлн. долл. в 2019 году.[11] Она находится на пути к тому, чтобы вновь обогнать Германию как крупнейшую экономику в Европе.

Россия позиционируется как страна с высоким средним уровнем дохода, с хорошо образованным и урбанизированным обществом, а доходы на душу населения выше, чем в Китае.

В российской экономике доминирует конкурентоспособный сектор добычи ресурсов и сектор, зависящий от доходов, который состоит в основном из неконкурентоспособных отраслей. Первый экспортирует ресурсы в мировую

[10] Российские оборонные фирмы также постоянно недооцениваются в международных рейтингах. Причина в том, что такие организации, как SIRPI, измеряют их по рыночному обменному курсу, даже несмотря на то, что основным источником дохода компаний являются продажи внутренней обороны. Это, по сути, измеряется так, как если бы российское правительство покупало свой оборонный комплект в долларах, а не в рублях. Такие меры также исключают российских гигантов, таких как «Росатом», которые производят ядерное оружие, и гигантский конгломерат «Ростех» с общими военными доходами в размере 16,9 миллиарда долларов в 2019 году, но фактически 42 миллиарда долларов при рассмотрении мер с поправкой на ППС. Для получения дополнительной информации см. Исследовательский отчет RSI «Анализ оборонной промышленности России», январь 2021 г., № 9.

[11] Здесь корректировки на основе ППС могут преувеличивать экономические показатели, поскольку они плохо отражают экспорт и импорт товаров по ценам международного рынка, и может быть предпочтительнее усреднить эти два показателя вместе для более справедливой оценки.

экономику, в то время как второй потребляет субсидии и продает в основном на внутренний рынок. Последняя не инвестирует в человеческий или основной капитал, поскольку состоит из крайне неконкурентоспособных или защищенных государством фирм.

Следовательно, большая часть государственных доходов поступает от экспорта ресурсов, даже если это представляет собой лишь один сектор более диверсифицированной экономики. Российская экономика страдает от недостаточных инвестиций, ежегодно инвестируется около 20% ВВП, в то время как производство также неконкурентоспособно. Таким образом, доходы от экспорта расходуются на поддержание производства и занятости в отстающих секторах. Поскольку большая часть доходов российского правительства поступает от экспорта нефти и газа (около 40-45 %), справедливо будет назвать Россию нефтегосударством. Экономический цикл России состоит из роста доходов от экспорта ресурсов, за которым следует рост внутреннего потребления и импорта. Российская экономическая стратегия основана на поддержании низкой стоимости рубля для стимулирования экспорта, наращивании валютных резервов, особенно в золоте, и сохранении высокой занятости даже в условиях стагнации роста заработной платы.

Это консервативный экономический подход, при котором вклад государства в рост ВВП или расходы на ускорение экономики невелик. Хотя в стране сохраняется стабильная макроэкономическая картина и низкий государственный долг, уровень жизни снижается, что приводит к общественному недовольству и экономической неопределенности (это является существенным фактором, стоящим за недавними протестами в России).

Инфляция в России относительно низкая по сравнению с предыдущими десятилетиями, но общая стратегия обеспечивает слабый экономический рост при одновременном максимальном смягчении режима в случае серьезных экономических потрясений или новых санкций.

По сути, государство накапливает резервы, когда цены на нефть высоки, а затем тратит некоторую сумму, когда цены на нефть низкие, чтобы избежать потрясений для финансовой системы.

Без структурных реформ Россия не сможет обеспечить рост ВВП на 4% или больше, что было бы необходимо для дальнейшего развития, и поэтому рост относительно застойный – около 1,3% в 2019 году (до пандемии). Этого можно было бы достичь при высоких ценах на нефть, но они цикличны, поэтому в течение десятилетия в России по-прежнему будут наблюдаться относительно низкие темпы роста. Хотя стоит учитывать, что эти темпы роста в среднем выше, чем у некоторых крупных европейских экономик. Поэтому слабые экономические показатели России часто преувеличиваются.

Российская политическая элита не желает проводить структурные реформы в экономике и вместо этого пытается ускорить рост ВВП с помощью инфраструктурных проектов, что оказалось неудачной стратегией.

Однако экономика России устойчива. ВВП России сократился на 3,1% в 2020 году, что оказалось значительно меньше, чем у европейских аналогов, поскольку ожидается, что экономика еврозоны сократится на 7,3%.[12]

Нынешнее мышление в российском политическом управлении заключается в том, что необходимо провести мета-реформы системы управления и практики, прежде чем будут начаты какие-либо значимые реформы.[13]

Этот подход проливает свет на разницу между проектами реформ, направленными на повышение эффективности управления и на предотвращение деградации режима, по сравнению с теми, которые могут глубоко изменить

[12] Анна Андрианова, «В 2020 году Россия переживает меньший экономический спад, чем аналогичные страны», Bloomberg, 1 февраля 2021 года, https://www.bloomberg.com/news/articles/2021-02-01/russia-suffers-smaller-economic-slump-than-peers-in - 2020. 13 Фабиан Буркхардт, «Защита от дураков путинизма», Загадка, 3 марта 2021 года, https://www.ridl.io/en/foolproofing- -putinizm/.

[13] Фабиан Буркхардт, «Защита от дураков путинизма», Загадка, 3 марта 2021 года, https://www.ridl.io/en/foolproofing-putinizm/.

систему и будут встречать сильное сопротивление со стороны других элит или сетей. Россия – это государственная капиталистическая система, в которой значительная часть экономики находится под контролем большинства государственных или контролируемых предприятий, а также более 70% финансовой системы. Это система, изобилующая клановостью, когда люди получают должности и контракты, которые предоставляют им доступ к арендной плате.

Таким образом, большая часть политической и экономической элиты организована как покровительственные сети и характеризуется поведением, направленным на поиск ренты.

Элита подотчетна тем, от чьего покровительства они зависят, а не общественным интересам. В системе есть компетентные учреждения и компетентные менеджеры, такие как Центральный банк или Министерство финансов, но значительная часть экономики де-факто находится в руках элит, чьи возможности получения доходов зависят от доступа в Кремль, а не от конкурентоспособности их предприятий или их компетентности в управлении ими.

Технологические инновации

Российские лидеры часто говорят о важности инноваций и в качестве документов планирования существует множество инновационных стратегий.[14] Однако эта риторика плохо согласуется с инвестициями и определением приоритетов. Расходы России на исследования и разработки составляют примерно 1% ВВП, что отстает от аналогичного показателя стран ОЭСР.[15]

---

[14] «Официальный сайт Президента Российской Федерации», Конференция по искусственному интеллекту. Владимир Путин выступил на пленарном заседании конференции «Путешествие по искусственному интеллекту», посвященной искусственному интеллекту, 9 ноября 2019 года, http://special.kremlin.ru/catalog/keywords/39/events/62003.

[15] «Российская Федерация», Прогноз ОЭСР по науке, технологиям и инновациям на 2016 год, https://read.oecd – ilibrary.org/science-and-technology/oecd-science-technology-and-innovation-outlook-2016/страница (https://dx.doi.org/10.1787/sti_in_outlook-2016-83-en).

Хотя показатели свидетельствуют о неуклонном повышении уровня инноваций и качества научных исследований[16], система образования не соответствует потребностям современной экономики.

Существует нехватка финансирования НИОКР и мало доступного частного капитала, поскольку большая часть финансовой системы находится под контролем государства или находится под прямым контролем. Количество заявок на патенты в России составляет около 30 000 в год, как и в Индии, хотя и довольно мало по сравнению с США (515 180 в 2018 году).[17]

В то же время в России есть несколько успешных технологических компаний, которые занимают доминирующие позиции на рынке страны по сравнению с западными фирмами. Россия – одна из немногих стран, где Google, Facebook и аналогичные американские бренды не владеют контрольными долями в ключевых секторах цифровой экономики. Действительно, Яндекс (российский Google), ВКонтакте (российский Facebook), Антивирус Касперского и аналогичные фирмы сохраняют контрольные доли рынка, несмотря на их ограниченную привлекательность на мировом рынке и неограниченный доступ к Google или Facebook в России. Несмотря на внешний вид экономики добычи ресурсов монокультуры, в информационном секторе России есть яркие пятна высоких технологий. В целом, позиции страны и мировые рейтинги в области технологических инноваций неуклонно улучшались в течение последних 20 лет, но набор навыков рабочей силы и общая структура экономики, в которой доминирует государство, предлагают плохую экосистему по сравнению с развитыми западными экономиками.

Среди российских элит существует постоянный страх того, что страна отстает, возможно, лучше всего об этом заявил в 2016 году глава российского Сбербанка (ныне называемого Sber) Герман Греф, когда он сказал,

---

[16] Россия переместилась в глобальной конкурентоспособности с 67-го места в 2012 году на 43-е место в 2019 году. См. Клаус Шваб, Доклад о глобальной конкурентоспособности за 2019 год, Всемирный экономический форум, 2019 год, http://www3.weforum.org/docs/WEF_TheGlobalCompetitivenessReport2019.pdf.

[17] Центр обработки данных ВОИС, доступ к которому получен 5 мая 2020 г., https://www3.wipo.int/ipstats/index.htm.

что «мы оказались в рядах стран, которые проигрывают, переходят на более низкую ступень». Позиционирование России как более успешной в области технологических инноваций потребует значительных инвестиций и серьезных внутренних реформ, ни то, ни другое не представляется вероятным в ближайшей перспективе.

Демография

Хотя в ближайшие десятилетия Россия столкнется с устойчивым сокращением численности населения, его вероятное влияние на государственную власть и экономический потенциал не является детерминированным. Взаимосвязь между демографией и государственной властью вряд ли линейна, и самое главное – это качество человеческого капитала, а не просто количество. Россия и Советский Союз часто подвергались демографическим предсказаниям конца света, которые неизменно не сбывались.

Средний сценарий, предсказанный демографами ООН, предполагает сокращение численности населения примерно на 7,5% к 2050 году, что означает, что население России сократится со 145 до 135 миллионов человек.[18] Более пессимистичные прогнозы предполагают снижение на 11-12%, но далеко не самые худшие сценарии, которые представлялись в начале 2000-х годов. Ожидается, что в 2050 году Россия по-прежнему будет самой густонаселенной европейской страной с большим отрывом.

Демографическая проблема России вызвана высоким уровнем смертности, особенно среди мужчин, и побочным эффектом низкой рождаемости в 1990-е годы. Рабочая сила значительно сокращалась из года в год, по сути, старея без замены. Однако Россия также является чистым бенефициаром значительной трудовой миграции, которая восполняет дефицит

[18] Департамент ООН по экономическим и социальным вопросам, Отдел народонаселения, Мировые демографические перспективы 2019, по состоянию на 19 апреля 2021 года, https://population.un.org/wpp/Graphs/Probabilistic/POP/TOT.

рабочей силы во многих секторах экономики.[19] Следовательно, сокращение численности населения России частично компенсируется трудовыми мигрантами, на долю которых приходится значительный процент ежегодной миграции.[20] Вопрос «утечки мозгов» является сложным и, хотя есть признаки того, что представители креативного класса эмигрируют из-за плохих возможностей, низкой оплаты труда или политических репрессий, влияние крайне неравномерно.

Россияне также живут намного дольше и здоровее по сравнению с 1990-ми и 2000-ми годами, а уровень рождаемости значительно повысился примерно до уровня США. С 2000 по 2015 год в общих демографических тенденциях России произошли значительные улучшения, даже если некоторые из достижений были обращены вспять в последние годы после экономического спада, санкций и последствий пандемии Covid-19. Население России начало сокращаться лишь на незначительную величину в 2019 году. Что еще более важно, главными трудовыми проблемами России исторически были производительность труда и качество рабочей силы, а не размер рабочей силы. Однако за последние два десятилетия в России наблюдался значительный рост производительности труда, сопоставимый со странами ЕС, и это одна из областей устойчивого улучшения, несмотря на сокращение рабочей силы.[21] Страна сталкивается с давлением сложной демографической проблемы, но она не собирается испытывать нехватку людей или «умственных способностей», хотя отстающая система образования и утечка талантов в некоторых секторах создают постоянную проблему.

Потенциал в развитии ИИ

[19] Татьяна Карабчук, «Экономические последствия миграции в Российской Федерации: налогообложение трудящихся-мигрантов», Азиатско-Тихоокеанский журнал по народонаселению 32, № 2 (2018), https://www.researchgate.net//Publication/329243042.

[20] Мария Липман и Юлия Флоринскава, «Трудовая миграция в России», ПОНАРС Евразия, январь 2019 г., https://www.ponarseurasia.org/labor-migration-in-russia.

[21] ОЭСР (2020), Производительность труда и его использование (показатель), doi: 10.1787/02c02f63-en (Дата обращения 31 июля 2020 г.), https://data.oecd.org/lprdty/labour-productivity-and-utilisation.htm#indicator-chart.

По мере того, как западные наблюдатели наблюдают за российским ландшафтом ИИ, важно применять взвешенный подход и противостоять прогнозам, которые предсказывают неизбежную гибель России и ее незначительность в глобальном стремлении к технологиям ИИ, а также тем опасениям, что Россия каким-то образом собирается выйти с новой технологией с поддержкой ИИ, которая дает ей решающее преимущество перед Соединенными Штатами.

Российский технологический ландшафт и инфраструктура не располагают возможностями для создания прорывов, связанных с ИИ. Тем не менее, он в состоянии внимательно следить за глобальными достижениями в области ИИ и извлекать из них выгоду.

Ситуация аналогична развитию Интернета и последующему потенциалу кибервойны.

Россия не была крупным игроком в фундаментальных исследованиях, которые позволили создать Интернет, однако недавние события показали, что она является лидером в вооружении Интернета. Как и в случае с ИИ, Россия не является лидером в исследованиях ИИ, но у нее, безусловно, есть потенциал стать мировым лидером в области ИИ-вооружения.[22] Интервью с профессором российского происхождения Сергеем Левиным, доцентом Калифорнийского университета в Беркли, и Крейгом Смитом из подкаста «Взгляд на ИИ», возможно, отражает эту динамику между тем, что Россия является лидером технологических прорывов и извлекает выгоду из самих прорывов.[23]

КРЕЙГ: Насколько мы знаем, что происходит в Китае или России, если на то пошло, и насколько они знают, что происходит здесь.

У вас есть мнение на этот счет?

СЕРГЕЙ: Это хороший вопрос. Я думаю, что, с моей точки зрения, я был бы очень удивлен, если бы произошел крупный прорыв в лаборатории,

---

[22] Аналогия, заимствованная у Грегори Аллена, начальника отдела стратегии и коммуникаций в Объединенном центре искусственного интеллекта Министерства обороны, https://www.ai.mil.

[23] Крейг Смит, «ЭПИЗОД № 014: Размышления о роботах II», подкаст «Взгляд на ИИ», https://www.eye-on.ai/podcast.

которая не принимает активного участия в научном сообществе в этой конкретной области.

Среди ученых существует тенденция, когда они публикуют результат, подчеркивать то, что является новым, особенно то, что радикально связано с этим результатом, но на самом деле каждый результат основывается на предыдущей работе.

На самом деле, это обычно очень, очень тесно связано с предыдущей работой.

Таким образом, более реалистичный взгляд на научный результат заключается в том, что он точно такой же, как и то, что кто-то делал раньше, с небольшими изменениями. В принципе, каждый крупный результат таков, от самых известных ученых в истории до сегодняшнего дня, и по этой причине я не думаю, что кто-то будет застигнут врасплох, по крайней мере, среди людей, которые действительно работают в этой области, чем-то вроде результата десятилетий секретных исследований.

Я думаю, что все идеи витают в воздухе, и хотя в целом могут быть небольшие местные вещи, которые люди могут придумать в тайне, не похоже, что где-то будет разрыв в год. Я просто не вижу, как это проявляется.

КРЕЙГ: И у вас есть мнение об этой конкуренции, о которой люди начинают беспокоиться, особенно между Китаем и США, но также и Россией. Я имею в виду, что вы читаете по-русски. Есть ли статьи, которые вы читаете на русском языке, которые не опубликованы на английском?

СЕРГЕЙ: Нет. Лучшие статьи из России сейчас написаны на английском языке. И я думаю, что это относится и к документам из Китая.

КРЕЙГ: Это верно, да. Итак, если только не будет масштабно финансируемого, что возможно в Китае, Манхэттенского проекта для достижения какой-то цели, мы знаем, что происходит в Китае, по крайней мере, на уровне фундаментальных исследований.

СЕРГЕЙ: Я думаю, что да. И я думаю, что массово финансируемый Манхэттенский проект, я имею в виду, я могу показаться наивным в этом

отношении, потому что я, конечно, не эксперт в области политологии или экономики, но я бы сказал, что усилия в стиле Манхэттенского проекта для ИИ были бы крайне неэффективными, потому что было бы трудно найти лучших людей и удержать лучших людей. И без лучших людей было бы очень трудно добиться существенного прогресса, который на самом деле опережает то, что делают люди, работающие на открытом воздухе.

Заключение

Россия сохраняет сильные стороны в области жесткой силы, экономической и военной, с заметным дефицитом технологических инноваций и нехваткой мягкой силы.

Экономика устойчива, как и политическая система, но находится на траектории стагнации, которая со временем может перейти в упадок, особенно в относительном выражении.

Без политических и экономических реформ страна не сможет обеспечить рост, необходимый для дальнейшего развития, а привычки к хроническому недоинвестированию негативно сказываются на ее экономических показателях.

В то время как Россия вряд ли станет свидетелем какого-либо резкого спада в ближайшей или среднесрочной перспективе, политическая окостенелость на самом верху и отсутствие экономических реформ обеспечивают вялый экономический рост с чрезмерной зависимостью от мировых цен на энергоносители.

Но в то же время Россия обладает мощной ресурсной базой, состоящей из крупной экономики, хорошо образованного населения, качество которого продолжает улучшаться, и технологических достижений в коммерческих секторах.

Государство может расставлять приоритеты и мобилизовывать свои ресурсы, когда политическое руководство хочет, чтобы что-то было сделано, фактически принуждая систему к достижению результатов. Это может иногда компенсировать плохую реализацию стратегического планирования.

Россия также накопила значительные финансовые резервы, несмотря на санкции, и во время пандемии COVID-19 дела у нее шли лучше, чем у некоторых других крупных экономик. Россия медленно втягивается в экономическую орбиту Китая, как из-за отсутствия альтернатив, так и из-за сознательной стратегии создания большей взаимозависимости с растущим экономическим гигантом. Сближение и последующее партнерство с Китаем составляют важный вектор российской внешней политики и, возможно, наиболее последовательный с 1989 года.[24] Хотя Россия находится в несколько невыгодном положении из-за относительной простоты и меньших размеров своей экономики, между двумя странами фактически заключен пакт о ненападении и множество соглашений о техническом сотрудничестве. Сотрудничество в области обороны между двумя странами продолжает расширяться, наряду с обменом технологиями, в отношениях, последствия которых продолжают расти для стратегии США.

Управление и правовые аспекты ИИ в России

В последние несколько лет российское правительство уделяло приоритетное внимание разработке руководящих документов и реформе своей юридической отрасли, чтобы добиться успеха в быстро развивающейся области ИИ. С помощью программ национального уровня, таких как федеральный проект ИИ, и новых законов, таких как нормативные песочницы, действующие в настоящее время по всей стране, Россия стремится предоставить россиянам, развивающимся в этой важной растущей отрасли, ресурсы, рычаги и юридическую возможность экспериментировать и учиться без многих традиционных и бюрократических препятствий.

Эти планы развития не обошлись без критики, поскольку недоверие к ИИ среди простых россиян возросло, а опасения по поводу этики, нарушений конфиденциальности, безопасности и юридических аспектов ИИ остаются.

[24] Подкаст «Взгляд на ИИ», https://www.eye-on.ai/podcast.

Однако COVID-19 еще больше выявил необходимость усиления цифровизации во всем обществе и побудил российское правительство уделять этому вопросу повышенное внимание, даже несмотря на то, что существующие проблемы и трудности, вызванные пандемией, угрожают задержать или затруднить усилия по развитию ИИ на неопределенный срок.

Документы и программы национального уровня

Правительство России подготовило свое первое предложение по ИИ после конференции «Искусственный интеллект: проблемы и решения – 2018», организованный Министерством обороны Российской Федерации (МО) совместно с Министерством науки и высшего образования Российской Федерации и Российской Академией наук в марте 2018 года.[25]

Участники конференции подготовили 10 рекомендаций по продвижению ИИ в России, включая проведение ежегодной конференции по ИИ, развитие инфраструктуры ИИ, создание системы подготовки специалистов по ИИ и формирование консорциума по большим данным и ИИ для объединения усилий правительства в области этих технологий.[26]

В рекомендациях основное внимание уделялось действиям правительства и не упоминалось о частных образованиях.[27]

Два месяца спустя, 7 мая 2018 года, президент России Владимир Путин издал указ о национальных целях развития России до 2024 года, в котором, среди прочего, подчеркивалась необходимость цифровой трансформации российской экономики.[28]

В указе изложены цели и задачи в этой области, включая разработку гибкой системы регулирования для цифровой экономики, в том числе в ИИ.[29]

---

[25] Министерство обороны Российской Федерации, Конференция «Искусственный интеллект: проблемы и пути их решения – 2018», http://mil.ru/conferences/is-intellekt.hm.
[26] Там же.
[27] Там же.
[28] Президент России подписал Указ «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года», (7 мая 2018 года), http://kremlin.ru/events/president/news/57425.
[29] Там же.

Документы/ Программы	Дата	Описание
Дорожная карта ИИ	Декабрь 2018	Предназначена для увеличения внутренних расходов на цифровизацию экономики по семи приоритетным программным направлениям
Программы цифровой экономики ИИ	Октябрь 2019	Описывают соответствующие вспомогательные технологии ИИ и описывают финансирование, необходимое для разработки каждой
Национальная стратегия развития ИИ	Октябрь 2019	Служит основой для планирования и реализации государственных программ ИИ до 2030 года
Федеральный проект ИИ	Август 2020	Добавляет показатели финансирования и эффективности к целям национальной стратегии; устанавливает график разработки и внедрения технологий искусственного интеллекта

Таблица 1. Документы и программы национального уровня

Программа цифровой экономики

В соответствии с майским указом 2018 года Правительство России разработало 13 национальных программ, соответствующих целям Путина.[30]

Одной из этих национальных программ, утвержденной в декабре 2018 года, была программа «Цифровая экономика», которая направлена на увеличение внутренних расходов на цифровизацию экономики.[31]

Программа «Цифровая экономика» включает шесть оригинальных программных областей: информационная инфраструктура, информационная безопасность, цифровизация государственных услуг, сквозные цифровые технологии, человеческий капитал и адаптация нормативной среды.[32]

[30] «Национальные проекты 2019-2024», Российская газета, https://rg.ru/sujet/6234.
[31] Опубликован паспорт национальной программы «Цифровая экономика Российской Федерации», Правительство России, 11 февраля 2019 г., http://government.ru/info/35568.
[32] Экономика данных Россия 2024, Дорожная карта цифровой экономики, Схема движения к цифровой экономике, https://data-economy.ru/dataeconomymap.

В 2020 году правительство добавило седьмую программную область ИИ.

В первоначальной дорожной карте программы «Цифровая экономика», опубликованной в декабре 2018 года, правительство указало, что оно увеличит внутренние расходы на развитие цифровой экономики (из всех источников, а не только из федерального бюджета) с 1,9% ВВП в 2018 году до 5,1% ВВП в 2024 году.[33]

В сентябре 2020 года «Коммерсант» сообщил, что правительство планирует увеличить бюджет программы «Цифровая экономика» с первоначальных 1,6 трлн рублей до почти 2 трлн рублей, уделяя особое внимание проектам в области цифровых технологий (включая большие данные и интернет вещей) и сокращению бюджета на проекты в области информационной безопасности.[34]

Дорожная карта ИИ

В рамках раздела цифровых технологий программы «Цифровая экономика» Правительство России поручило Sber, пытающемуся превратиться в технологическую компанию, с разработкой дорожной карты по развитию ИИ и нейротехнологий.[35] Дорожная карта, опубликованная в октябре 2019 года, описывает соответствующие субтехнологии ИИ, включая обработку естественного языка, распознавание речи и компьютерное зрение, и определяет долю финансирования, необходимую из бюджета и внебюджетных источников для развития каждой из них.[36]

---

[33] «Паспорт национальной программы «Цифровая экономика Российской Федерации», Правительство России, 24 декабря 2018 г., http://static.government.ru/media/files/urKHm0gTPPnzJlaKw3M5cNLo6gczMkPF.pdf.

[34] Никита Королев, «Цифровая экономика» будет расширяться за счет бюджета», Коммерсант, 16 сентября 2020 г., https://www.kommersant.ru/doc/4492928.

[35] Сбербанк недавно исключил слово «банк» из своего логотипа и за последний год инвестировал в технологии, начиная от облачных сервисов и заканчивая автоматизированными транспортными средствами и высокотехнологичными гаджетами. Компания заявляет, что становится «цифровой экосистемой», что означает, что она стремится играть определенную роль во всех аспектах жизни людей, а также в большом количестве корпоративных услуг. Некоторые примеры услуг, которые он предлагает с этой целью, включают онлайн-покупку продуктов, возможность отправлять деньги в цифровом виде за товары и/или услуги, цифровые медицинские услуги, варианты покупки и продажи транспортных средств и т.д. Игорь Королев, «Сбербанк объяснил государству, как потратить 120 миллиардов на искусственный интеллект» «С-Новости, 18 декабря 2019 г., https://www.cnews.ru/news/top/2019-12-11_sberbank_obyasnil_gosudarstvu.

[36] М.Е. Мазуров «Дорожная карта развития сквозных цифровых технологий» Нейротехнологии и искусственный интеллект», (2019), https://digital.gov.ru/ru/documents/6658.

В документе говорится, что для развития в этой области до 2024 года необходимо в общей сложности 392 миллиарда рублей, хотя из бюджета поступит только 57 миллиардов рублей, что в три раза больше, чем указано в первом проекте документа.[37]

Национальная стратегия по развитию ИИ

27 февраля 2019 года Путин поручил Правительству создать национальную стратегию по ИИ, отдельную от дорожной карты.[38]

Цель документа, также подготовленного Sber и утвержденного в октябре 2019 года, состоит в том, чтобы служить основой для планирования и реализации государственных программ, связанных с ИИ, до 2030 года.[39]

Национальная стратегия не содержит подробных сведений о финансировании этих программ и должна рассматриваться как центральный документ планирования. Однако в нем содержится первое определение «искусственного интеллекта», встречающееся в российском законодательстве.[40]

Искусственный интеллект – это комплекс технологических решений, который позволяет имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее определенного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые, по крайней мере, с результатами интеллектуальной деятельности человека. Комплекс технологических решений включает в себя информационно-коммуникационную инфраструктуру (включая информационные системы, информационно-телекоммуникационные сети, другие технические средства обработки информации), процессы и услуги по обработке данных и поиску решений.[41]

---

[37] Игорь Королев, «Российский искусственный интеллект стал мудрее». Сейчас на это нужно 392 миллиарда. C-Новости, 28 октября 2019 года, ttps://www.cnews.ru/news/top/2019-10-28_rossijskij_iskusstvennyj.
[38] Советник, «Национальная стратегия развития искусственного интеллекта», https://www.tadviser.ru.
[39] Там же.
[40] Маргарита Сазонова «Искусственный интеллект и закон: есть ли контракт?», Garant.ru, Гарант., 16 июля 2020 г., https://www.garant.ru/news/1401154.
[41] Tadviser, «Национальная стратегия развития искусственного интеллекта».

Федеральный проект ИИ

Для достижения целей, изложенных в национальной стратегии, Кремль затем распорядился о разработке федерального проекта ИИ, который должен стать седьмым аспектом программы «Цифровая экономика».[42]

В очередной раз Sber подготовил проект документа, который правительство одобрило в августе 2020 года.[43] Федеральный проект добавляет показатели финансирования и эффективности к целям, перечисленным в документе национальной стратегии и устанавливает график разработки и внедрения технологий ИИ.[44]

В пояснительной записке к проекту говорится, что финансирование составит около 36 миллиардов рублей, при этом 22,5 миллиарда рублей будут привлечены из программы «Цифровая экономика» – значительное сокращение по сравнению с первоначально предложенными 128,4 миллиардами рублей.[45]

Однако в декабре 2020 года вице-премьер России Дмитрий Чернышенко – куратор федерального проекта ИИ, сообщил Путину, что финансирование проекта фактически составит 86,5 миллиарда рублей, из которых 24,6 миллиарда рублей поступит из федерального бюджета, а 55 миллиардов рублей предоставит сам Sber.[46] Даже эта увеличенная цифра немного ниже суммы (392 миллиарда рублей), которую Sber первоначально предлагал в качестве необходимой для развития ИИ в своей первой дорожной карте, опубликованной в октябре 2019 года.[47]

Правовая реформа для содействия развитию ИИ

Для достижения своих высоких целей в области ИИ Россия приступила к осуществлению ряда правовых реформ, направленных на стимулирование

[42] «Сбербанк объяснил государству, как потратить 120 миллиардов на искусственный интеллект».
[43] Владислав Скобелев и Анна Балашова «Государственный проект «Искусственный интеллект» обойдется почти в 37 миллиардов рублей», РБК, 28 августа 2020 года, https://www.rbc.ru/technology_and_media/28/08/2020.
[44] Tadviser, «Пояснительная записка к предложению инициировать новый федеральный проект национальной программы «Цифровая экономика Российской Федерации» № D7-2020/001», https://www.tadviser.ru/images/; Альманах искусственного интеллекта, № 6, (2020), стр.44, https://aireport.ru.
[45] «Национальная стратегия развития искусственного интеллекта».
[46] ТАСС ТАСС, «Финансирование федерального проекта ИИ составит 86,5 млрд рублей», 9 декабря 2020 года, https://tass.ru/ekonomika/10214415.
[47] «Российский искусственный интеллект поумнел. Сейчас на это нужно 392 миллиарда».

инноваций и создание условий для экспериментов путем ослабления некоторых предыдущих нормативных актов.

В этом разделе будут рассмотрены основные отраслевые законы и концепции регулирования развития ИИ, хотя правительство также приняло ряд положений, направленных на содействие инновациям в конкретных секторах. Например, в ноябре 2020 года премьер-министр России Михаил Мишустин подписал закон «Дорожная карта» под названием «Новые виды предпринимательства, основанные на внедрении передовых технологий», в которой содержались положения, позволяющие Правительству России завершить тщательный анализ отечественного производства беспилотных летательных аппаратов.[48]

Аналогичным образом, Мишустин утвердил указ в декабре 2020 года, который дал инструкции по участию в эксперименте, связанном с автономными кораблями.[49]

«Регуляторная песочница»

1 июля 2020 года вступил в силу российский закон № 123-ФЗ, экспериментальный правовой режим (или «регуляторная песочница») для города Москвы[50] Закон направлен на содействие инновациям в течение следующих пяти лет, позволяя разрабатывать и тестировать определенные типы технологий ИИ, даже если это противоречит действующему законодательству.[51]

В нем также содержатся определения «искусственного интеллекта» и «технологий искусственного интеллекта», которые могут оказаться полезными при разработке будущих нормативных актов.[52]

---

[48] Распоряжение Правительства Российской Федерации от 5 ноября, 5 ноября 2020 г., № 2871-р http://static.government.ru media/files/ PmWKZG0Bw67e1 dKjzuQIhsgjoyy6NlYW.pdf.

[49] «Правительство официально запустило эксперимент по использованию беспилотных судов в России», Глонасс, 14 декабря 2020 года, http://vestnik-glonass.ru/news/vo_vlasti/pravitelstvo-ofitsialno-dalo-start-eksperimentu.

[50] «Искусственный интеллект и закон».

[51] «Федеральный закон Российской Федерации от 24 апреля 2020 г. № 123-ФЗ», апрель. 24, 2020, https://cis - legislation.com/document.fwx?rgn=124089. «Вероника Фридман и Анна Ботвинкина, «Новая экспериментальная правовая база в России показывает опасности и перспективы будущего регулирования ИИ», Gowling WLG, 14 сентября 2020 г., https://gowlingwlg.com/en/insights-resources/articles/2020/future-ai-regulation-in-russia.

[52] «Новая экспериментальная правовая база в России показывает опасности и перспективы будущего

Важно отметить, что 123-ФЗ также содержит поправку к закону «О персональных данных», принятую в 2006 году, которая позволяет обрабатывать анонимизированные персональные данные о здоровье граждан.

Предыдущая редакция закона «О персональных данных» требовала письменного согласия физического лица, прежде чем его или ее биометрические данные могли быть обработаны.[53]

Авторы законопроекта заявили, что это изменение в законе было необходимо, поскольку разработка и тестирование новых технологий требуют больших объемов данных, а требование согласия для каждого фрагмента ограничит эффективное развитие технологий ИИ.[54]

Затем Правительство России решило распространить эксперимент на всю страну, и 31 июля 2020 года оно приняло закон об экспериментальном правовом режиме на всей территории России.[55]

Федеральный закон № 258-ФЗ вступил в силу в январе 2021 года. Подобно московскому закону, он также направлен на содействие развитию цифровых технологий, однако он распространяется не только на технологии ИИ и имеет более короткий срок действия – всего три года с возможностью продления.[56] Для участия в экспериментальном режиме индивидуальным предпринимателям или организациям необходимо будет подать заявку, после чего сначала Министерство экономического развития, а затем соответствующее отраслевое министерство рассмотрят заявку и решат, дадут ли они одобрение.[57]

В июле 2020 года Министерство экономического развития и торговли выбрало первые проекты к которым будут применяться регулирующие песочницы, в том числе создание роботизированных отелей, грузоперевозки,

---

регулирования ИИ».

[53] Юлия Степанова «Персональные данные будут переданы», Коммерсантъ, 26 июня 2020 года, https://www.kommersant.ru/doc/4391725.

[54] Маргарита Грошева «Разработчикам ИИ будет разрешено использовать данные пациентов без их согласия» Медицинский вестник, 17 июля 2020 года, https://medvestnik.ru/content/news/.html.

[55] «Федеральный закон об экспериментальном правовом режиме в области цифровых инноваций в Российской Федерации», 22 июля 2020 г., http://www.consultant.ru/document/cons_doc_LAW_358738/.

[56] «Новая экспериментальная правовая база в России показывает опасности и перспективы будущего регулирования ИИ».

[57] «Как будет работать закон о «цифровых песочницах» – заместитель Министра экономического развития», D-Russia.ru, 11 августа 2020 года, https://d-russia.ru/kak-budet-rabotat-zakon-o-cifrovyh-pesochnicah-zamministra-jekonomicheskogo-razvitija.

предоставляемые дронами, и коммерческое использование самоуправляемых автомобилей.[58]

В конце октября 2020 года Правительство России утвердило постановление о технологиях, которые будут подпадать под особый правовой режим, включая ИИ, квантовые технологии, технологии для работы с большими данными и робототехнику.[59]

Концепция развития регулирования ИИ

19 августа 2020 года Россия сделала дополнительный шаг к реформированию своей правовой системы для содействия развитию ИИ с принятием «Концепции развития регулирования отношений в области ИИ и робототехнических технологий до 2024 года».[60]

Этот документ, разработанный в соответствии с Национальной стратегией развития ИИ, принятой в октябре 2019 года, определяет основные средства, с помощью которых Россия может преобразовать свою систему регулирования для обеспечения эффективное и результативное развитие ИИ и роботизированных технологий.[61]

Он состоит из пяти частей: общие положения, такие как цели концепции и регулирования; общепромышленные вопросы, такие как юридическая ответственность и условия экспорта; отраслевые области, которые могли бы улучшиться с помощью этих технологий, такие как медицина и транспорт; меры регулирования для финансового стимулирования технологического развития, включая государственно-частное партнерство; методы реализации концепции.[62]

Ключевые организации и частные лица

---

[58] «Экспериментальное правовое регулирование цифровых инноваций в России», Tadviser, https://www.tadviser.ru.
[59] Там же.
[60] «Подробнее о видении правительства по регулированию отношений с ИИ», D-Russia.ru, 27 августа 2020 года, https://d–russia.ru/podrobnee-o-pravitelstvennoj-koncepcii-regulirovanija-otnoshenij-voznikajushhih-v-svjazi-s-ii.html.».
[61] Там же.
[62] Там же.

В то время как правительство несет основную ответственность за принятие политики и законодательства, связанных с ИИ, задача реализации стратегии развития ИИ в России, как правило, ложится на государственные предприятия, а не на частные организации.[63]

В правительстве вице-премьер Дмитрий Чернышенко отвечает за разработку, реализацию и надзор за программой «Цифровая экономика», в то время как Министерству экономического развития поручено осуществлять программу «Песочницы регулирования».[64]

Министерство связи и массовых коммуникаций возглавляет ряд инициатив, связанных с данными и Интернетом.[65]

Правительство поручило компании Sber, возглавляемой Германом Грефом, давним союзником Путина, разработать все основные национальные документы, связанные с ИИ, включая первую дорожную карту ИИ, национальную стратегию развития ИИ и федеральный проект ИИ.[66]

Sber попытался превратиться из банка в более широкую цифровую экосистему, которая будет проникать в жизнь людей с помощью своих интеллектуальных устройств и сервисов.

Однако в декабре 2020 года Путин предупредил Грефа, чтобы он помнил, что Sber – это прежде всего банк.[67] Также в декабре Sber объявил, что скоро откроет первый Институт ИИ в России с миссией продвижения исследований в области ИИ.[68]

---

[63] Стефани Петрелла, Крис Миллер и Бенджамин Купер, «Стратегия искусственного интеллекта России: Роль государственных фирм», Институт исследований внешней политики, 2020, стр. 75, doi: 10.1016/j.orbis.2020.11.005.

[64] «Распределение обязанностей между заместителями премьер-министра», Правительство России, http://government.ru/gov/responsibilities/366; «Экспериментальные правовые режимы цифровых инноваций в России».

[65] «Национальная программа Российской Федерации «Цифровая экономика», Tadviser, https://www.tadviser.ru.

[66] Крис Миллер, Стефани Патрелла и Майя Отарашвили, российская «Программа цифровой экономики» и повестка Кремля в области информационной безопасности, Институт исследований внешней политики, 2020, стр.6.

[67] «Цифровая экосистема Sber», Цифровая экосистема Сбера, Сбербанк, https://www.sberbank.com/ru/eco; Евгений Калюков и Михаил Котляр, Путин указал Грефу на необходимость помнить банковскую сущность Трезвости.

[68] Екатерина Кинякина, «Сбербанк заработает 450 миллиардов рублей на искусственном интеллекте», Ведомости, февраль. 20, 2020, https://www.vedomosti.ru/technology/articles/2020/02/19/823464-sberbank-zarabotaet.

Организация выделила значительную часть собственных средств на реализацию правительственных проектов в области ИИ в течение следующих нескольких лет, хотя Sber также намерен заработать много денег на разработке ИИ.[69]

Несколько других государственных компаний играют определенную роль в реализации более широкой программы «Цифровая экономика».

Правительство поручило Ростеху, крупной военно-промышленной организации, поддерживаемой государством, разработать дорожные карты для технологии блокчейна и распределенной бухгалтерской книги, интернета вещей и телекоммуникаций 5G (наряду с Ростелекомом, крупнейшими цифровыми сервисами России и провайдерами).

Росатом, государственная корпорация по атомной энергии, также активно участвует в цифровой экономике, отвечая в первую очередь за развитие квантовых вычислений.[70]

27 августа 2020 года Ростех и Росатом совместно подписали соглашение о намерениях с правительством России по реализации федерального проекта «Цифровые технологии».[71]

Ряд дополнительных финансируемых государством организаций, таких как «Сколково», также играют более второстепенную роль в цифровой модернизации России.

«Сколково»

Тогдашний президент Дмитрий Медведев запустил «Сколково» в 2010 году с намерением создать инновационный кластер, эквивалентный Силиконовой долине в Соединенных Штатах.

Сколково включает в себя пять исследовательских кластеров: Информационные технологии (ИТ), Энергетика, Ядерная промышленность,

---

[69] Там же.
[70] «Деньги за цифру».
[71] Вика Рябова, «Правительство, Росатом и Ростех подписали соглашение о разработке новых технологий цифрового производства», D-Russia.ru, 31 августа 2020 года, https://d-russia.ru/pravitelstvo-rosatom-i-rosteh-podpisali-soglashenie-o-razvitii-novyh-cifrovyh-proizvodstvennyh-tehnologij.html.

Биомедицина и Космос. Развитие технологий ИИ является одним из основных направлений деятельности ИТ-кластера.

Российские государственные учреждения, которые сами не участвуют в цифровой модернизации России, также все чаще объявляют об инициативах по использованию ИИ в рамках своих обязанностей.

В декабре 2020 года Министерство цифрового развития России опубликовало список проектов ИИ, которые оно предложило реализовать в четырех российских министерствах и трех правительственных ведомствах к 2024 году.

Проекты включают использование ИИ Министерством внутренних дел, анализ изображений ИИ Министерством по чрезвычайным ситуациям для выявления стихийных бедствий и управления ими, а также создание чат-бота на основе нейронных сетей для оказания помощи Министерству промышленности и торговли.[72]

Правительство будет финансировать эти усилия агентства по цифровизации, каждый из которых может стоить десятки миллиардов рублей.[73]

Учитывая, что импульс для этих усилий исходит от высшего российского руководства, инициативы агентства, вероятно, заслуживают доверия, хотя неясно, насколько равномерно министерства смогут реализовать свои проекты или насколько успешными будут попытки.

Вполне вероятно, что будут разные уровни успеха, поскольку каждое министерство пытается реализовать свои собственные инициативы. Мы ожидаем увидеть разные скорости в выполнении усилий и, в то время как некоторые будут выполнять все свои цели, другие не смогут реализовать все планы должным образом. Кроме того, неясно, какие министерства располагают достаточным количеством персонала и экспертов, способных реализовать планы, связанные с ИИ.

---

[72] Там же.
[73] Там же.

Несмотря на усилия России по обучению как можно большего числа людей возможностям ИИ, вполне вероятно, что некоторые государственные учреждения будут обладать большим ноу-хау для осуществления своих планов, чем другие.

Когда министерства получают доступ к огромным государственным средствам, мы также можем ожидать появления определенного количества труб для печей, а также поиска арендной платы и оборонительного отношения к своим конкурентам (т.е. другим государственным учреждениям). Чтобы оправдать свои расходы и показать руководителям правительства, что они выполняют свои задачи, некоторые министерства могут в определенной степени искажать свои усилия (вероятно, заявляя, что они делают больше, чем на самом деле), чтобы получить дополнительные средства из бюджета.

Критика усилий по развитию ИИ

Российские усилия по цифровизации и планы по развитию индустрии ИИ не обошлись без противодействия, в том числе со стороны простых российских граждан.

В ходе опроса в июле 2020 года 20% российских респондентов сообщили о негативном отношении к ИИ, сославшись на опасения утечки информации, нарушения конфиденциальности, технических сбоев и непредсказуемости развития ИИ.[74]

Это число увеличилось по сравнению всего с 12%, которые сообщили о негативном отношении в январе 2020 года, вероятно, из-за более широкого использования ИИ в результате пандемии.[75]

Некоторые планы правительства по цифровизации вызвали особую критику. Поправка к закону «О персональных данных», содержащаяся в Федеральном законе 123-ФЗ, которая позволила использовать анонимизированные медицинские данные физического лица без их согласия,

[74] «Опрос: Россияне стали меньше доверять искусственному интеллекту из-за пандемии», Фингазета, 23 июля 2020 г., https://fingazeta.ru/events/meropriyatiya/464641.
[75] Там же.

вызвала серьезную озабоченность по поводу того, что это может означать для прав на данные и защиты конфиденциальности.[76]

Многочисленные эксперты говорили о возможности злоупотреблений, которые могут возникнуть, когда люди теряют контроль над своими данными, и о невозможности восстановления целостности биометрических данных в случае утечки.[77]

Много информации о россиянах, включая записи их звонков, местоположение мобильных телефонов, и записи о авиаперелетах уже доступны нелегально для покупки по чрезвычайно низким ценам в приложении Telegram или в темной сети, но предлагаемые правила позволят использовать определенные типы информации, например, анонимизированные медицинские данные, законные в некоторых сценариях.[78]

Были высказаны дополнительные опасения по поводу нормативных «песочниц», учитывая возможность киберугроз в некоторых случаях, и эксперты настоятельно призвали уделять особое внимание безопасности данных при проведении экспериментов по использованию цифровых технологий.[79]

Развитие ИИ также вызывает нерешенные юридические и этические проблемы. Правовой статус созданных ИИ творений остается неоднозначным, как и юридическая ответственность в случае аварии с участием беспилотного транспортного средства.[80]

Что касается прав интеллектуальной собственности (ИС), по крайней мере, в октябре 2020 года было предложено предоставить права интеллектуальной собственности на созданные ИИ творения разработчикам ИИ

---

[76] «Персональные данные будут переданы».
[77] Там же.
[78] Бен Смит, «Как журналистские расследования процветали во враждебной России», «Нью-Йорк Таймс», 21 февраля 2021 года, https://www.NY times.com/2021/02/21/business/media/probiv-investigative-reporting-russia. html.
[79] Юлия Степанова, «Песочницы с зыбучими песками», Коммерсант, 20 августа 2020 г., https://www.kommersant.ru/ doc/4459389?query.
[80] «Искусственный интеллект и закон».

(а не самому ИИ, как в настоящее время закреплено в российском законодательстве), хотя закон был встречен неоднозначной реакцией.[81]

Граждане также обеспокоены возможностью того, что ИИ займет рабочие места и заменит работников, особенно на низкоквалифицированных должностях.

В недавнем опросе трех тысяч российских граждан со всей России каждый третий участник опасался, что ИИ в конечном итоге будет конкурировать за их рабочие места.

Дискуссия об этике использования ИИ в рабочей силе граждане могут получить больше информации о развитии ИИ, серии лекций по ИИ и индексе доверия ИИ.[82]

Программа нацелена на охват в общей сложности 33 миллионов человек к 2024 году.

Заглядывая в будущее

Экономический кризис, вызванный COVID-19, оказался существенным препятствием для реализации национальных программ России, в том числе в рамках программы «Цифровая экономика», хотя серьезные проблемы существовали еще до начала пандемии.[83]

В то время как российское правительство ставит перед собой высокие цели по цифровизации экономики и развитию технологий ИИ, реалии экономической ситуации потребовали корректировки планов реализации.

В конце 2019 года программа «Цифровая экономика» имела худшее исполнение бюджета из всех национальных проектов – было потрачено всего 53,6 % бюджета.[84] В статьях высказывалось предположение, что это связано

[81] «Российские власти хотят отобрать авторские права у искусственного интеллекта», C-News, ноябрь. 10, 2020, https://www.cnews.ru/news/top/2020-11-11vlasti_zadumali_otobrat.
[82] «Российские власти хотят отобрать авторские права у искусственного интеллекта».
[83] Там же.
[84] «Национальная программа Российской Федерации «Цифровая экономика».

с рядом причин, включая проблемы управления и отсутствие целостной концепции реализации программы.[85]

За первые девять месяцев 2020 года исполнение бюджета составило всего 20,6 % от того, что было выделено на этот год.[86]

13 июля 2020 года Путин дал поручение правительству изменить национальные цели, намеченные на 2018 год, и перенести крайний срок реализации с 2024 на 2030 год.[87] Он сказал, что России необходимо «исходить из реальности», и обвинил региональных лидеров в неисполнении программных бюджетов, как предполагалось изначально.[88]

Указ Президента от 21 июля официально закрепил продление до 2030 года и включил ряд целей цифровой трансформации, которые должны быть достигнуты к тому времени, включая «цифровую зрелость» во всей экономике и социальной сфере и увеличил инвестиции в отечественные технологические решения.[89]

После распоряжения Путина правительственные чиновники заявили, что начнут подготовку поправок к национальным проектам, которые они надеются завершить в ближайшие месяцы.[90]

В том же месяце Министерство финансов предложило сократить большую часть государственных расходов на 10% до 2023 года в попытке сбалансировать федеральный бюджет, который пострадал из-за COVID-19 и обвала цен на нефть.[91]

---

[85] «Цифровая экономика». Как реорганизовать национальную программу, чтобы она работала в полную силу», С-Новости, октябрь. 22, 2019, https://www.cnews.ru/articles/2019-10-22_tsifrovaya_ekonomikakak_reorganizovat.
[86] «Национальная программа Российской Федерации «Цифровая экономика».
[87] Максим Рубченко, «Путин перенес крайний срок реализации национальных программ», Ведомости, 14 июля 2020 г., https://www.vedomosti.ru/economics/articles/2020/07/13/834504-prezident-otlozhil-natsproekti.
[88] Там же.
[89] «Указ о национальных целях развития России до 2030 года», 21 июля 2020 года, http://kremlin.ru/events/ president/ news/63728.
[90] Евгений Калюков, «Орешкин рассказал о целях меняющихся национальных проектов», РБК, 21 июля 2020 г., https://www.rbc.ru/economics/ 21/07/2020/ 5f16ae089a79472547f0211f.
[91] Иван Ткачева и Юлия Старостина, «Министерство финансов предложило программу сокращения бюджетных расходов», Минфин предложил программу сокращения расходов бюджета, РБК, 21 июля 2020 г., https://www.rbc.ru/economics/ 21/07/2020/ 5f15ab829a7947382f5ec57e.

30 сентября Правительство представило в Государственную Думу проект бюджета на 2021-2023 годы с поправками, внесенными в связи с COVID-19.[92]

В отчетах говорится, что правительственный проект, возможно, сократил финансирование программы «Цифровая экономика» с почти 2 триллионов рублей до всего 92,1 миллиарда рублей, при этом на федеральный проект ИИ было выделено всего 16,5 миллиарда рублей по сравнению с 22,5 миллиардами, выделенными в первоначальной концепции проекта.[93]

В окончательной версии законопроекта, который был принят Думой 9 декабря, содержались несколько более скромные сокращения, сократив бюджет на цифровизацию до 550 миллиардов рублей.[94]

Конечно, последствия COVID-19, вероятно, будут продолжаться еще долго после окончания пандемии.

Негативные последствия для бюджета и задержки в реализации программы «Цифровая экономика» и федерального проекта ИИ будут по-прежнему оказывать влияние на способность правительства эффективно осуществлять свои планы по цифровизации в будущем.

Более того, кризис только усугубит другие проблемы, уже стоящие на пути этих планов, в том числе низкое денежное исполнение необходимых расходов и тот факт, что национальные программы пытаются охватить такой широкий круг задач.

Одним из положительных показателей для будущего программы «Цифровая экономика» является то, что пандемия выявила важность цифровизации во всех аспектах жизни общества, хотя, по мнению Совета Федерации, она также выявила некоторые нерешенные проблемы, такие как неравный доступ к цифровым технологиям во всем обществе.[95] Поэтому Правительство, скорее всего, будет уделять приоритетное внимание быстрой

---

[92] Ирина Пешкова, «Бюджет «Цифровой экономики» может быть сокращен до 92 миллиардов рублей», С-Новости, 21 сентября 2020 года, https://www.rbc.ru/economics/21/07/2020/5f16ae089a79472547f0211f.

[93] Там же.

[94] Роман Маркелов, «О цифрах», В порядке цифр, Российская газета, 10 декабря 2020 г., https://rg.ru/2020/12/10/kakim-budet-novyj-federalnyj-biudzhet-na-tri-goda.html.

[95] «О реализации национального проекта «Цифровая экономика Российской Федерации», Совет Федерации, 18 ноября 2020 года, http://council.gov.ru/activity/documents/121565.

реализации определенных аспектов повестки дня в области цифровизации, таких как те, которые обеспечивают равный доступ к Интернету, одновременно проводя работу в других областях, таких как ИИ, насколько это возможно, учитывая ограниченные и ограниченные ресурсы. Мы не ожидаем, что доля участия государства в усилиях по цифровизации уменьшится, и она, скорее всего, увеличится, поскольку Правительство уделяет повышенное внимание цифровым усилиям (и ИИ в частности) как важному элементу взаимодействия граждан и государства.

Правительство считает, что, если большая часть финансирования этих инициатив будет поступать от государства, оно сможет соответствующим образом увеличить свою долю участия в российской жизни. Как упоминалось ранее, вполне вероятно, что инициативы министерства по развитию искусственного интеллекта не будут развиваться такими же темпами, и, по сути, некоторые из них могут оказаться полностью неудачными.

В отличие от более гибкой экосистемы США, которая развивалась на протяжении десятилетий, Россия пытается втиснуть несколько десятилетий роста всего в несколько лет.

Однако персонал и инфраструктура для осуществления необходимых реформ еще не созданы во всех подразделениях Правительства, поэтому, в то время как некоторые приоритетные министерства (такие как службы государственной безопасности) могут рассчитывать на выделение большего объема ресурсов, другие не смогут достичь своих целей в установленные сроки.

Поскольку Правительство продолжает настаивать на этих усилиях и финансировать их, будет важно периодически пересматривать результаты, чтобы оценить, какие усилия министерства продвигаются быстрыми темпами, а какие отстают.

РОССИЙСКАЯ ЭКОСИСТЕМА ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

В этой главе представлена российская экосистема ИИ, ключевые компоненты которой обсуждаются в последующих главах. Сначала в нем

обсуждаются цели российской экосистемы и приоритеты, которые правительство выделило для инноваций.

Затем в нем описывается структура экосистемы ИИ в России, включая ключевых спонсоров.

Наконец, в нем освещаются проблемы, препятствующие росту и динамичности российской экосистемы ИИ.

Ключевой особенностью экосистемы является лидерство государственных компаний (таких как Sber, Ростех и «Газпром нефть») и непропорциональное финансирование со стороны Правительства России для разработки технологий с поддержкой ИИ.

Существуют государственные инкубаторы (Сколково), спонсоры (Российский фонд прямых инвестиций) и инициативы (Национальная технологическая инициатива), направленные на содействие развитию технологий с поддержкой ИИ. В то время как частный сектор разнообразен с точки зрения размера (от крупных Yandex.ru до гораздо меньших компаний), количество стартапов невелико по сравнению с цифрами в Соединенных Штатах и Китае. Правительство определило приоритетные области здравоохранения, транспорта, сельского хозяйства, топливно-энергетической промышленности и обрабатывающей промышленности в качестве ключевых областей для внедрения технологий с поддержкой ИИ.

Кроме того, значительные усилия направлены на внедрение технологий с поддержкой ИИ в государственные процессы России, включая взаимодействие между гражданами и государственными службами. Пандемия COVID-19 стимулировала некоторые ключевые технологические разработки.

Как обсуждалось в этом разделе, ключевые проблемы для развития ИИ в России включают потенциальное стремление к получению ренты компаниями, использующими государственное финансирование, необходимость увеличения вычислительной мощности и отечественного оборудования, учитывая проблемы с закупкой западного оборудования в свете санкций, низкие

темпы внедрения цифровых технологий в частном секторе и необходимость расширения международного сотрудничества.

Российская экосистема искусственного интеллекта в более широком контексте

Цели российской экосистемы ИИ лучше всего поняты в более широком контексте усилий по экономическому развитию и модернизации России и включают улучшение благосостояния россиян, а также условий для бизнеса и предпринимательской деятельности.

В области технологий с поддержкой ИИ предпринимаются значительные военные усилия в сочетании с пониманием того, что гражданские инструменты ИИ будут применяться в военной области. Российское руководство также рассматривает способность к инновациям как один из признаков суверенной великой державы и военных инноваций, в том числе в области ИИ, и считает это необходимым для общей позиции России по сдерживанию в противодействии ее предполагаемой среде угроз, следовательно, для усилий стать одним из мировых лидеров в области ИИ.

В то время как президент России Путин объявил 2021 год Годом науки в России, Россия продолжает бороться с инновациями, как показывают ключевые показатели.

Согласно данным Глобального инновационного индекса (GII) 2020 года, Россия занимает 47-е место (из 131 страны), и эти данные свидетельствуют о том, что, хотя Россия больше инвестировала в инновации, ее инновационные результаты и выпуск снизились.[96]

В рейтинге GII также отмечается, что Россия занимает 32-е место из 39 европейских экономик по уровню инноваций.[97]

Общее финансирование НИОКР в России остается сравнительно низким. Ожидается, что финансирование НИОКР будет постепенно увеличиваться

[96] См. Данные по России за 2020 год на веб-сайте: «Глобальный инновационный индекс», доступ к которому получен 22 февраля 2021 г., https://www.globalinnovationindex.org/analysis-economy.
[97] Там же.

в течение следующих нескольких лет, при этом 40% гражданских НИОКР будут сосредоточены на фундаментальных исследованиях.[98]

Согласно данным базы данных Scopus, Россия занимает 11-12-е место по количеству научных публикаций в таких дисциплинах, как астрономия, инженерия, материаловедение, химия и математика[99] (количество научных публикаций в этих областях аналогично числу научных публикаций в Австралии, Бразилии, Иране и Южной Корее). Это улучшение по сравнению с местом (с 15-го по 16-е), которое она занимала всего семь лет назад.[100]

Российские аналитики отмечают, что российская наука по-прежнему страдает от проблем с качеством стипендий, включая плагиат и самоцитирование.[101]

Правительственные инициативы уделяют приоритетное внимание подготовке нового поколения ученых и решению проблем утечки мозгов (см. раздел «Образование» настоящего доклада). Как обсуждалось в предыдущей главе, Стратегия ИИ России и многочисленные дорожные карты ее реализации определяют ориентиры для эволюции экосистемы ИИ в целом. Цели лучше всего понятны в рамках двух национальных проектов 2018 года: национального проекта «Цифровая экономика», возглавляемого Министерством цифрового развития; и, поскольку общие усилия встроены в более широкую инновационную экосистему России, национальный проект «Наука», возглавляемый Министерством науки и образования.

Ключевые показатели, установленные Правительством России по развитию ИИ в стратегических документы, некоторые из которых были подготовлены с учетом значительных отраслевых консультаций, включают количество публикаций российских авторов в международных научных

---

[98] Центр Гайдара, Тенденции и перспективы российской экономики в 2019 году, стр.499, https://www.iep.ru/en/publications/russian-economy-in-2019-trends-and-outlooks-issue-41.html.

[99] Там же. См. Данные ОЭСР по России: «Российская Федерация», Данные ОЭСР, доступ к которым получен 22 февраля 2021 г., https://data.oecd.org/russian-federation.

[100] Е. Ерохина, «Российская наука в Scopus и WoS: количество или качество», Индикатор, февраль. 8, 2019, https:// indicator.ru/engineering-science/rossijskaya-nauka-v-scopus-i-wos-kolichestvo-ili-kachestvo.htm.

[101] Там же. Центр Гайдара, Тенденции и перспективы российской экономики в 2019 году, стр.495.

журналах и на ведущих конференциях, а также количество патентов и инструментов, разработанных компаниями.

Эти показатели неуклонно улучшаются, но все еще недостаточны. В рейтинге научных журналов Россия занимает 25-е место (1996-2019 годы из 190 стран).

Однако в области ИИ его рейтинг вырос с 21 до 16 в период с 2018 по 2019 год.[102]

По общему количеству работ российские исследователи оценивают, что Россия занимает 20-е место в мире. По их оценкам, в 2019 году в России насчитывалось 16 000 активных исследователей в области ИИ, 4 340 публикаций в рецензируемых журналах и 16 публикаций на конференциях по ИИ.[103]

Федеральный проект «Зарождающийся ИИ» в России предоставляет ключевые показатели, которые будут важны для аналитиков для отслеживания продвижения вперед.[104]

Согласно инструменту глобальной динамичности ИИ Стэнфордского университета, показатели российской экономики и НИОКР сравнительно низки.[105]

Россия также занимает 29-е место из 194 по Индексу готовности Таиланда.[106]

Российские аналитики из Московского физико-технического института (МФТИ) утверждают, что «Россия находится между 20-м и 30-м местами в мире по общему состоянию индустрии ИИ, разработкам, финансированию, персоналу и т.д.».[107]

---

[102] См. Данные: «SJR – Международный научный рейтинг», Scimago, доступ к 22 февраля 2021 г., https://www.scimagojr.com/countryrank.php?category-1702&year-2019.
[103] Альманах Московского физико-технического института (МФТИ) за 2019 год, стр.8-9.
[104] См. текст резюме Федерального проекта ИИ, доступ к которому получен 22 февраля 2021 г.
[105] См. Данные: «Инструмент глобальной вибрации ИИ», HAI, Стэнфордский университет, доступ к 22 февраля 2021 г., https://hai.stanford.edu/ai-global-vibrancy-tool.
[106] См. Данные: «Индекс готовности правительства к ИИ 2020», Oxford Insights, доступ к февр. 22, 2021, https://www.oxfordinsights.com/ government-ai-readiness-index- 2020.
[107] Альманах Московского физико-технического института (МФТИ) за 2019 год, стр.8-9.

Совсем недавно в отчете МФТИ указывалось, что, хотя объем деятельности, связанной с ИИ, в России растет примерно в 10 раз быстрее, чем ВВП России, он по-прежнему недофинансируется государством, утверждая, что уровень инвестиций в ИИ в России в 350 раз ниже, чем в Китае.

МФТИ является ведущим российским университетом и координационным центром российской академической работы в области ИИ, предоставляя полезную информацию об экосистеме ИИ в России.

МФТИ является ведущим академическим учреждением, которое помогает другим российским университетам с помощью AI RDT&E.

Недостаточные инвестиции российского правительства в ИИ приводятся в качестве одного из основных факторов отставания России в области ИИ в 2020 году по сравнению с другими ведущими странами.[108]

Структура экосистемы

Экосистему ИИ в России лучше всего понимать как кластеры взаимосвязанной деятельности в правительственной, государственно-корпоративной, военной, академической и частной сферах, каждый из которых более подробно обсуждается в следующих главах этого отчета.

Ключевой особенностью экосистемы является лидерство государственных компаний (Sber, Ростех и «Газпром нефть») и значительный объем финансирования со стороны Правительства России для исследований и разработок технологий с поддержкой ИИ.

Существуют государственные инкубаторы (Сколково), спонсоры (Российский фонд прямых инвестиций) и инициативы (Национальная технологическая инициатива), направленные на содействие развитию технологий с поддержкой ИИ.

Частный сектор разнообразен по размеру (начиная от крупных компаний Яндекс и Mail.ru до небольших венчурных фирм). Экосистема сосредоточена

[108] «Объем рынка искусственного интеллекта в России почти достиг 300 миллиардов рублей» Известия, 4 апреля 2021 года, https://iz.ru/1151591/2021-04-14/obem-rynka-ii-v-rossii-prakticheski-dostig-300-mlrd-rublei.

в Сколково и Сколтехе при активном участии Sber, «Газпром нефти» и таких компаний, как Яндекс и Mail.ru. Sber и Герман Греф играют заметную роль в экосистеме, учитывая ключевую роль Sber в разработке Стратегии ИИ и соответствующей дорожной карты развития ИИ в России (другие участники процесса включали Яндекс, Mail.ru и «Газпром нефть»).

Наряду с МТС и RFDI они образуют альянс ИИ-Россия. Крупные хозяйствующие субъекты участвовали, в том числе в рамках АНО «Цифровая экономика», в процессе разработки законов и нормативных актов. Важная роль отводится ключевым городам и регионам.

Москва была площадкой как для юридического, так и для практического внедрения инструментов с поддержкой ИИ.

Некоторые регионы России участвовали в программах «умные города» и «умные регионы», предпринимались усилия по созданию региональных инновационных центров.

Они столкнулись с некоторой критикой со стороны отраслевых комментаторов, которые утверждают, что такой подход может быть неэффективным.

Российские аналитики также отмечают, что «как движущая сила цифровых изменений стартапы более типичны для развитых регионов».[109]

Предпринимаются многочисленные усилия по координации исследований и разработок с участием академических институтов и бизнеса, что обеспечивается государственным финансированием, как подробно обсуждается в следующих разделах отчета.

Некоторые отметили активное стимулирование Правительством академического сектора, например, посредством федерального финансирования проекта 5-100, направленного на повышение конкурентоспособности. Но предпринимались и другие усилия, например, путем создания центров, специально ориентированных на ИИ, в ключевых институтах, таких как

[109] Центр Гайдара, Тенденции и перспективы российской экономики в 2019 году, стр.480.

Национальная технологическая инициатива. Федеральное финансирование поступило по нескольким каналам во многие из этих университетов.

Например, центр ИИ МФТИ специализируется на исследованиях разработок и коммерциализации. Военные инновации осуществляются Министерством обороны России в рамках Государственных программ вооружения и при содействии Ростеха и других оборонных предприятий при финансировании из специальных инкубаторов, как обсуждается в последующих разделах настоящего отчета.

Но, в то время как Россия тратит значительное количество усилий и средств на военные усилия в области технологий с поддержкой ИИ, есть также надежда, что гражданские разработки приведут к военным достижениям.

В настоящее время прямое военно-гражданское сотрудничество находится на относительно низком уровне, и только некоторые учебные заведения, такие как Южный федеральный университет, сотрудничают с Министерством обороны.

Приоритетные области и технологии

Правительство определило приоритетные области здравоохранения, транспорта, сельского хозяйства, топливно-энергетической промышленности и обрабатывающей промышленности в качестве ключевых областей для внедрения технологий с поддержкой ИИ. Кроме того, значительные усилия направлены на внедрение технологий с поддержкой ИИ в государственные процессы России. Как обсуждалось в дальнейших разделах настоящего доклада, пандемия COVID-19 стимулировала некоторые ключевые технологические достижения.

Особенностью российской системы является то, что российское государство сохранит доступ ко всем данным, даже несмотря на то, что государство возглавило усилия по предоставлению разработчикам лучшего доступа к таким данным. Федеральный проект ИИ определяет несколько

приоритетных областей для развития, включая здравоохранение, транспорт, сельское хозяйство, топливно-энергетическую и обрабатывающую промышленность, как обсуждается далее в этом отчете.

В свою очередь, дорожная карта ИИ определяет следующие приоритетные области (с более значительными уровнями финансирования в первую очередь): системы принятия решений, компьютерное зрение, обработка естественного языка, распознавание и синтез речи, а также передовые методы и технологии ИИ.

Кроме того, предпринимаются усилия по преобразованию взаимодействия российского Правительства со своими гражданами и сокращению бюрократии с помощью инструментов с поддержкой ИИ.

В цифровой экономике есть несколько направлений: сквозные цифровые технологии (5G, робототехника, виртуальная реальность, блокчейн, квантовые вычисления, новые производственные технологии) и ИИ.

В то время как правительство уделяет приоритетное внимание разработке технологических решений для указанных выше областей, частный сектор работает над разработкой решений в своих собственных интересах, включая цифровых помощников и других, как обсуждается далее в этом докладе.

По мнению российских ученых, российская ИТ-индустрия является одной из немногих областей, где экспорт превышает внутренние продажи, и «Стратегия развития ИИ указывает приоритетные области включая автономное самообразование, автономную декомпозицию сложных задач, алгоритмическое моделирование биологических систем принятия решений и т.д.)».[110] Аналитические отчеты США свидетельствуют о шестикратном увеличении числа публикаций российских ученых в период с 2010 по 2018 год в «таких областях, как машинное обучение, алгоритмы и робототехника», почти половина из которых посвящена «компьютерному зрению,

[110] Там же, стр.506.

распознаванию образов, лингвистике, обработка естественного языка, алгоритмы и робототехника».[111]

В следующем разделе этого отчета будут более подробно рассмотрены элементы академической и деловой среды, которые формируют развитие этих конкретных технологий в России.

Проблемы для российской экосистемы ИИ

Аналитики утверждают, что ключевыми проблемами для развития ИИ в России являются: стремление к получению ренты компаниями, привыкшими к государственному финансированию, потребность в большей вычислительной мощности и потребность в отечественном оборудовании.

Две другие проблемы, «утечка мозгов» и необходимость международного сотрудничества, обсуждаются в соответствующих главах ниже в этом докладе.

Стремление к получению ренты

Стратегия экономического развития России в настоящее время опирается на то, что государство будет играть ведущую роль в модернизации. Кроме того, наблюдается общая тенденция сокращения иностранных инвестиций в венчурные проекты в сочетании с заменой частного финансирования государственным.[112] Это имеет много недостатков.

Как отмечает аналитик авторитетного российского Института экономической политики имени Е.Т. Гайдара, потенциальная ключевая проблема заключается в том, что прямые государственные субсидии не будут мотивировать участников рынка повышать свою эффективность, напротив, субсидируемым компаниям будет предложено принять поведение, ориентированное на получение ренты.

[111] Маргарита Конаева и Джеймс Данэм, Российские исследования ИИ с 2010 по 2018 год: Темы, тенденции и институты, Краткий выпуск CSET, октябрь 2020 года, https://cset.georgetown.edu/wp-content/uploads/CSET-Russian-AI-Research-2010-to-2018.pdf.
[112] Центр Гайдара, Тенденции и перспективы российской экономики в 2019 году, стр.504.

Соответственно, представляется необходимым поощрять интерес бизнеса к процессам цифровой трансформации, чтобы обеспечить рост доли затрат частного сектора на НИОКР в области информационно-коммуникационных технологий.[113]

В подтверждение этого в российском частном секторе, в частности среди средних и малых компаний, высказывались опасения, что государственное руководство и финансирование будут формировать рынок таким образом, чтобы это давало преимущества государственным фирмам и крупным компаниям.[114]

Уже сейчас опросы показывают, что инструментами государственной поддержки пользуются 72% крупных компаний, 45% средних компаний и только 42% малых предприятий.

Они также отмечают, что «39% стартапов разочарованы инструментами государственной поддержки, в том числе через институты развития, поскольку, согласно их аргументам, они не получают никакой ощутимой выгоды».[115]

Как обсуждается далее в этом отчете, текущая стратегия России в области ИИ предусматривает предоставление грантов средним и малым компаниям.

Однако такая поддержка также увековечивает зависимость от государственного финансирования, что, в свою очередь, может препятствовать инновациям.

Внедрение аппаратного обеспечения и цифровых технологий

Существуют опасения, что Россия в целом не располагает достаточной ИТ-инфраструктурой по всей стране или достаточными вычислительными мощностями для ведения современной науки, что приводит к усилиям ученых, направленным на разработку дорожной карты суперкомпьютеров.[116]

---

[113] Там же, стр.549.
[114] См. «Правительство России взаимодействует с отраслью ИКТ и сталкивается с критикой», Выпуск 7, Программа изучения России, CNA, DOP-2020-U-027701-Финал2, 2020.
[115] Центр Гайдара, Тенденции и перспективы российской экономики в 2019 году, стр.505.
[116] «В России разработали концепцию национальной суперкомпьютерной инфраструктуры», ТАСС, 22 апреля 2020 г., https://nauka.tass.ru/nauka/8309573.

Хотя существуют конкретные суперкомпьютерные инструменты для ИИ, в том числе суперкомпьютер «Жорес» Сколтеха, который совершенствуется, чтобы войти в Топ-500, и Кристофари от Sber, рейтинг России по мощности суперкомпьютеров остается низким.[117]

Кроме того, российские экономисты признают сохраняющуюся проблему зависимости от американского, тайваньского и южнокорейского полупроводникового оборудования для запуска алгоритмов ИИ, учитывая, что российская электронная промышленность невелика и в значительной степени ориентирована на конкретное военное производство, а не на обобщенные продукты.[118] Кроме того, хотя было много положительных тематических исследований, свидетельствующих о распространенности цифровых технологий в российских компаниях, оценки глубины и интеграции в бизнес предполагают некоторые причины для беспокойства.

По мнению российских аналитиков, наиболее показательным в этом отношении является использование робототехники компаниями по сравнению с численностью их сотрудников.

По данным 2017 года Международной федерации робототехники в среднем в Европе на 10 000 рабочих мест приходилось 99 роботов, а в таких странах, как Сингапур и Южная Корея, этот показатель составлял более 600 роботов; однако российский показатель был рядом с Индией – 4 и 3 робота на 10 000 рабочих мест соответственно.

Следует отметить, что роботизация является важнейшим фактором обеспечения конкурентоспособности в таких высокотехнологичных отраслях, как автомобилестроение, оптика и электроника.

Безусловно, учитывая стремление российского правительства к ИИ и инновациям в последние несколько лет, показатели России могут улучшиться, хотя наверстать упущенное может оказаться невозможным.

---

[117] См. «Список ТОП 500 - ноябрь 2020 года», доступ к которому получен 22 февраля 2021 года, https://www.top500.org/lists/top500/list/2020/11.

[118] Петрелла, Миллер и Купер, Стратегия искусственного интеллекта России.

АКАДЕМИЧЕСКИЕ ОРГАНИЗАЦИИ, СВЯЗАННЫЕ С ИСКУССТВЕННЫМ ИНТЕЛЛЕКТОМ, ОБРАЗОВАНИЕМ И ОБУЧЕНИЕМ

Россия сталкивается со значительными проблемами, когда дело доходит до ее демографической ситуации, связанной с технологиями. В этом разделе рассматривается растущий спрос России на высококвалифицированных технических специалистов и анализируются ее усилия по удовлетворению этих потребностей путем реализации образовательных инициатив во всех демографических группах.

В нем содержится обзор ключевых академических институтов, занимающихся разработкой специалистов в области ИИ и технологий, а также усилий, финансируемых правительством, включая конференции, хакатоны, соревнования по программированию и интенсивные учебные модули, используемые в российских аудиториях.

Кроме того, отмечая успехи в усилиях России по наращиванию потенциала, мы также рассматриваем недостатки, препятствия и предстоящие задачи.

Наконец, мы обсудим, что эти тенденции в человеческом капитале означают для будущего российских ИТ и способности Москвы достичь своих целей в области ИИ.

Проблемы, связанные с нехваткой технических экспертов среди ИТ-населения России

После знаменитой цитаты Путина об ИИ в 2017 году Кремль выдвинул ряд стратегических инициатив по повышению качества и количества российских исследований в области ИИ и дальнейшей разработке и внедрению цифровых решений, направленных на достижение смелых показателей к 2024 и 2030 годам.[119]

[119] Путин: «Лидер в области искусственного интеллекта будет править миром», CNBC, 4 сентября 2017 г., https://www.cnbc.com/2017/09/04/ putin-leader-in-artificial -intelligence-will-rule-world.html.

Однако Россия сталкивается с ошеломляющей нехваткой технических экспертов, что приводит к тому, что это можно объяснить, как стремительно растущим спросом, так и проблемами, связанными с обучением и удержанием квалифицированной рабочей силы.

По словам заместителя главы Министерства цифровой науки, дефицит численности ИТ-персонала в России в настоящее время составляет от 500 000 до 1 миллиона человек, несмотря на усилия государства по преодолению этой нехватки.[120]

Эта цифра включает как высококвалифицированных специалистов, так и специалистов широкого профиля, которые могут работать в разных отраслях.

Директор по кадрам для цифровой экономики Валентина Куренкова отмечает: «Прогнозируемый взрывной рост рынка технологий искусственного интеллекта приведет к дополнительному спросу в 95 тысяч человек ежегодно, а это означает, что дефицит будет увеличиваться из года в год».[121]

Согласно недавнему отчету Министерства образования, из-за роста спроса на ИИ во всех секторах к 2025 году будет не хватать 2 миллионов специалистов.[122]

Начало пандемии COVID-19 имеет только ускорил эту тенденцию, поскольку более 24% опрошенных ИТ и технологических компаний сообщили об увеличении инвестиций в ИИ.[123]

Число российских экспертов в области ИИ, в отличие от технических экспертов в целом, оценить сложнее, поскольку эта область несколько туманна и не имеет четкого определения.

По словам генерального директора Sber Германа Грефа сегодня в России в качестве разработчиков ИИ работают всего около 6000-6500 экспертов,

---

[120] «Программисты на Python в России получают до 400 тысяч рублей. Но девушки не идут к ним работать», CNews, 2021, https://www.cnews.ru/news/top/2021-01-14_raskryt_potolok_rossijskih.

[121] Георгий Воронович «Сотни тысяч новых сотрудников: как поддерживается ИТ-сектор в России», Gazeta.Ru, 12 декабря 2020 года, https://www.gazeta.ru/tech/2020/12/04_a_13387279.shtml.

[122] «В России растет нехватка персонала в области искусственного интеллекта, больших данных и машинного обучения», CNews, март. 28, 2018, https://data.cnews.ru/news/top/2018-03-28.

[123] «Основы искусственного интеллекта будут преподаваться в начальной школе».

что, как он отмечает, даже не соответствует числу работников в одной лаборатории Microsoft.[124]

Эту цифру следует отличать от большего числа академических исследователей в областях, связанных с ИИ, и числа выпускников университетов, в целом связанных с ИИ, на которых также ссылаются в этом разделе.

Эти цифры отражают результаты академической деятельности и указывают на человеческий капитал/потенциал, но не обязательно на «рабочую силу ИИ».

Утечка мозгов

Причиной этой острой нехватки российских ИТ-специалистов является феномен «утечки мозгов», когда эксперты мигрируют на работу в конкурирующие страны.

Несмотря на глобальную нехватку специалистов в области ИИ, большинство стран активно стремятся привлекать и удерживать технических экспертов, другие страны добились гораздо большего успеха в этих начинаниях.

Основываясь на данных о занятости из публикаций ИИ 2019 года, «Американские работодатели привлекают львиную долю лучших талантов в области искусственного интеллекта – 46% работали на американского работодателя.

Китай занял второе место в списке, на его долю приходится 11% занятости, за ним следует Великобритания с 7%. На Канаду, Германию и Японию приходилось по 4%».

Хотя существует множество факторов, способствующих утечке мозгов, таких как качество жизни в данной стране, заметно отличающиеся зарплаты, предлагаемые выпускникам ИТ, вероятно, являются самым большим фактором.

[124] «Греф призвал устранить нехватку специалистов по искусственному интеллекту», РИА Новости, 30 мая 2019 года, https://ria.ru/20190530/1555110473.html.

Согласно отчету Института исследований внешней политики за 2020 год, российские ИТ-разработчики зарабатывают всего около 25% от зарплаты своих американских коллег.[125]

Некоторые отмечают, что утечка мозгов оказала особенно заметное влияние на оборонный сектор России.[126]

По данным Института исследований внешней политики (FPRI) «В 2016 году половина предприятий российского оборонно-промышленного комплекса испытывала нехватку кадров. Доля специалистов оборонной промышленности в возрасте до 30 лет составляла всего четыре процента. Существует мало доказательств того, что эти показатели улучшились».[127]

Патрелла и др. объясняют такие трудности в привлечении и удержании талантов в оборонном секторе в первую очередь низкими государственными инвестициями в технологии.[128]

Российские фирмы пытались использовать различные стратегии для ограничения утечки мозгов, включая продление сроков контрактов, повышение заработной платы и набор иностранных кандидатов и студентов.

Однако до сих пор ничто в достаточной степени не смягчило бегство ИТ-специалистов. Это также усугубляется продолжающейся пандемией. В письме представителей бизнеса премьер-министр Мишустин предупредил, что к концу 2021 года 10-15 000 тысяч ИТ-специалистов могут покинуть Россию из-за воздействия COVID-19 на отрасль.[129]

Образовательные центры ведущих российских университетов.

В то время как в России создан ряд исключительных институтов, которые проводят высококачественные исследования, лишь несколько ее университетов занимают первые места в мире, согласно трем наиболее авторитетным спискам:

---

[125] Петрелла, Миллер и Купер, Стратегия искусственного интеллекта России.
[126] Там же.
[127] Там же.
[128] Тамже.
[129] «Российская техническая индустрия сталкивается с утечкой мозгов» Moscow Times, июнь 17, 2020, https://www.themoscowtimes.com/2020/06/17/russian-tech-industry-faces-coronavirus-brain-drain-a70607.

Рейтинг Times Higher Education (THE), рейтинг Quacquarelli Symonds (QS) и Шанхайский академический рейтинг университетов мира.[130]

В надежде улучшить мировое положение России и создать образовательные центры мирового класса Кремль попытался устранить этот недостаток в 2012 году, поставив перед собой официальную цель к 2020 году иметь пять университетов, входящих в топ-100, по стандартам этих трех рейтинговых систем.[131]

Однако эта цель не была достигнута.

По состоянию на февраль 2021 года единственным российским университетом, включенным либо в Шанхайский рейтинг, либо в рейтинг Quacquarelli Symonds 100, был Московский государственный университет имени М.В. Ломоносова (МГУ, 93-е и 73-е места соответственно).[132] В рейтинге 2020 года МГУ занял 174-е место, а следующий по рейтингу российский университет – МФТИ, занял 201-250-е место в группе.[133]

Ведущие российские университеты в области искусственного интеллекта

Чтобы получить представление о том, как российские институты оцениваются с точки зрения исследований в области ИИ, одним из показателей для изучения является общее количество опубликованных научных работ, что, по мнению российских исследователей, ставит Россию на 20-е место в мире.

По их оценкам, в 2019 году в рецензируемых журналах было 4 340 публикаций по ИИ, 16 публикаций на конференциях по ИИ

[130] RBC, https://www.rbc.ru/society/30/01/2017/588f0cab9a794716f7e77440.
[131] Конаев и Данэм, Российские исследования ИИ с 2010 по 2018 год: Темы, тенденции и институты.
[132] «Академический рейтинг университетов мира 2020», доступ к которому получен 31 января 2021 г., http://www.shanghairanking.com/ARWU2020.html; «Рейтинг университетов мира QS 2021», «Лучшие университеты QS», доступ к 31 января 2021 года, https://www.topuniversities.com/university-rankings/world-university-rankings/2021.
[133] 142 «Обучение в Российской Федерации», Times Higher Education, 31 января 2021 г., https://www.timeshighereducation.com/student/where-to-study/study-in-russian-federation.

и 16 000 активных исследователей в области ИИ в России, хотя эта цифра, вероятно, включает исследователей в смежных областях.[134]

Аналитические отчеты США показывают, что за последнее десятилетие это значительно улучшилось, отметив шестикратное увеличение числа публикаций российских ученых в период с 2010 по 2018 год в «таких областях, как машинное обучение, алгоритмы и робототехника», почти половина из которых посвящена «компьютерному зрению, распознаванию образов, лингвистике, обработке естественного языка, алгоритмы и робототехника».[135]

Что касается конкретных российских университетов, то в рейтинге Quacquarelli Symonds для ведущих инженерных и технологических университетов МГУ занимает 59-е место, за которым следуют Санкт-Петербургский политехнический университет (191-е место) и Новосибирский университет (193-е место).

В диапазоне 200-300 есть ряд российских университетов: МФТИ (202-е место), Санкт-Петербургский государственный университет (СПбГУ, 207-е место)[136], Петербургский университет информационных технологий, механики и оптики (ИТМО, 207-е место), Московский государственный университет им. Н.Э. Баумана (243-е место), Национальный научно-технический университет (МИСИС, 247-е место), Национальный исследовательский Томский политехнический университет (282-е место) и согласно Альманаху ИИ МФТИ 2020, в 2019 году около 18 300 студентов окончили российские университеты по специальностям, в том числе: прикладная математика и информатика; фундаментальная информатика и информационные технологии; информатика и вычислительная техника; информационно-коммуникационные технологии и системы связи; математика и компьютерные науки; информационные системы и технологии; и прикладная информатика – все из которых считаются относящимися к области ИИ.

---

[134] Альманах Московского физико-технического института (МФТИ) за 2019 год, стр.8-9.
[135] Конаев и Данэм, Российские исследования ИИ с 2010 по 2018 год: Темы, тенденции и институты.
[136] Там же.

Около 2 000 из этих студентов окончили ведущие российские университеты ИИ, которые в отчете определены как Московский государственный университет (МГУ), МФТИ, Московская высшая школа экономики (ВШЭ), Санкт-Петербургский государственный университет (СПбГУ), Санкт-Петербургский университет информационных технологий, механики и оптики (ИТМО) и Сколтех.

Однако рейтинги лучших российских программ ИИ различаются.[137]

В Москве есть несколько выдающихся университетов, известных подготовкой ведущих экспертов и проведением высококачественных исследований в области ИИ. МГУ, который часто получает самые высокие рейтинги, является одной из школ, находящихся на переднем крае этих исследований.

Согласно индексу ИИ МФТИ, в 2019 году в МГУ было около 350 выпускников и почти 500 студентов бакалавриата по ИИ.[138]

МФТИ – еще один университет, лидирующий в области ИИ. Согласно рейтингу ведущих российских технических университетов Superjob 2020 года, составленному на основе средней заработной платы выпускников школ, МФТИ занял первое место (средняя зарплата выпускников ИТ составляет 180 000 рублей (2 403 доллара)).[139]

В 2017 году Правительство России выбрало МФТИ местом размещения нового Центра искусственного интеллекта в рамках Национальной технологической инициативы.

---

[137] Например, CSET Джорджтаунского университета входит в топ-20 российских исследовательских институтов в области искусственного интеллекта, соответственно, следующим образом (на основе количества результатов исследований в области искусственного интеллекта на английском языке): Российская академия наук, Национальный исследовательский университет – Высшая школа экономики, Московский государственный университет, Санкт-Петербургский государственный университет, Московский физико-технический институт, Казанский федеральный университет, Сколковский институт науки и технологий, Национальный исследовательский ядерный университет МИФИ, Южный федеральный университет, Томский политехнический университет, Уральский федеральный университет, Российский университет Дружбы Народов, Московский государственный технический университет им. Баумана, Яндекс, Сибирский государственный аэрокосмический университет, Томский государственный университет, Санкт-Петербургский государственный политехнический университет, Новосибирский государственный технический университет, Новосибирский государственный университет и Дальневосточный федеральный университет; Конаев и Данэм, Российские исследования ИИ с 2010 по 2018 год: Темы, тенденции и институты.

[138] Альманах искусственного интеллекта: Индекс ИИ 2019 - Россия, МФТИ, Москва, № 4, март 2020 г.

[139] «Рейтинг технических университетов России 2020», SuberJob, доступ к 31 января 2021 г., https://students.superjob.ru/reiting-vuzov/it.

В 2019 году в МФТИ обучалось около 250 выпускников и 300 студентов бакалавриата по ИИ.[140]

Третьей примечательной школой является Высшая школа экономики (ВШЭ), в которой в 2019 году обучалось около 250 выпускников и 550 студентов бакалавриата по ИИ.[141]

В Санкт-Петербурге также находится ряд известных университетов, преподающих предметы, связанные с ИИ. В Санкт-Петербургском государственном университете (СПбГУ) в 2019 году обучалось около 150 аспирантов и 300 студентов бакалавриата по ИИ.[142]

Также следует отметить Санкт-Петербургский политехнический университет (СПбПУ).

В июле 2020 года СПбПУ также открыл Институт кибербезопасности и защиты информации с первыми курсами по некоторым предметам, включая киберпсихологию, защиту от цифрового воспроизведения и тестирование на проникновение.[143] Институт также сотрудничает в проектах с отраслевыми партнерами, такими как LG, Bosch, Cisco, Huawei, «Газпром нефть», ГосНИИАС и АО «Трансмашхолдинг».[144]

Также следует отметить Университет информационных технологий, механики и оптики (ИТМО) в Санкт-Петербурге. С 2018 года Университет ИТМО также предлагает магистерскую программу по нейротехнологии и программной инженерии, которая руководит исследованиями в области технологий, включая ИИ, виртуальную реальность и дополненную реальность (VR/AR), интернет вещей (IoT) и технологии, используемые для изучения «мозга, нервной системы, сердечно-сосудистых, дыхательных и мышечных функций, а также движений глаз».

---

[140] Альманах искусственного интеллекта: Индекс ИИ 2019 – Россия.
[141] Там же.
[142] Там же.
[143] «Институт кибербезопасности открылся в Петербургском Политехе» TASS, июль 3, 2020, https://tass.ru/obschestvo/8879257; «В Политехе создан Институт кибербезопасности и защиты информации», июль 6, 2020, https://www.spbstu.ru/media/news/education/institute-cybersecurity-informationprotection-polytech.
[144] Там же.

Многие университетские программы ИИ сотрудничают с предприятиями отрасли, которые предоставляют студентам возможность применить полученные знания в реальных условиях с помощью выездных практикумов и стажировок.

В свою очередь, эти предприятия надеются привлечь некоторых из лучших, востребованных выпускников России для работы на полную ставку. Эти совместные образовательные программы включают телекоммуникационное программное обеспечение ИТМО и Nexign, программное обеспечение для нейротехнологий ИТМО и Robotrack, международную школу квантовых вычислений Росатома и Университета Сириус, а также двухгодичную магистерскую программу МФТИ «Цифровые технологии в бизнесе» с Мобильными телесистемами (МТС) и Бизнес-школой Сколково.[145]

Еще одним примером может служить ИТ-академия Samsung, которая проводит годичные курсы по ИИ, IoT и разработке мобильных приложений в 34 университетах по всей России, привлекая более 1000 студентов в год.

Эта симбиотическая связь между учебными заведениями и бизнесом также играет важную роль в удержании российских талантов и противодействии утечке мозгов в конкурирующие страны.

Новые программы и новые инициативы

Другие российские университеты, которые лидируют в области ИИ, включают Южный федеральный университет (ЮФУ), Уральский федеральный университет (УФУ) и Университет Иннополис.

---

[145] «Магистерская программа по нейротехнологии и программной инженерии получает корпоративный статус и предложит две новые специализации», Новости ИТМО, 29 июля 2020 г., https://news.itmo.ru/ru/education//news/9607/; «О нас», Роботрек, https://robotrack-rus.ru/o - nas/; МТС, МФТИ и СКОЛКОВО открывают магистерскую программу «Цифровые технологии в бизнесе» COMNEWS, 22 июля 2020 г., https://www.comnews.ru/content/208225/2020-07-22/2020-w30/mts-mfti-i-skolkovo-otkryvayut - магистратуру-цифровые технологии-бизнес; «Открыт набор на новую степень магистра МФТИ, СКОЛКОВО и МТС: «Цифровые технологии в бизнесе» МТС: «Цифровые технологии в бизнесе», МФТИ, ttps://mipt.ru/news/otkryt_nabor_na_novuyu_magistraturu_ot_mfti_skolkovo_i_mts_tsifrovye_ tekhnologii_v_biz nese; «Росатом и РКЦ запустили первую международную школу по квантовым вычислениям,» Росатом и RQC запустили первую международную школу по квантовым вычислениям, ТАСС, 14 сентября 2020 г., https://nauka.tass.ru/nauka/9447715.

В июле 2020 года СФУ и МФТИ совместно начали предлагать магистерскую программу под названием «Компьютерная математика: теория и приложения».[146]

В августе 2020 года ЮФУ объявил, что в 2021 году начнет предлагать магистерскую программу по ИТ-безопасности, состоящую из 22 дисциплин, в том числе «правовые аспекты информационной безопасности, организация защищенных сетевых коммуникаций, а также методы и инструменты анализа больших данных».

Эксперты МФТИ и Уральского центра систем безопасности будут оказывать помощь в обучающей программе.

Первый в России институт ИИ открылся в Татарстанском университете Иннополис в декабре 2020 года. Институт будет разрабатывать образовательные программы на уровне бакалавриата, магистратуры и аспирантуры, предлагая обучение по таким темам, как наука о данных, микроэлектроника ИИ и машинное обучение.[147]

Хотя все больше сельских регионов улучшают свои возможности для проведения высококачественных исследований в области ИИ, было отмечено, что многие из этих регионов, включая Дальний Восток, Иркутск и Татарстан, сталкиваются со значительной нехваткой технических экспертов, а также с развитием ИИ и сквозных технологий.[148]

Кремль подчеркнул необходимость создания новых образовательных центров и развития существующих, как в соответствии со своей целью увеличить число российских университетов в ведущих мировых рейтингах, так и в стремлении развивать высококачественные центры ИИ и технического образования по всей России.

---

[146] «ЮФУ и МФТИ реализуют совместную магистерскую программу для рынков Национальной технической инициативы», Южный федеральный университет, 22 июля 2020 г., https://www.sfedu.ru/www2/web/press-center/news/63261; НТИ Автонет, «О нас», Научно-конструкторское бюро вычислительных систем, https://autonet-nti.ru/en/autonet/; https://www.nkbvs.ru/en/o-firme.

[147] Владимир Бахур, «Первый институт ИИ в России был создан в кампусе Университета Иннополис» CNews, 10 декабря 2020 г., https://www.cnews.ru/news/line/2020-12-10_pervyj_v_rossii_institut; Владимир Бахур» «Университет Иннополис разработает платформу искусственного интеллекта для прогнозирования спроса», https://www.cnews.ru/news/line/2020-12-24_.

[148] Дмитрий Степнов, «Россия испытывает нехватку кадров в области искусственного интеллекта», Русская планета, 18 ноября 2020 года, https://rusplt.ru/society/rossiya-ispitivaetdefitsit-kadrov-5fb5464d.html.

В рамках своего национального проекта «Наука» Россия также намерена к 2021 году создать не менее 15 инновационных площадок мирового уровня, объединяющих науку и технологии.[149]

Приоритетными направлениями для этих центров являются ИИ, робототехника и цифровые технологии.[150]

В период с 2020 по 2022 год из федерального бюджета будет выделено 3,28 миллиарда рублей (43 миллиона долларов) в виде субсидий на поддержку этого проекта.

В 2020 году 721,1 миллиона рублей (10 миллионов долларов) поступило в Тюменский государственный университет, Белгородский государственный национальный исследовательский университет, Кемеровский государственный университет, Пермский федеральный исследовательский центр Уральского отделения Российской академии наук и Управляющую компанию РЭЦ из Нижегородской области.[151]

В соответствии с этим проектом Самарский научно-образовательный центр также уделяет особое внимание разработке новых инженерных систем на основе ИИ, двигательных и топливных систем нового поколения, а также интеллектуальных транспортных систем.[152]

В связи с возросшим спросом на технических специалистов, другие российские университеты недавно начали предлагать новые программы бакалавриата или магистратуры в различных областях ИИ или технологий.

Эти школы включают Институт цифровых технологий Марийского государственного университета, который открылся в июне 2020 года; магистерскую программу по новым наукам о данных и ИИ Института экономики, математики и информационных технологий РАНХИГС (EMIT);

---

[149] «Татьяна Голикова и Андрей Фурсенко провели заседание Совета научно-образовательных центров мирового уровня», Правительство России, 20 февраля 2020 г., http://government.ru/news/39005.

[150] «Правительство определило список получателей грантов среди научно-образовательных центров», D-Россия, 29 июня 2020 г.; «Утвержден список получателей грантов среди научно-образовательных центров», Правительство Российской Федерации, 27 июня 2020 г., http://government.ru/news/39940.

[151] «Правительство определило список получателей грантов среди научных и образовательных центров»; «Утвержден список получателей грантов среди научных и образовательных центров».

[152] «Самарский РЭЦ претендует на статус мирового класса», Regnum, 30 октября 2020 г., https://regnum.ru/news/innovatio/3103265.html.

курсы Департамента информационной и коммуникационной политики Новгородского государственного университета по интеллектуальному анализу данных и ИИ; курс новых нейронных сетей Тюменской школы программирования.[153]

Они также включают новую совместную образовательную программу по робототехнике между Пермским национальным исследовательским политехническим университетом (ПНИПУ), Санкт-Петербургским государственным электротехническим университетом (ЛЭТИ) и Казанским авиационным институтом.[154]

Часто федеральное правительство субсидирует создание этих программ путем прямого финансирования или оплаты обучения студентов.

В дополнение к своим усилиям по развитию университетов мирового класса, Кремль выдвинул ряд инициатив и учебных программ для развития потенциала своих ИТ-специалистов.

В правительственных отчетах и указах говорится о настоятельной необходимости обеспечить подготовку достаточно многочисленной и квалифицированной рабочей силы для удовлетворения потребностей будущего.

Согласно недавнему отчету Министерства образования, к 2022 году каждый пятый сотрудник, занимающийся «нестандартными задачами», будет использовать ИИ.[155]

Решая основные ИТ-проблемы России

Поэтому все большее число россиян должны развивать компетенции в том, как использовать ИИ и взаимодействовать с ним, а также в том, как разрабатывать инструменты на основе ИИ.

---

[153] «МАРГУ будет готовить специалистов в области цифровых технологий», Поток Медиа, 29 июня 2020 года, https://potokmedia.ru/news/198650/v-margu - будут-готовить-специалистов-в-области-цифровых технологий/; «Представители команды по науке о данных ВТБ говорят о профессиях будущего и объясняют, почему их банкам нужны выпускники РАНХИГС» Новости AI, 27 июля 2020 г., https://ai.

[154] «Пермский Политех продолжает прием студентов в первую в России сетевую онлайн-магистратуру по робототехнике», ПГТУ, 20 июля 2020 г., https://pstu.ru/news/2020/05/15/10556.

[155] «Основы искусственного интеллекта будут преподаваться в начальной школе».

Эти учебные инициативы организуются, осуществляются и финансируются рядом организаций, включая Национальную технологическую инициативу, Агентство стратегических инициатив (АСИ), некоммерческую организацию «Россия – страна возможностей», Фонд содействия инновациям, Фонд Президентских грантов и Союз молодых специалистов.

Программы, ориентированные на российскую молодежь

Программы, ориентированные на программы дополнительного обучения российской молодежи, которые могут быть использованы в классе, широко внедряются в учебные планы по всей России.

Одним из таких примеров является «Урок цифр» (который также можно перевести как «Урок чисел»), проект, начатый в 2018 году, организованный Министерством образования, Министерством цифрового развития, связи и массовых коммуникаций России и некоммерческой организацией (АНО) «Цифровая экономика».[156]

Курсы представлены в форме онлайн-игр, предназначенных для трех возрастных групп учащихся: учащихся начальной, средней и средней школ. В 2020-2021 годах курсовая работа включает уроки по ИИ и машинному обучению (в партнерстве со Sber), нейронным сетям и коммуникациям, социальным сетям (в партнерстве с @Mail.ru), кибербезопасность (в партнерстве с Лабораторией Касперского), беспилотные транспортные средства (в партнерстве с Яндексом) и цифровое производство (в партнерстве с Клубом программистов 1С). В конце каждого курса студенты получают сертификат.

Программа реализуется во всех 85 регионах России и недавно была доступна в 100 странах для русскоязычных студентов.

---

[156] «Принципы искусственного интеллекта будут изучаться школьниками Карачаево-Черкесии на «Цифровом уроке», «Интерфакс Россия, 11 сентября 2020 г., https://www.interfax-russia.ru/south-and-north - caucasus/news/principy-rabotyiskusstvennogo-intellekta-izuchat-shkolniki-karachaevo-cherkesii-na-uroke-cifry; «Всероссийский образовательный проект в области цифровой экономики», «Номера уроков, https://xn--h1adlhdnlo2c.xn--p1ai.

Кроме того, Министерство образования недавно приняло решение более регулярно проводить обучение ИИ в рамках учебной программы по информатике, при этом курсовые работы будут введены на экспериментальной основе уже в сентябре 2021 года.[157]

В дополнение к занятиям студентам и школьникам доступны различные внеклассные учебные мероприятия.

Одна из таких программ, Robotrack, с 2015 года разрабатывает клубы робототехники и технологий для детей в рамках Национальной технологической инициативы.[158]

Согласно его веб-сайту, Robotrack предлагает учебные курсы различной степени развития для детей в возрасте 4-6, 7-10, 11-14 и 15-17 лет. В общей сложности насчитывается 104 клуба в более чем 40 городах России и семи городах Казахстана.[159]

За пределами класса проводятся разнообразные мероприятия по ИИ, ориентированные на школьников, как правило, в формате начальной программы обучения, за которой следует какое-либо соревнование.

Одним из заметных событий является конкурс WorldSkills, который открыт для студентов в возрасте 16-22 лет (с версией WorldSkills для юниоров в возрасте 12-16 лет).[160]

Мероприятие состоит из 130 компетенций, ориентированных на семь секторов навыков: строительные технологии, информационные и коммуникационные технологии, производственные и инженерные технологии, социальные и персональные услуги, транспорт и логистика, образование, а также творчество и мода.

Секция информационных и коммуникационных технологий включает компетенции, включая разработку VR/AR, проектирование нейронных сетей,

---

[157] «Основы искусственного интеллекта будут преподаваться в начальной школе».
[158] «О нас».
[159] Там же.
[160] «WorldSkills Russia 2020», https://worldskills.ru/final2020.

машинное обучение и большие данные, кибербезопасность, технологию блокчейна и разработку приложений.[161]

Секция производственных и инженерных технологий мобильную робототехнику, интернет вещей и разработку космических систем.[162]

В конкурсе приняли участие более 2 800 участников. Еще одним таким событием является Юношеская олимпиада движения NTI Circle, инженерное соревнование с пятью технологическими направлениями области: виртуальная, роботизированная, космическая, среда обитания и нейротехнологии.

В нем приняли участие более 28 000 учащихся 5-7 классов.[163]

Программы для молодых специалистов и конкурсы для взрослых, ориентированные на более опытных и опытных экспертов в области ИИ, выполняют двойную функцию: оттачивают навыки участников, а также определяют жизнеспособные цифровые решения реальных проблем.

Такие мероприятия, как правило, частично финансируются корпоративными партнерами, которые извлекают выгоду из цифровых решений, разработанных участниками.

Во многих случаях призы за эти конкурсы включают стажировки или контракты с корпоративными спонсорами. Частыми спонсорами этих мероприятий являются Росатом, Ростех, Яндекс, Sber, Ростелеком, Газпром нефть, МТС и Мегафон.

Более крупные мероприятия проводятся поэтапно: сначала по всей России в отборочных региональных блоках, затем переходят к более мелким раундам финала.

К таким мероприятиям относятся фестивали интенсивного обучения ИИ и алгоритмическому программированию RuCode, которые проводились трижды в 2020 году и собрали более 20 000 участников.[164]

---

[161] Там же.
[162] Там же.
[163] «Об олимпиаде», Олимпиада по круговому движению НТИ, доступ к которому получен 7 января 2021 года, https://junior.nti-contest.ru/; Ксения Колесникова, «Объявлены победители Олимпиады Кружкового движения НТИ», Российская газета, 22 декабря 2020 г., https://rg.ru/2020/12/22/nazvany-pobediteliolimpiady-kruzhkovogo-dvizheniia-ntijunior.html.
[164] «О ФЕСТИВАЛЕ», RuCode, доступ к 31 января 2021 года, https://rucode.net.

Мероприятия бесплатны и доступны для всех – от студентов до экспертов на местах.

Первая часть этих онлайн-фестивалей состоит из бесплатных обучающих курсов, в том числе: «Быстрый старт для развлекательного программирования»,

«Быстрый старт для языка программирования C++» и «Быстрый старт для искусственного интеллекта». После образовательного этапа программы участники представляют проекты, которые решают реальные современные проблемы с использованием ИИ, и соревнуются в чемпионате по алгоритмическому программированию.[165]

Еще одним крупным конкурсом является мероприятие «Цифровой прорыв», где участники разрабатывают цифровые решения для задач в области образования, инфраструктуры и коммуникаций, цифровизация производства, большие данные и ИИ. В 2020 году отраслевыми партнерами стали «Ростелеком», Федеральная налоговая служба, Росстат, ПАО «Газпром нефть», Госкорпорация «Росатом», МТС и Мегафон.

Согласно веб-сайту Digital Breakthrough, было зарегистрировано 94 333 претендентов и создано более 4 700 цифровых помощников.

Общий призовой фонд конкурса достиг 50 миллионов рублей, при этом дополнительный грантовый фонд составил 100 миллионов рублей и более 2 000 победителей.

Призы за участие в гранд-финале включают предложения о работе, контракты и инвестиции в проекты.[166] В России также проводится ряд образовательных международных конференций по ИИ.

Крупнейшей из них была конференция Sber AI Journey, которая собрала более 9 000 участников в 2019 году и транслировалась более 1 миллиона раз в 2020 году.[167]

---

[165] Там же.

[166] «Крупнейшие хакатоны в России! – Финал» Цифровой прорыв, доступ к 30 ноября 2020 г., https://leadersofdigital.ru/#topics.

[167] «Сбербанк проведет онлайн-конференцию для школьников по искусственному интеллекту», ТАСС, 26 октября 2020 г., https://tass.ru/ekonomika/9821223, Путешествие по искусственному интеллекту, доступ к 30 ноября 2020 г., https://ai - journey.ru/en/about.

В 2020 году трехдневная конференция была посвящена темам науки, общества и регионов России.

Конференции предшествовал онлайн-конкурс из трех частей, в котором тестировалось компьютерное зрение, обработка естественного языка и наборы навыков построения графиков знаний.[168]

За ними последовала конференция «AI Journey Junior», которая была проведена для учащихся средних и старших классов.

Более обширный список российских конференций по ИИ приведен в Приложении В к настоящему отчету. Одной из заметных инициатив, направленных на обучение широкого круга людей, включая студентов, предпринимателей, руководителей служб обработки данных (CDO) и технологических лидеров, является Университет 20.35[169], основанный Национальной технологической инициативой. Университет 20.35. предлагает интенсивные 10-15-дневные курсы, а также индивидуальное обучение сроком до трех месяцев, где для каждого участника создается индивидуальный трек на основе его или ее опыта и желаемой конечной цели.[170]

Иногда также существуют бесплатные программы обучения для среднего взрослого россиянина, который еще не достиг пенсионного возраста. В 2020 году, после успешной реализации пробной версии в прошлом году, была запущена новая программа в рамках федерального проекта «Человеческие ресурсы для цифровой экономики», которая позволяет россиянам в 48 регионах проходить виртуальные курсы обучения.

После подачи заявки участники могут записаться на курс продолжительностью до 72 академических часов по любой из 22 компетенций, включая ИИ, кибербезопасность и защиту данных, программирование и создание ИТ-продуктов, цифровой маркетинг и 3D-производство. Участники

---

[168] «О компании»; «Сбербанк» проведет онлайн-конференцию для школьников по искусственному интеллекту».
[169] «РВК», https://www.rvc.ru/en/eco/education/2035_university/. С другими проектами Национальной технологической инициативы можно ознакомиться здесь: https://nti2035.ru/talents/circles.
[170] Там же.

получают сертификат по окончании курса. Программа бесплатна и финансируется из федерального бюджета.[171]

Влияние и перспективы

Такие проблемы, как нехватка рабочей силы, утечка мозгов, география, исторически низкие государственные инвестиции и сложные бюрократические препятствия, создают препятствия для желания России сравняться или превзойти других мировых лидеров в области ИИ.

В свете этих вызовов Кремль разработал ряд стратегических планов по повышению своего глобального авторитета в сфере ИИ, среди которых немалую роль играют учебные инициативы. Обучение молодежи, создание центров технического образования мирового уровня, а также создание и сохранение потенциала высококвалифицированных технических экспертов – все это является приоритетным направлением в недавних усилиях правительства по разработке ИИ.

Например, согласно Паспорту Федерального проекта ИИ за декабрь 2019 года Россия должна удвоить численность сообщества ИИ к 2024 году.[172]

Кроме того, она должна увеличить количество специалистов по ИИ, обучающихся в высших учебных заведениях, с 650 в год (по состоянию на 31 декабря 2019 года) до 4241 в год к 2024 году.

Россия может показаться чрезмерно амбициозной в попытке достичь этих и подобных целей, поставленных Кремлем в такие сжатые сроки.

Однако Россия демонстрирует четкую приоритетность развития своего потенциала в области исследований ИИ и внедрения цифровых решений на основе ИИ, что требует повышенного внимания со стороны Запада.

Если Россия добьется успеха в осуществлении этих реформ, предполагая продолжение инвестиций с течением времени, ее глобальный авторитет

---

[171] «Жители 48 регионов России получат персональные цифровые сертификаты» Известия, 15 октября 2020 г., https://iz.ru/1074361/2020-10-15 «Жители 48 регионов России получат персональные цифровые сертификаты», CNews, 15 октября 2020 г., https://cnews.ru/link/n516959, 2035, https://2035.university/en.

[172] Петрелла, Миллер и Купер, Стратегия искусственного интеллекта России.

и потенциал в области исследований и создания систем, использующих ИИ, будут постепенно расти, открывая возможности для потенциальной конкуренции с другими ведущими странами, занимающимися исследованиями ИИ.

Если Россия не сможет осуществить эти реформы, она продолжит бороться в глобальных рейтингах, за сохранение отечественных талантов и привлечение иностранных талантов, а также за достижение цифровизации.

ИИ ЧАСТНОГО СЕКТОРА В РОССИИ

Обзор

Технологические разработки и рост на российском частном рынке ИИ обусловлены в первую очередь научно-исследовательскими разработками, поддерживаемыми государством, хотя частный спрос на решения в области ИИ растет.

В целом, на частном рынке ИИ доминирует ориентация на использование достижений в области обработки естественного языка (NLP) и других форм автоматизированного анализа данных, хотя интерес к компьютерному зрению и другим типам возможностей распознавания быстро растет.[173]

Наиболее важными технологиями ИИ, которые привлекли внимание частного рынка за пределами широких автоматизированных приложений NLP для финансовых и розничных целей, являются программное обеспечение для распознавания лиц, безопасность объектов и периметра, беспилотные перевозки грузов и агробизнес, системы управления общественным транспортом и интеграция железнодорожной сети, автоматизированные платформы для обучения нейронных сетей и других протоколов ИИ, а также автоматизированный медицинский анализ.

Большинство усилий в области НИОКР по-прежнему поддерживаются или проводятся непосредственно государственными учреждениями

[173] Альманах Искусственный интеллект, «Индекс ИИ 2019 – Россия», Аналитический отчет Альманаха, № 4, (2019), https://aireport.ru/en/results2019.

и программами, но значительная часть мотивации со стороны спроса на частные исследования в области ИИ исходит также от российского государства, особенно в области общественной безопасности и транспорта, а также в областях, в которых доминирует государство, таких как здравоохранение.

Многие основные инвесторы являются государственными или ассоциированными банками и другими финансовыми корпорациями. Российское государство остро заинтересовано как в увеличении частных инвестиций, так и в доступе российских продуктов на международные ИТ-рынки.

Таким образом, государство активно стимулирует развитие стартапов и совместные инициативы как на этапе исследований и разработок, так и на этапе вывода продуктов на рынок.[174]

Национальная стратегия «Цифровая экономика» – часть обновленного пакета инвестиционных стратегий национальных программ – стала источником критической поддержки, финансирования и стимулом для дальнейшего развития ИИ в стране.[175]

Стратегия способствовала ряду крупных цифровых проектов по всей стране, прежде всего Фонд «Сколково», и стимулировал спрос государства на решения для цифровизации на основе ИИ для федеральных и региональных бюрократий.[176]

В рамках этой новой программной и финансовой системы было выделено большое количество ресурсов на ослабление барьеров для входа для новых частных участников ИИ, помощь в создании инфраструктуры поддержки, создание реестров отечественных фирм ИИ и другие усилия по уменьшению

---

[174] Ярослав Лисоволик, «Национальные проекты: новая парадигма развития России», Клуб «Валдай», 20 февраля 2020 г., https://valdaiclub.com/a/highlights/national-projects-russia-s-new-development.

[175] Указ Президента Российской Федерации № 490 «О развитии искусственного интеллекта в Российской Федерации» от 10 октября 2019 года, http://www.garant.ru/products/ipo/prime/doc/72738946/; Петрелла, Миллер и Купер, российская стратегия искусственного интеллекта.

[176] Указ Президента Российской Федерации № 490 «О развитии искусственного интеллекта в Российской Федерации» от 10 октября 2019 года, http://www.garant.ru/products/ipo/prime/doc/72738946/; Петрелла, Миллер и Купер, российская стратегия искусственного интеллекта.

проблем с информацией, сотрудничеством и расширением масштабов в частном секторе.

Хотя российская экономика по-прежнему подвергается серьезному уравновешивающему давлению государственной коррупции и нерационального использования ресурсов, тенденции к дальнейшему росту и развитию очевидны.

Ориентация на ИИ на национальном уровне как на ключевой сектор роста, концентрация значительной политической воли и широкие интересы государства и бизнеса в интеграции внутреннего рынка с экспортными возможностями и возможностями сотрудничества за рубежом означают, что частные субъекты нашли относительно более благоприятные условия, чем в других секторах российской экономики.

Структура

Подавляющее большинство российских исследований и разработок в области ИИ проводится в государственных фирмах, при этом крупнейшая технологическая компания страны Яндекс несколько отстранена в этой сфере из-за напряженности в отношениях с правительством.[177]

Таким образом, в отличие от США и Китая, где сотрудничество между государственным и частным секторами принесло большие успехи, российское правительство предпочло держать разработку ИИ близко, в первую очередь доверяя эти усилия государственным компаниям.

Большая часть исследований и разработок в области ИИ поступает из государственных источников и в основном направляется через Фонд «Сколково» и его дочерние компании, ассоциированные организации и учреждения-грантополучатели.

Запланированный как новая российская «Силиконовая долина» при Президенте Медведеве, он переориентировался как крупный

[177] Эван Гершкович, «Нелегкое сосуществование Яндекса и Кремля», Обзор технологий, 19 августа 2020 г., https://www.technologyreview.com/2020/08/19/1006438/yandex-putin-arkady-volozh-kremlin.

институциональный сайт для финансирования и размещения технологических стартапов, физическое предприятие для молодых разработчиков и координирующая организация, оказывающая поддержку в интеграции стартапов на более широкие международные рынки.[178]

Помимо предоставления скоординированных потоков финансирования и грантов, в течение 2020 года «Сколково» организовало или спонсировало несколько профессиональных и любительских конкурсов, выставок, конференций и других совместных и конкурентных форумов, все с целью поддержки российских отечественных стартапов в области ИИ и преодоления разрыва между исследованиями и разработками и рыночными приложениями.[179]

Учитывая относительный размер российской области ИИ по сравнению с западными и китайскими конкурентами, эти площадки были особенно важны для стимулирования инноваций и сотрудничества, популяризации исследований и новых продуктов, и облегчение связей с лучше финансируемыми программами за рубежом.

Сеть «Сколково» не ограничивается опорой на потоки и программы государственного финансирования, однако инвестиции частного сектора теперь также направляются через «Сколково».

Это в первую очередь связано с его координирующей ролью и с учетом важности учреждения в организации конференций, дружеских соревнований и размещении центров фундаментальных исследований, таких как AI Journey.[180]

Растущая важность интернет-платформ для оказания помощи в тестировании и обучении алгоритмов ИИ также удерживает Сколково в центре инфраструктуры развития ИИ в России.

Многие стартапы и новые исследовательские платформы полагаются на арендуемую или совместно используемую инфраструктуру обработки,

---

[178] Игорь Дроздов, «Фонд «Сколково»: содействие инновациям и предпринимательству в Российской Федерации», Журнал ВОИС, сентябрь 2020 г., https://www.wipo.int/wipo_magazine/en/2020/03/article_0007.html - «Что такое Сколково?», Фонд «Сколково», https://old.sk.ru/foundation/about.

[179] «В Москве пройдет интенсивный курс по подготовке проектов и стартапов в области ИИ», Контент - Review.com, 23 октября 2020 года, http://www.content-review.com/articles/51402, «Первая платформа для сбора данных исследований была представлена на «Архипелаге 20.35.», ТАССНАУКА, ноябрь. 16, 2020, https://nauka.tass.ru/ nauka/ 10018715.

[180] «Путешествие искусственного интеллекта», Путешествие ИИ, https://ai - journey.ru/en.

отечественные версии которой часто предоставляются или размещаются через Сколково, например, новый суперкомпьютер Christofari, разработанный совместно Sber и Nvidia.[181]

Помимо Сколково, в кластерах государственных университетов существуют значительные исследовательские центры, особенно МФТИ, Высшая школа экономики (ВШЭ) и Дальневосточный федеральный университет (ДВФУ).

Эти центры получают значительную государственную поддержку, но также широко используются частными субъекты рынка и инвесторы.

Тесное сотрудничество с государственными фирмами, такими как Sber, Газпромбанк, Росатом и Ростех, также помогло стимулировать эти все более одаренные центры научных и правительственных исследований и разработок напрямую взаимодействовать с приоритетами корпоративного и потребительского рынка.[182]

Как отметил Элер, Sber является пионером в области разработки ИИ в России. Он имеет обширные государственные и частные деловые связи, а также растущее участие в координации научных исследований, частных инвестиций и международных интересов в рамках совместных проектов.[183]

Компания уже давно инвестирует в технологии, чтобы диверсифицировать свои предложения и повысить свою банковскую и финансовую эффективность.

Он рано признал, что ИИ может оказаться полезным для этих целей, и инвестировал средства в разработку соответствующих технологий (включая обработку данных) для собственного использования. Sber также находится на переднем крае развития российской экосистемы ИИ в целом, возглавляя усилия правительства в этой области.

---

[181] «Сбербанк и SberCloud открывают свое суперкомпьютерное облако для всех разработчиков», CNews, 4 декабря 2020 г., https://www.cnews.ru/news/top/2020-12-04, «Сбербанк планирует открыть первый в России институт искусственного интеллекта», ТАСС, 3 декабря 2020 года, https://tass.com/economy/1230907.

[182] Оборонная промышленность и политическая экономия России: российская «Программа цифровой экономики» и Повестка Кремля в области информационной безопасности, Программа FPRI Евразия, сентябрь 2020 г.

[183] См. обсуждения в выпуске «ИИ в России» № 17 (стр.20-21) среди прочих.

Как обсуждалось ранее, правительство возложило на Sber особенно большую роль в разработке нынешней нормативно-правовой базы ИИ.[184] Хотя когда-то это была слабая, сильно бюрократизированная организация советской эпохи.

В настоящее время Sber рассматривается в России как пример того, как инновации могут привести к повышению эффективности, а лояльность его генерального директора Германа Грефа Кремлю, вероятно, способствовала тому, что Sber занял лидирующую роль в развитии ИИ в России.[185]

Несмотря на очевидные преимущества ИИ в военном секторе, Ростех, государственный оборонный гигант, сыграл менее заметную роль в развитии ИИ с точки зрения частного рынка.

В рамках Программы цифровой экономики Ростех несет ответственность за ряд дорожных карт, включая 5G, блокчейн и «Интернет вещей», но не имеет официального роль в разработке ИИ.[186]

Организация работает над рядом технологий ИИ, включая распознавание лиц в гражданском секторе и интеграцию ИИ в военные системы, такие как системы радиоэлектронной борьбы, но не занимает видного места в создании официальной стратегии государства в области ИИ.[187]

Аналогичным образом, государственные энергетические компании, такие как «Газпром нефть» и «Лукойл», работают над разработкой и интеграцией ИИ, имеющих отношение к нефтегазовой отрасли, хотя сами они не занимают видного места в общих планах развития ИИ в России.

Скорее, правительство разрешило этим компаниям разрабатывать технологии ИИ для содействия производству, что, в свою очередь, позволит России более эффективно конкурировать на мировых рынках.

---

[184] «Сбербанк объяснил государству, как потратить 120 миллиардов долларов на искусственный интеллект».
[185] Петрелла, Миллер и Купер, Стратегия России в области искусственного интеллекта.
[186] «Правительство России утвердило дорожную карту развития 5G»; «Интернет ненужных вещей»; «Деньги за цифру».
[187] Felix Light, «Россия строит одну из крупнейших в мире сетей распознавания лиц», Moscow Times, 12 ноября 2019 г., https://www.themoscowtimes.com/2019/11/12/russia-building-one-of-worlds-largestfacial-recognition - сети - a68139; «Ростех разрабатывает боевое Снаряжение 4-го Поколения», Rostec.ru, 29 января 2021 года, https://rostec.ru/en/news/rostec-develops-4th-generation-combat-gear/; «Пехота: Ратник, Сотник И Плащи-Невидимки», StrategyPage.com, август. 9, 2020, https://www.strategypage.com/htmw/htinf/20200809.aspx.

Например, «Газпромнефть» с 2012 года проводит инициативу «Развитие электронных активов», которая поддерживает разработку собственного программного обеспечения для использования методов машинного обучения для оценки наиболее эффективных способов разработки новых и зрелых нефтяных месторождений.[188]

Однако введение Западом санкций в отношении этих компаний в некоторой степени затруднило эти усилия, затруднив установление международных партнерских отношений.[189]

Таким образом, частная экосистема ИИ на удивление энергична, учитывая ее небольшую долю в общем развитии технологий ИИ во всем мире и проблемы российской экономики.

Частные инвестиции в развитие ИИ в России остаются низкими по сравнению с устоявшимися инвестиционными экосистемами в Европе, Соединенных Штатах и Восточной Азии.

В то же время он быстро растет с этого сравнительно низкого уровня. По данным IDC, российские частные инвестиции в ИИ в 2019 году составили 172,5 миллиона долларов, при ожидаемом росте примерно на 23%.

Большая часть частных инвестиций по-прежнему сосредоточена на серверах, ИТ-услугах и приложениях ИИ, особенно в финансовом секторе и розничной торговле.[190]

Крупные частные технологические компании оказываются в значительной степени отстраненными от официальных усилий правительства по развитию российского сектора ИИ.

В то время как Яндекс разработал некоторые продукты ИИ, в том числе виртуальный помощник, подобный Siri, под названием «Алиса», который

---

[188] «Как искусственный интеллект находит месторождения», Газпром нефть Пресс, 31 октября 2018 г., https://www.gazprom-neft.com/press-center/lib/2152397.

[189] Конаев и Данэм, Российские исследования ИИ с 2010 по 2018 год: Темы, тенденции и институты; «Шелл выходит из предлагаемого совместного предприятия Мертояханефтегаза с «Газпром нефтью»», NS Energy, апрель. 14 декабря 2020 года, https://www.nsenergybusiness.com/news/shell-exit-meretoyakhaneftegaz-jv.

[190] Андреа Минонне, Дэвид Шубмель и Такаши Манабе, «Мировое руководство по расходам на искусственный интеллект», Международная корпорация данных, 2020 год, https://www.idc.com/getdoc.jsp?containerId=IDC_P33198.

использует алгоритмы ИИ, организация в целом отошла на второй план перед Sber в создании экосистемы ИИ в России.

Российское правительство относится к Яндексу с подозрением из-за его частной собственности, и Путин ранее предположил, что американцы приложили руку к созданию компании. В 2019 году Яндекс заключил сделку, которая реструктурировала компанию и предоставила право вето на основные решения группе, связанной с Кремлем, что, вероятно, повысит государственный надзор в компании и позволит Кремлю поддерживать тесную связь с крупной российской технологической компанией.[191]

Несмотря на эти несколько напряженные отношения, Яндекс, наряду с другими крупными компаниями, такими как Mail.ru, «Газпром нефть», МТС, RFDI сформировали «Альянс AI-Россия», который успешно обеспечивает обратную связь для правительственных инициатив.

Другие крупные технологические и смежные с ними компании с точки зрения выручки в России включают Лабораторию Касперского, Avito и Yota. Относительная нехватка участия частного бизнеса в разработке ИИ в России может оказать серьезное влияние на инновации, поскольку государственным фирмам, как правило, не хватает конкурентного давления, обычно необходимого для быстрого прорыва.

Организации, связанные с правительством, также подвержены прихотям политики, как видно из ареста Александра Повалко, главы российской венчурной компании, поддерживаемой государством. В июне 2020 года его арестовали по обвинению в мошенничестве. Этот тип присущего политическому риску может помешать потенциальным новаторам присоединиться к работе на местах и улучшить процесс разработки. Поэтому тот факт, что государственные фирмы несут основную ответственность за разработку и внедрение ИИ, безусловно, способствует тому, что в будущем российские усилия будут отставать от усилий других крупных государств.

---

[191] Макс Седдон, «Яндекс координирует реструктуризацию с Кремлем», Financial Times, ноябрь. 18, 2019, https://www.ft.com/content/999e3ca6-09db-11ea-bb52-34c8d9dc6d84.

Процессы

Рост стартапов в России значительно возрос за последние несколько лет, и это напрямую связано с формированием согласованной государственной политики в области исследований и разработок в области ИИ и поддержкой частного рынка.

Мало того, что гранты и другие источники финансирования развиты лучше, чем в предыдущие годы, но и значительные средства были вложены в конкурсы, конференции и другие направления исследований, которые привели как к эффективности, так и к инновациям.[192]

Хотя эти источники, безусловно, все еще ограничены, учитывая сохраняющуюся слабость альтернатив частного венчурного капитала, российские аналитики отмечают, что «как движущая сила цифровых изменений (стартапы) более типичны для развитых регионов».[193]

Некоторые утверждают, что продвижение государственно-частных центров для инвестиций и развития может быть неэффективным, и хотя это приводит к неравномерному распределению концентрации стартапов по регионам, у него есть потенциал для создания ядер компетенций, которые могут быть использованы по мере дальнейшего развития более широкой инфраструктурной экосистемы ИИ.[194]

Кроме того, учитывая тенденцию к кластерным моделям в технологической отрасли в целом, неясно, не компенсируются ли потери от неэффективности концентрированным человеческим и инфраструктурным капиталом в краткосрочной и среднесрочной перспективе, особенно при попытке решить проблемы «утечки мозгов» в России.[195] Что еще более важно, крупные отечественные и международные компании в настоящее время

---

[192] Обратите внимание, что довольно небольшие частные организации венчурного капитала только начинают появляться, см., Например: «Запуск закрытого частного клуба венчурного капитала Digital Disrupt», Советник ТА, 3 декабря 2020 г., https://www.tadviser.ru/index.php F.

[193] Центр Гайдара, Российская экономика в 2019 году Тенденции и перспективы, стр.480.

[194] Оцифруйте это: Поможет ли Национальный план создать Собственную Силиконовую долину в России?

[195] Роберт Кобза, «Проблема людей в России», Обзор исследований безопасности Джорджтауна, апрель. 6, 2020, https://Georgetown security studiesreview.org/2020/04/06/russias-people-problem.

регулярно посещают спонсируемые выставки новых технологий ИИ, которые, в свою очередь, создают новые возможности для разработки продуктов и дальнейшего выявления актуальных потребностей рынка.

Это увеличение контактов с международными компаниями, а также более последовательные оценки фактического состояния частного рынка внутри страны, вероятно, со временем принесут значительные выгоды за счет решения проблем координации между институциональными инвесторами и улучшения инвестиционного климата в целом.

Это было ускорено экзогенным шоком, вызванным кризисом COVID-19. Российские исследователи ИИ и технологические предприниматели быстро нашли инновационное применение ИИ.

Они включают в себя новые функции общественной безопасности с использованием программного обеспечения для распознавания лиц, которые теперь интегрированы в плотную сеть камер видеонаблюдения в крупных городах России, а также использование передовых алгоритмов нейросетевых изображений для обработки медицинских данных, особенно изображений легких, которые, как было установлено, помогают в диагностике и прогнозировании COVID-19.[196]

В самой Москве в настоящее время установлено более 100 000 камер видеонаблюдения высокого разрешения в сложной сети, которая позволяет легко интегрировать новое программное обеспечение для ИИ.

Технология распознавания лиц была в центре внимания всех участников российской экосистемы ИИ, от государственных тендеров до программ исследований и разработок в области ИИ и разработчиков до частных компаний, стремящихся вывести продукты на рынок.

---

[196] «Москва расширит свой эксперимент по внедрению искусственного интеллекта в медицине», Lenta.ru, 24 ноября 2020 года, https://lenta.ru/news/2020/11/24/med/; «Власти Москвы решили расширить число медицинских приложений искусственного интеллекта до 10», D-Россия, 26 ноября 2020 г., https://d-russia.ru/vlasti-moskvy-reshili-rasshirit-do-10-chislo-medicinskih-primenenij-ii.html-«Искусственный интеллект помогает проверить 500 000 компьютерных томографов на COVID-19 в Москве», ТАСС, 25 ноября 2020 г., https://tass.com/society/1227967.

Технология распознавания лиц, имеющая важное значение для наблюдения, контроля доступа к инфраструктуре и услугам, а также для домашних устройств, имеет множество приложений, которые стимулируются значительным государственным и частным спросом.

От автоматизированного доступа в Московское метро до процедур блокировки COVID-19, распознавание лиц, вероятно, станет основным источником постоянных инноваций.

Интеграция в уже существующие режимы видеонаблюдения в Москве и других крупных городах России стала сравнительным успехом в ответных мерах России на COVID-19 с явными последствиями для безопасности за пределами пандемии.[197]

Российское правительство не стесняется простого двойного назначения – включения передовых алгоритмов ИИ для распознавания лиц в и без того обширную инфраструктуру наблюдения.

Следует ожидать, что нынешняя система, поставляемая российским стартапом NtechLab в Москву – первоначально созданная для содействия полицейским расследованиям, а теперь измененная для обеспечения карантинных блокировок – будет использоваться для контрразведки и внутриполитического наблюдения, чего аналитики давно ожидали.[198]

О новых развертываниях систем распознавания лиц для использования против протестных движений, выступающих за освобождение лидера оппозиции Алексея Навального, например, уже сообщалось в международных СМИ.

Продвижение процессов цифровизации и поощрение нового частного предпринимательства имеют то преимущество, что являются прямой целью крупных государственных программ.

---

[197] Патрик Ривелл, «Как Россия использует распознавание лиц для защиты от коронавируса», ABC News, 30 апреля 2020 г., https://abcnews.go.com/International/ - блокировка/история id-70299736.

[198] Дженна Маклафлин и Зак Дорфман, Разрушенный: Внутри секретной битвы за спасение американских шпионов под прикрытием в цифровую эпоху», 30 декабря 2019 г., https://news.yahoo.com/shattered-inside-the-secret-battle-to-save-americas-undercover-spies-in-the-digital-age-100029026.html.

Государственная поддержка в рамках «Цифровой экономики», включая гранты в размере до 20 миллионов рублей для стартапов и до 300 миллионов рублей для крупных инициатив, направленных на цифровизацию проектов, была хорошо приспособлена для решения проблем в инвестиционной инфраструктуре и инфраструктуре развития, хотя проблемы по-прежнему отмечаются из-за задержек в расходах на региональном уровне, даже с учетом наличия федеральных средств.[199]

Как отмечалось выше, правительство Москвы, в частности, впервые внедрило многие формы интеграции ИИ в государственные процедуры и внутренние проекты цифровизации, что также стимулировало разработку новых продуктов стартапами частного рынка.

Таким образом, Москва является важным фактором увеличения совокупного спроса на продукты ИИ, что, вероятно, продолжит приводить к самым большим новым достижениям частного рынка в области изображений и NLP.

Ключевые технологии и инициативы

Особенно сильный рост наблюдается в областях коммерческого банковского дела, розничной торговли и отраслях, которые используют обработку естественного языка ИИ для анализа больших объемов неструктурированных данных; это особенно относится к закупкам, бухгалтерскому учету, персоналу и службам поддержки клиентов.[200]

Например, согласно визуализационной «карте» российской экосистемы ИИ, разработанной МФТИ (интерактивный веб-сайт можно найти по адресу http://airussia.online/titul), всего по состоянию на февраль 2021 года насчитывается 420 компаний.

---

[199] Владимир Козлов, «Национальная программа России по цифровой экономике спотыкается», BNE Intellinews, 4 сентября 2020 г., https://www.intellinews.com/russia-s-national-program-for-digital-economy-stumbles-188718.

[200] «В 2021 году российский рынок искусственного интеллекта вернется к двузначным темпам роста», CRN, 2 сентября 2020 года, https://www.crn.ru/news/detail.php?ID=147880; «Рынок Искусственного Интеллекта Растет В Условиях Пандемии», Volbusiness.ru, 13 августа 2020 года, http://www.volbusiness.ru/news-page/13045.

Количество компаний по кластерам их усилий выглядит следующим образом, хотя обратите внимание, что существует некоторый двойной подсчет более крупных компаний, таких как Яндекс, который осуществляет проекты в нескольких различных областях, таких как NLP и анализ данных).[201]

Многие ключевые технологии предполагают использование больших объемов данных изображений либо для автоматизированной обработки, либо для управляющих машин.

В первом случае это имело особое значение для сети видеонаблюдения «Умный город», которая была развернута в Москве и продвигается в других регионах.[202]

Эта сеть позволяет повысить автоматизацию городского движения, доступа к общественному транспорту, безопасности периметра и различных гражданских услуг, таких как коммунальные платежи.

Хотя эти проекты финансируются государством, они поставляются частными поставщиками, которые затем также используют технологию ИИ для других продуктов частного рынка, таких как отечественные технологии виртуальных помощников.[203]

Интересно, что доминирование областей, связанных с компьютерным зрением, распознаванием образов и обработкой естественного языка, тесно связано с соответствующими публикациями по ИИ, подготовленными российскими исследователями, как сообщают Конаев и Данэм.[204]

Многие виды использования ИИ в частном секторе относятся к области самоуправляемых транспортных средств, которые используются для управления транспортными потоками на грузовых верфях; в сетях общественного транспорта; для новых достижений в области самоуправляемых

[201] Эти данные взяты из http://airussia.online/#titul, дата обращения 23 февраля 2021 года.
[202] Мария Становая, Аналитический отчет «Политика», Бюллетень № 1 (65), Политик, 12 января 2021 г., стр.18-19. Смотрите также отчет «ИИ в России» № 9 (стр.4-5) о программах «Безопасный город», которые, в частности, стимулируют разработку продуктов видеонаблюдения.
[203] См. обсуждения в отчетах «ИИ в России» № 14 (стр.8-9), №15 (стр.9) и № 19 (стр.12) среди прочих.
[204] Конаев и Данхэм, Российские исследования ИИ с 2010 по 2018 год: Темы, тенденции и институты, стр.8.

сельскохозяйственных комбайнов, которые начинают конкурировать на международном рынке агробизнеса.[205]

Например, компания Cognitive Pilot, совместное предприятие Sber и Cognitive Technologies, является одним из примеров успешного маркетолога беспилотных систем в области сельского хозяйства. Sber, Яндекс и другие компании также занимаются самоуправляемыми транспортными средствами. Кроме того, существует множество компаний, больших и малых, занимающихся разработкой беспилотных летательных аппаратов различных размеров для государственных, промышленных и коммерческих применений.

Как отмечалось выше, наблюдается значительный рост решений для распознавания лиц и распознавания изображений, особенно в свете необходимости управления медицинскими данными во время пандемии COVID-19, а также множества компаний и стартапов, работающих в области анализа медицинских изображений.

С этой целью была проделана большая работа по автоматизированному компьютерному зрению и изображениям, программному обеспечению распознавания и анализу больших данных с помощью машинного обучения для обработки огромного количества изображений и видеоданных, создаваемых существующей инфраструктурой камер.

Российское правительство более целостно относится к своим ключевым направлениям поддержки развития частного ИИ, даже если в настоящее время экосистема наиболее многообещающе развивается в направлении беспилотных летательных аппаратов транспортные средства, распознавание и анализ изображений, а также цифровизация бизнес-процессов. Федеральный проект ИИ 2020 года определяет следующие приоритеты развития ИИ:

- В здравоохранении ИИ может использоваться для бизнес-процессов; оцифровка, повышение качества и аналитика данных; построение прогнозных моделей для помощи в диагностике и прогнозировании.[206]

[205] См. Обсуждение ИИ в российском сельском хозяйстве в отчете «ИИ в России» № 15 (стр.17-18).
[206] Краткое изложение Федерального проекта ИИ, 27 августа 2020 г., доступ к 22 февраля 2021 г.

- На транспорте цель – инструменты с поддержкой ИИ для создания «единой цифровой транспортно-логистической среды (в том числе с точки зрения обеспечения функционирования магистральной сети транспортно-логистических центров)»; внедрение управления объектами транспортной инфраструктуры информационными системами с использованием биометрических данных с элементами ИИ; оснащение беспилотных транспортных средств системами с улучшенным ИИ, обеспечивающими их использование в качестве мобильных постов транспортной безопасности (диспетчеров) в инфраструктуре общественного транспорта».[207]
- В сельском хозяйстве основное внимание уделяется данным, связанным с почвой и конкретными отраслями промышленности. Он включает в себя «классификацию типов сельскохозяйственных культур, оценку состояния сельскохозяйственных культур (мониторинг урожая, оценка ущерба), оценку урожайности, отображение характеристик и типов почвы, эрозию почвы, многоспектральные изображения, стереофотосъемку, визуализацию земель в любых погодных условиях, трехмерную структуру леса, высоту поверхности земли и объектов.[208]
- В топливно-энергетической промышленности: «будет оказана поддержка внедрению ИИ в промышленных компаниях. В частности, ИИ будет использоваться для создания модернизированной технологии интерпретации сейсмических данных, методологии комплексной интерпретации данных геоинформационной системы, системы моделирования ресурсов нефтяных и газовых месторождений для выявления перспективных объектов, технологии геологического моделирования для учета и автоматического обновления геологических и физических данных, модуля ИИ для прогнозирования, добычи и движения нефтепродуктов в нефтяной промышленности на цифровой платформе GIS TEK для нефтяных компаний».[209]

---

[207] Там же.
[208] Там же.
[209] Там же.

В отношении производства, в наброске отмечается, что «решения ИИ также будут внедрены в деятельность федеральных органов исполнительной власти.

В частности, будет создан модуль самообучающейся системы распознавания неструктурированного текста и интеллектуальной классификации, который поможет оптимизировать процедуру предоставления государственных услуг».

Кроме того, «Вспомогательные мероприятия включают создание центра компетенций для цифровой трансформации промышленности, обеспечивающего агрегирование и анализ отраслевых данных, переподготовку и тиражирование лучших практик и решений в области сквозных цифровых технологий и искусственного интеллекта».[210]

Проблемы ИИ частного сектора в России

Хотя Россия по-прежнему сталкивается со значительным негативным давлением в отношении свободы частного бизнеса от политического вмешательства и поддержания верховенства закона в условиях широко распространенной и глубокой коррупции, сфера ИИ была более изолирована от этих проблем, чем другие секторы.

Отчасти это объясняется тем, что она остается небольшой, развивающейся областью, в которой много стартапов, но мало крупных, быстрорастущих и высокорентабельных бывших стартапов.

Еще одна причина заключается в том, что из-за онлайн-характера большей части работы относительно легко вести бизнес виртуально или в небольших офисах, а не в централизованных центрах.

Это относится ко всему постсоветскому пространству, где цифровые сектора в Украине и Беларуси были относительно изолированы от затрат, связанных с коррупцией и неравномерным правоприменением, из-за широкой доступности быстрых подключений к Интернету и вычислительной мощности,

[210] Краткое описание Федерального проекта ИИ, 27 августа 2020 г., доступ к 22 февраля 2021 г.

ограниченной потребности в физической инфраструктуре или дорогостоящем присутствии, подлежащем лицензированию и регулированию, и возможности резервного копирования IP-адресов и других выходных данных через иностранные серверы.[211]

Наконец, российское государство проявляет значительный интерес к области технологий ИИИ как к сфере, в которой «наверстывание упущенного» необходимо для обеспечения безопасности и экономических целей.

Он хочет оцифровать российскую бюрократию по соображениям эффективности и борьбы с коррупцией, а также по причинам, основанным на экономической и иностранной конкуренции.

Этот интерес привел к значительной государственной поддержке в виде экосистемы грантов, исследовательских институтов, университетов и поддерживаемых государством программ, призванных упростить и упростить разработку стартапов и тестирование продуктов. Хотя существуют значительные сомнения в подлинности и правдивости заявлений российского правительства о коррупции, несомненно, верно, что бюрократическая инертность и неэффективность по-прежнему вызывают значительное раздражение у руководства режима.[212]

Нынешний премьер-министр России Михаил Мишустин хорошо известен как технократическая фигура, способная сбалансировать потребности коррумпированного высшего порядка – политическая система, стремящаяся к бюрократическим и процедурным реформам между государством и обществом с целью повышения аполитичной эффективности.[213]

---

[211] Татьяна Тищук и Андрей Кириленко, От наследия к цифровым технологиям: Подключенная экономика Украины, Voxukraine, https://voxukraine.org/longreads/plugged-in-economy/index-eng.html; Марк Хиллари, «Что Беларусь предлагает технологическому сектору», 4 апреля 2018 г., https://www.computerweekly.com/opinion/What-Belarus-offers-the-tech-sector.

[212] Чен Чен, «Что стоит за борьбой с коррупцией? Сравнение России и Китая, «Коммунистические и посткоммунистические исследования 53, № 4 (2020); Ноа Бакли, Коррупция и политическая власть в России, Институт исследований внешней политики, 2018, https://www. fpri.org/wp-content/uploads/2018/04/buckley.pdf.

[213] См. Крис Джайлс, «Роль России в создании налоговика будущего», Financial Times, 19 июля 2019 г., https://www.ft.com/content/38967766-aec8-11e9-8030-530adfa879c2.and Леонид Бершидский, «Новый премьер-министр России – бюрократический супермен», Moscow Times, 16 января 2020 г., https://www.the Moscow times. Com/2020/01/16/russias-new-prime-minister-is-a-bureaucratic-superman – a68935.

С этой целью программы ИИ российского государства, безусловно, попадают в последний лагерь, особенно с учетом их в настоящее время небольшой рыночной стоимости по сравнению с энергетическим сектором. Поскольку существуют возможности для негативного давления со стороны государственных субъектов, существует сильное противодействующее давление с самого верха, особенно когда общественные интересы и сообщения в прессе наиболее эффективны.

Тем не менее, проблемы с верховенством закона сохраняются, поскольку как кумовство, так и коррупция влияют на институты и программы, которые обеспечивают исследования и разработки для последующего использования в продуктах для частного сектора.[214]

Еще одной проблемой остается постоянная зависимость от государственного финансирования, спонсорства и поддержки в области ИИ. Хотя государственная поддержка была необходима для обеспечения базовой инфраструктуры и экономических условий для инноваций и производства, она все еще не является зрелой системой конкурирующих венчурных фондов.

Разработчики ИИ в России продолжают чрезмерно полагаться на процессы, подверженные бюрократической инерции, дублированию, неэффективности и манипуляциям, даже если государство официально выступает за оптимизацию таких операций. Кроме того, полагаться на российское государство означает полагаться на ограниченный бюджетом источник средств, который не сможет финансировать все потенциальные стартапы в области ИИ и созданные предприятия. Частный капитал необходимо будет интегрировать в эту область, если мы хотим добиться экономии за счет масштаба, придерживаться более агрессивных графиков развития и поощрять большое число новых компаний.

Военный ИИ и автономия в России

[214] С.С. Донецкая, «Исследование коррупции в российских университетах», Проблемы экономического перехода 59, № 7-9, https://www.tandfonline.com/doi/full/10.1080/10611991.2017.1394746.

С момента запуска программы модернизации в 2009 году российские вооруженные силы быстро развивались, неуклонно интегрируя уроки, извлеченные из наблюдений за иностранными военными, своих исследований и разработок, а также своих недавних боевых операций, особенно операций в Сирии.

Российские военные в значительной степени подчеркивают автономность разработок в области воздушных, наземных и морских беспилотных и роботизированных платформ и компонентов.

В то время как он работает над развитием технических возможностей для более эффективного использования беспилотные системы, российские стратеги продолжают обсуждать и размышлять о природе современной и будущей войны и о том, как будут представлены улучшенные ИИ и автономные системы.

Одновременно с разработкой военных беспилотных систем Министерство обороны начало вкладывать значительные людские и материальные ресурсы в развитие ИИ.

Связь ИИ и беспилотных систем представляет особый интерес для Министерства обороны, поскольку оно стремится учиться на сирийском и украинском боевом опыте для формулирования и концептуализации будущей войны.[215]

С Президентом России Владимиром Путиным и Министром обороны Сергеем Шойгу, призывающими Россию начать интеграцию ИИ в военные системы, отечественная оборонно-промышленная экосистема отвечает концепциями, испытаниями и технологиями, направленными на то, чтобы Россия стала одной из ведущих держав в этой новой военно-технологической гонке.

[215] Лестер Грау и Чак Бартлз, «Интеграция беспилотных авиационных систем в российскую артиллерию», Пожары: Совместное Публикация для профессионалов артиллерии США, нет. Июль-август (2016).

РОЛЬ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ВООРУЖЕННЫХ СИЛАХ РОССИИ

Российское политическое и военное руководство, стратеги и ключевые деятели отрасли активно обсуждают роль ИИ в будущем вооруженных конфликтов и роль, которую он должен играть в вооруженных силах России.

Как и в других странах, изучающих возможности ИИ и автономии, технологические и военные экосистемы России планируют, чтобы ИИ управлял информацией и расширял пространство для миссий.

В апреле 2021 года Министерство обороны России объявило, что намерено создать специализированный отдел в рамках Министерства обороны для разработки ИИ.[216]

Оцифровка. Хотя российское правительство официально не определило этот термин, он часто встречается в российских трудах о слиянии технологий и военных возможностей. Оцифровка в значительной степени понимается как «широкое внедрение, развитие и применение информационных технологий в вооруженных силах». Применение информационных технологий в вооруженных силах ведет к качественному преобразованию военного потенциала, которое кардинально повлияет на системы вооружений и способы их применения.

Интеллектуализация. Также официально не определенный, один профессиональный военный журнал называет интеллектуализацию широко распространенным внедрением ИИ (предположительно военного в данном контексте), способного выполнять творческие функции, которые традиционно считаются прерогативой человека (т.е. воспринимаются человеком как разумные)». Другое более раннее описание 2008 года относится к внедрению специально разработанных «интеллектуальных» систем, созданных экспертами-людьми, хранящихся в заранее созданных базах данных, которые повышают эффективность информационных процессов.

---

[216] «Министерство обороны создаст департамент по искусственному интеллекту», (Министерство обороны создаст департамент искусственного интеллекта), Риа Новости, 26 апреля 2021 года, https://ria.ru/20210426/minoborony-1730064599.html.

Российские военные писатели обычно ссылаются на «интеллектуализацию» или «оцифровку» вооруженных сил с «широким внедрением, разработкой и применением современных информационных технологий на основе компьютерных технологий и связи».[217]

В дополнение к потенциальным преимуществам, которые дает эта новая технология сама по себе, российские стратеги высоко оценивают технологические возможности других стран, особенно Соединенных Штатов и Китая, и выражают озабоченность по поводу них. Они подпитываются давней проблемой безопасности, такой как страх внезапного нападения или все более мощная роль информации в воздействии на местное население.

Значительная часть населения, по правде говоря, уже давно оценили, что Запад постоянно стремится держать Россию обездоленной и слабой, и что он будет искать возможности для изменения России, ее политического руководства и отношения местного населения, чтобы сделать Россию более сговорчивой.

Показательно, что тогдашний заместитель Министра обороны Юрий Борисов в 2018 году утверждал, что кибервойны уже стали реальностью в современных противостояниях и что эти сражения непрерывно разыгрываются в информационном пространстве, где победа зависит от Технологии с поддержкой искусственного интеллекта.[218]

Соизмеримо с растущей областью военной авиации в мире российские военные лидеры, стратеги и представители промышленности обсуждают потенциальные риски и преимущества ИИ и автономных систем, играющих все большую роль в управлении информацией и принятие решений.

---

[217] О.В. Масленников, «Интеллектуализация - важная составляющая цифровизации вооруженных сил Российской Федерации, VM, no. 7 (2020), https://vm.ric.mil.ru/upload/site178/RJvfqCrBxZ.pdf.

[218] Юрий Борисов, «Развитие искусственного интеллекта имеет важное значение для успешного ведения кибервойны», Развитие искусственного интеллекта необходимо для успешного ведения кибервойн, Министерство обороны Российской Федерации, март 2018 г., https://function.mil.ru/news page/person/more.htm?id=12166660@egNews.

Российские военные рассматривают потенциальные технологии с поддержкой ИИ для смягчения естественных, физических и психологических ограничений для людей-операторов.

В то же время существует озабоченность по поводу последствий того, что будущие системы с улучшенным ИИ смогут ставить цели, устраняя оператора.[219]

Российские дискуссии о военном ИИ четко признают технические проблемы и этические риски полностью автономных систем, но также имеют ощущение неизбежности того, что военные системы станут полностью автономными.

Существует также некоторый скептицизм в отношении широкого ИИ и способности систем ИИ заменить способность военного лидера принимать решения. Аналитики отмечают, что отсутствие обучающих данных не позволяет системам ИИ создавать оригинальные, изобретательные, креативные и рискованные решения.[220]

Напротив, военные лидеры, такие как генерал-полковник Владимир Зарудницкий, глава Военной академии Вооруженных Сил, утверждали, что оценка тенденций военного ИИ приводит к выводу, что переход от человеческого контроля над военной робототехникой до большей автономии неизбежен и России необходимо это спланировать.[221]

Еще одна военная статья утверждает, что технология ИИ «усиливает любую военную профессиональный опыт, расширяющий возможности военных с помощью опыта и способности к прогнозированию, недоступных людям».[222]

Бывший вице-премьер Юрий Борисов, упомянутый ранее, настаивает на том, что, поскольку новые технологии создаются людьми, они просто не будут работать без людей.[223]

---

[219] В.М. Буренок, Р.А. Дурнев и К.У. Крюков, «Интеллектуальное вооружение: Будущее искусственного интеллекта ввоенном деле», Оружие и экономика 1, № 43 (2018), http://www.viek.ru/43/4-13.pdf.
[220] Там же.
[221] Полковник В.Б. Заруницкий, «Природа и содержание военных конфликтов сегодня и в обозримом будущем», Военная мысль, № 1 (январь 2021), https://vm.ric.mil.ru/upload/site178/8sGnTJ8GHJ.pdf.
[222] Масленников и др., «Интеллектуализация является важной составляющей оцифровки Вооруженных Сил Российской Федерации». Российская Федерация».

Президент России Владимир Путин лично принял участие в дебатах, заявив, что, хотя использование усовершенствованного ИИ оружия, скорее всего, определит будущее боевых действий, ИИ никогда не заменит людей.

Системы ИИ должны в конечном счете контролироваться людьми и должны рассматриваться как «верные помощники».[224]

Это подчеркивает напряженность, существующую в официальных дискуссиях о роли ИИ.

Некоторые заявления предсказывают окончательную автономию систем ИИ, в то время как другие заявляют, что люди всегда должны контролировать ситуацию. Кроме того, МОД, похоже, уже строит планы для роботизированных систем с поддержкой ИИ, которые могут действовать автономно и предположительно независимо от людей. Чего, по-видимому, не хватает в разговоре, так это способа сбалансировать эти две точки зрения. В российском военном мышлении неясно, где закончится человеческий контроль и независимость, и где начнется действие с поддержкой ИИ.

Тем временем также обсуждается вопрос о том, чего можно разумно достичь, развивая ИИ и автономные технологии и интегрируя их в российскую армию. Согласно статье Академии ракетных войск России, российские военные должны быть в состоянии достичь больших возможностей за счет использования военных роботов, боевых и разведывательных полуавтономных платформ, анализа информации и разведданных с помощью ИИ и повышения эффективности принятия решений с помощью ИИ на основе анализа сложных динамических сред в реальном времени.[225]

Генерал-полковник Зарудницкий заявил, что для российских военных будет иметь решающее значение создание самообучающихся систем, способных анализировать большие объемы данных для применения

---

[223] «Развитие искусственного интеллекта имеет важное значение для успешного ведения кибервойны».
[224] Президент России Владимир Путин: «Искусственный интеллект – главная технология 21 века», Путешествие ИИ Конференция 2020 года, 4 декабря 2020 года, http://kremlin.ru/events/president/news/64545.
[225] Буренок, Дурнев и Крюков, «Интеллектуальное вооружение: Будущее искусственного интеллекта в военном деле».

в управлении вооружениями, стратегическом прогнозировании и принятии решений.[226]

Среди российских военных ученых и комментаторов также обсуждается относительный путь, по которому пойдет эволюция военного ИИ, чтобы свести к минимуму роль человека в операциях.

Военные авторы признают, что узким технологиям с поддержкой ИИ не хватает единой организационной среда, в которой может взаимодействовать разнообразный набор военных систем. Если бы страна могла производить единая информационная среда для своих военных, которая связывала бы разрозненные системы с улучшенным ИИ, эти системы могли бы затем разрабатывать свои собственные цепочки убийств, решения и т.д., что в корне изменило бы то, как современные военные проводят операции на всех уровнях. Эта линия мышления обычно заканчивается российскими спекуляциями о полной замене людей на тактическом и тактико-оперативном уровнях.[227]

Информационное противостояние и доминирование на поле боя

Российское руководство рассматривает информационное противостояние как один из основных способов конкуренции стран. Перспектива ИИ в области управления информацией ставит технологию прямо в центр российских проблем. Российские стратеги разбивают информационное противостояние на его психологическую и техническую составляющие, хотя и то, и другое формирует стратегическую среду.

С точки зрения технологии, ИИ обладает потенциалом помочь российским войскам добиться информационного доминирования на поле боя. Огромное количество информации, доступной через сетевые датчики, космические архитектуры и киберпространство делают быстрый сбор информации, анализ, прогнозирование/распространение решений необходимым условием для победы на современном поле боя. Информационное

[226] Заруницкий, «Характер и содержание военных конфликтов сегодня и в обозримом будущем».
[227] Полковник Д.В. Галкин, полковник П.А. Поляндра и полковник А.В. Степанов, «Состояние и перспективы применения ИИ в военном деле» Военная мысль, январь 2021 г., стр.113-124.

доминирование требует, как оборонительных возможностей, так и способности дезорганизовывать наступательные возможности противника. Необходимость дезорганизовать силы противника возникла в литературе, посвященной радиоэлектронной борьбе (РЭБ), но вышла за рамки этой области военных исследований и перешла к дискуссиям о том, как другие наступательные операции, которым помогают передовые технологии, такие как ИИ и автоматизация, могут сделать командование и управление силами противника неспособными справиться со скоростью изменений на современном поле боя.

Во многих обсуждениях информационной и современной войны упоминается центральная роль сетецентрической войны, определяемой на русском языке как «интеграция военного командования и управления на всех уровнях от отдельных военнослужащих до более высоких уровней в единую сеть, которая обеспечивает качественно новый уровень интеграции».

По мнению некоторых авторов, такая интеграция необходима для получения оперативного превосходства над силами противника.[228]

Однако, помимо военных, ИИ играет определенную роль в более широком информационном противостоянии между странами.

Российские политические и военные лидеры и стратеги говорят об изменении характера международной конкуренции и использовании невоенных средств для разрешения конфликтов – те инструменты, которые использует государство, которые выходят за рамки обычных инструментов войны.

С этой точки зрения Россия находится в состоянии непрерывного конфликта низкого уровня, особенно с Соединенными Штатами.

Большая часть этого конфликта происходит в киберпространстве через все различные средства, с помощью которых люди получают информацию. Поскольку ИИ упоминается в связи с кибернетикой, обычно это связано с тем, что ИИ создает инструменты, используемые

[228] Масленников и др., «Интеллектуализация является важной составляющей оцифровки Вооруженных Сил Российской Федерации».

в информации. Конфронтация более эффективна и, следовательно, представляет большую угрозу для психологического настроя внутреннего населения России.[229]

По мнению одного автора в журнале Военная мысль – специальное издание Генерального штаба ВС РФ – говорится, что цифровые технологии и ИИ могут применяться как «активные инструменты для десуверенизации» России.[230] Здесь он имеет в виду концепцию суверенитета часто используется российским руководством в отношении целостности государства и необходимость сдержать иностранное влияние – информация в данном случае – от воздействия на население России.[231]

В то время как российское политическое и военное руководство активно обсуждает, широко освещаемое в военных журналах, информационную конфронтацию и «психологическую войну», меньше обсуждается вопрос о том, как ИИ участвует в этом конфликте. Это может быть по двум возможным причинам.

Во-первых, использование ИИ в киберпространстве является сугубо техническим и менее склонным к упрощенным описаниям.

Во-вторых, наступательные и оборонительные аспекты кибернетики строго засекречены, учитывая период полураспада кибернетических технологий, как только они становятся известны противнику.

Искусственный интеллект и международная безопасность

Политические и военные лидеры, а также научные исследователи и дипломатический персонал выразили озабоченность по поводу потенциального влияния ИИ на международную стабильность и безопасность. Эти проблемы могут быть разделены примерно на две общие темы: угрозы,

[229] Алексей Рамм, Российские информационные и кибероперации, Центр анализа стратегий и технологий, 2017.
[230] Д.Г. Евстафьев и А.М. Ильницкий, «Приоритеты управления национальной безопасностью и обороной в постглобальном мире», Военная мысль, № 3 (2021).
[231] Галкин, Поляндра и Степанов, «Состояние и перспективы применения ИИ в военном деле».

присущие ИИ как технологии, и преднамеренное использование ИИ теми, кто имеет недобрые намерения по отношению к другой стране.

Обе эти угрозы озвучены в России в терминах, в значительной степени соответствующих общим темам в ИИ, а также отображающим существующие российские опасения по поводу международная безопасность и ее влияние на Россию.

Например, как повышение способности принимать решения и самостоятельности повлияет на безопасность работы?

Евгений Пашенцев в интервью российскому журналу международных отношений Министерства иностранных дел отмечает, что растущая роботизация и замена людей может привести к росту нестабильности в обществе и, что это относится не только к производству, но и в более высокооплачиваемых сферах занятости, таких как финансы, услуги и управление.[232]

Другая очевидная проблема заключается в опасности того, что алгоритмы и технологии не могут заменить человека в цепочке решений. Обычно это связано с этическими соображениями по поводу создания смертоносных автономных систем оружия.

Другая широкая категория угроз – это множество способов, которыми люди представляют себе ИИ, влияющий на международную безопасность в результате его преднамеренного использования как государственными, так и негосударственными субъектами.

Выступая в Организации Объединенных Наций в 2002 году, Путин выразил обеспокоенность по поводу неконтролируемого распространения цифровых технологий и, подобно реальному оружию, попадания в руки негосударственных субъектов, что приводит к чрезвычайным рискам для международной безопасности.

---

[232] Евгений Пашенцев, «Искусственный интеллект и безопасность: что хорошо и что плохо», Искусственный интеллект и безопасность: что во благо, а что во зло?, Международные отношения (2019), https://interaffairs.ru/news/show/24219.

Он также заявил о необходимости регулирования ИИ, которое уменьшает не только технологические угрозы, но и угрозы традициям, закону и морали – это постоянная озабоченность российского руководства возможностью воздействия внешних сил на психологическое состояние населения России.[233]

Сравнение информационных операций с реальным оружием не ново в российской дискуссии.

В 2019 году Секретарь Совета Безопасности России Николай Патрушев назвал ИИ, среди прочих технологий, потенциально способным нанести такой же ущерб, как и оружие массового уничтожения.[234]

В российских дискуссиях по вопросам безопасности существует глубокая озабоченность по поводу потенциальных преднамеренных и непреднамеренных опасностей, создаваемых продолжающимся внедрением и возможными последствиями ИИ. Хотя существует общая озабоченность по поводу сохранения контроля над системами, улучшенными ИИ, особое внимание уделяется потенциалу ИИ для повышения сложности и смертоносности с психологической точки зрения – инструментов информационной войны.

Искусственный интеллект, автономия и ядерное оружие

ИИ и автономия играют важную роль в ядерных силах России точно так же, как они играли важную роль в советских ядерных силах во время холодной войны. Во многих отношениях роль ИИ и автономия соответствуют конкретным российским соображениям безопасности, включая потенциальную надежность и живучесть российского ядерного сдерживания.

Меньший размер как российского, так и американского ядерных арсеналов по сравнению с их соответствующими размерами во время холодной войны в сочетании с гиперболическими оценками Москвы нападения США

---

[233] Владимир Путин, «75-я сессия Генеральной Ассамблеи ООН: Владимир Путин выступил с видеообращением на пленарном заседании 75-й сессии Генеральной Ассамблеи Организации Объединенных Наций» (Организация Объединенных Наций, Нью-Йорк, 22 сентября, 2020, 2020), http://www.kremlin.ru/events/president/news/64074.

[234] «Глава службы безопасности России призывает регулировать использование новых технологий в военной сфере: новые технологии могут быть «столь же смертоносными, как оружие массового уничтожения», предупреждает чиновник», ТАСС, 2019, https://tass.com/defense/105534.

и возможности противоракетной обороны усилили озабоченность России по поводу потенциальной эффективности противоракетной обороны. С меньшими арсеналами противоракетная оборона рассматривается как потенциально более эффективная в снижении воздействия второго удара – краеугольного камня взаимно гарантированных разрушений.

Сценарий выглядит следующим образом.

Соединенные Штаты по какой-либо причине начинают атаку, нацеленную на политическое руководство России, ядерное командование и контроль ядерных сил и критически важной инфраструктуры.

Эта атака использует такие возможности, как высокоточный удар с использованием боеприпасов большой дальности, наступательные кибероперации и средства космического базирования.

В зависимости от его успеха, российские военные аналитики оценивают, что существует вероятность того, что у России не останется достаточного количества ядерного арсенала, чтобы проникнуть в системы противоракетной обороны США с достаточным количеством боеголовок, чтобы вызвать недопустимый ущерб.[235]

Если это правда, это может привести к сценариям, в которых у Соединенных Штатов действительно есть стимул нанести удар первыми, потому что результирующий ущерб будет ниже неприемлемых пороговых значений. Эта логика является ключевой движущей силой продолжающейся апоплексической реакции российского руководства на инициативы США и НАТО по противоракетной обороне и особенно на выход США в 2002 году из Договора по противоракетной обороне (ПРО) 1972 года. Трудно переоценить ту роль, которую вывод войск США играет в российских дискуссиях об угрозе, которую он видит со стороны Соединенных Штатов.

---

[235] Петр Топычканов, «Автономия в российских ядерных силах», Влияние искусственного интеллекта на стратегическую стабильность и ядерный риск», Том 1, под ред. Винсента Буланина (май 2019 г.), стр.73, https://www.sipri.org/publications/2019/other-publications/impact-artificial-intelligence-strategic-stability.

Так, в декабре прошлого года, Путин заявил, что Соединенные Штаты инициировали нынешнюю гонку вооружений, выйдя из договора.[236]

Один конкретный пример: озабоченность России в связи с разработкой наступательной космической оптико-электронный системы разведки и угрозой, которую она представляет для России и ее стратегических ракетных войск.[237]

В отличие от США, самой надежной опорой ядерной триады России являются подводные лодки с баллистическими ракетами, на суше сдерживающим фактором, являются дорожно-мобильные ядерные силы, которые считаются наиболее живучим компонентом российского ядерного сдерживания.[238]

Поэтому любая технология, которая облегчила бы обнаружение и уничтожение российских ядерных сил, особенно сухопутных войск, вызывает особую озабоченность у российского руководства.

Эта озабоченность, возможно, является движущей силой российской ядерной стратегии «запуск по предупреждению». Запуск по предупреждению – это позиция, в которой страна, получив указания о готовящемся нападении, запускает свои средства ответного удара до того, как эти средства могут быть уничтожены.[239]

После холодной войны военные аналитики подозревали, что это была позиция Российской Федерации и наиболее недавняя декларативная политика, по-видимому, подтверждает эту точку зрения.[240]

Общая озабоченность по поводу возможной аэрокосмической атаки США в частности, стимулируют российские инициативы по интеграции автономии и ИИ в свои ядерные системы.

---

[236] «Путин: Гонка вооружений уже началась», Коммерсантъ, 2020, https://www.kommersant.ru/doc/4617177.

[237] А.В. Евсюков и А.Л. Хряпин, «Роль новых систем стратегических вооружений в обеспечении стратегического сдерживания. Военная мысль, № 12 (2020), https://vm.ric.mil.ru/upload/site178/AMIei6v9c7.pdf.

[238] В.Ф. Лата, «Настоящее и будущее Ракетных войск стратегического назначения как гаранта обороны и безопасности России», Вестник Академии Военных наук, № 63 (2018), http://www.avnrf.ru/attachments/article/1125/AVN-2 (63).

[239] Лоуренс Фридман и Джеффри Майклз, Эволюция ядерной стратегии, 4-е изд. (Лондон: Пэлгрейв МакМиллан, 2019), стр.286.

[240] Синтия Робертс, «Откровения о политике ядерного сдерживания России», Война на скалах, июнь 2020 года, https://warontherocks.com/2020/06/revelations-about-russias-nuclear-deterrence-policy.

Российские военные рассматривают интеграцию автономии и элементов ИИ как ключ к укреплению доверия к своим средствам ядерного сдерживания для Соединенных Штатов, поддержанию сил, повышению их способности к раннему предупреждению, поддержанию надежного потенциала второго удара и поражению систем противоракетной обороны противника (США), среди других применений. Раннее предупреждение, учитывая приведенную выше логику, это особенно важно, и технологии ИИ обещают улучшить российскую систему раннего предупреждения для лучшей оценки угроз и прогнозирования ущерба.

Следует отметить, что даже во время Холодной войны, эксперты признали важность управления ядерным кризисом и снижению рисков ядерной эскалации, вызванной третьей стороной.

В статье, опубликованной в журнале «Военная мысль», авторы утверждают, что Россия должна интегрировать ИИ в свою поддержку принятия решений для защиты от американской концепции «глобального удара» и для мониторинга динамичных геополитических и военных событий.[241]

В случае надвигающейся атаки ИИ и полуавтономные системы могут помочь в принятии решений, учитывая короткое время отклика. Это может включать совершенствование способов защиты вооруженных сил и ресурсов от надвигающегося удара и наилучшего планирования ответных мер.[242]

В свою очередь, сообщалось, что Российский национальный центр управления обороной (NDMC) – который является ключевым военным узлом в кризисной ситуации или конфликте, и в нем размещается суперкомпьютерная мощь российских военных, используемая для анализа военно-политической ситуации в реальном времени и перспективного анализа, может использовать технологии с поддержкой ИИ для сбора и анализа информации в качестве помощи в принятии решений.[243]

---

[241] Галкин, Поляндра и Степанов, «Состояние и перспективы применения ИИ в военном деле».
[242] «Искусственный интеллект и ядерное оружие».
[243] «Российский национальный центр управления обороной использует искусственный интеллект», Regnum.ru, 27 января 2020 г., https://regnum.ru/news/polit/2836730.html.

Совсем недавно сообщалось, что радиолокационные станции, входящие в состав российской системы предупреждения о ракетном нападении, будут модернизированы с помощью технологии ИИ, чтобы повысить их способность измерять и оценивать поступающие угрозы. Однако ни одна часть этой системы не будет «думать» сама по себе, и доступная информация предупреждает о рисках расширения роли ИИ в ядерной инфраструктуре и планировании.[244]

Это мнение часто повторяется в российских дискуссиях о роли ИИ в ядерных арсеналах, несмотря на многочисленные дискуссии по поводу системы ядерного управления и контроля по периметру России.

Система «Периметр», получившая прозвище «Мертвая рука», представляет собой автоматизированную систему ядерного командования и управления, разработанную Советским Союзом, и считается, что она все еще используется для обеспечения гарантированного ядерного возмездия.

Эта система включается в кризисный период, когда угроза ядерного нападения считается высокой. Используя различные датчики, он может обнаружить происходящую ядерную атаку и командовать нанесением ответного удара российскими ядерными силами в случае когда политическое руководство недееспособно.

Первоначальная цель системы была двоякой: обеспечить сохранение потенциала ответного удара в случае первого обезглавливающего удара и сократить время, необходимое руководству для принятия решения относительно ядерного запуска, путем создания условий, позволяющих нанести ответный удар, уже находясь под ядерным ударом.

Система позволяла делегировать полномочия политического руководства в эмоциональный и трудный момент, повышая уверенность военных в принятии кризисных решений.

Система не полностью автоматическая, а полуавтоматическая по конструкции, предположительно использующая человеческое командное

[244] «Россия повысит возможности системы предупреждения о ракетном нападении после модернизации», Tass.ru, 15 февраля 2021 года, https://tass.com/defense/1256603.

устройство, которое все равно согласовывало бы предоставленные делегированные полномочия с ситуацией, о которой сообщают различные датчики системы.

Его существование подразумевает предпочтение полуавтоматических, а не полностью автоматизированных систем при решении проблем, вызванных нехваткой времени, несовершенной информацией и эмоциями, которые фундаментально влияют на людей, принимающих решения, и тем самым снижают риск просчета с обеих сторон и вероятности того, что эти обстоятельства приведут к неправильному решению.[245]

В недавней статье в «Военной мысли» несколько военных авторов, связанных с российским Министерством обороны и Московским государственным техническим университетом имени Н.Э. Баумана обсудили дебаты в США о роли ИИ в ядерном оружии.

Они утверждали, что большинство исследований предполагают, что ИИ может нанести ядерный удар, если увидит преимущество, и указали на противоположные перспективы в Соединенных Штатах по этому вопросу: доклад RAND за 2018 год Эдварда Гейста и Эндрю Джона под названием «Как может искусственный интеллект повлиять на риск ядерной войны?» и статья Адама Лоутера и Кертиса Макгиффина «Война со скалами» 2019 года под названием «Америке нужна мертвая рука».

Они утверждают, что России «необходимо будет поддерживать принятие решений о применении ядерных сил, определенно используя ИИ в качестве инструмента анализа динамично меняющейся геополитической и военной обстановки и оставляя окончательное решение за уполномоченными лицам».[246]

Однако в статьях не упоминается, что в сентябре 2019 года генерал-лейтенант Дж. Шанахан, тогдашний директор Объединенного центра

---

[245] Управление военной разведки, Военная мощь России: Создание вооруженных сил для поддержки устремлений Великой Державы, 2017, https://www.dia.mil/portals/27/documents/news/military pdf.
[246] Галкин, Поляндра и Степанов, «Состояние и перспективы применения ИИ в военном деле».

искусственного интеллекта, публично отверг логику, изложенную в «Войне» Лоутера.[247]

Как обсуждается далее в этой статье, Россия использует ИИ и автоматизацию в своих системах противовоздушной и противоракетной обороны. Российские стратеги считают вычислительную мощность ИИ необходимой для ускорения скорости, с которой интегрированная система противовоздушной обороны (IADS) может отслеживать, обнаруживать и реагировать на надвигающуюся аэрокосмическую атаку.

Это включает в себя систему ПВО «Панцирь», а также Систему противоракетной обороны С-500 – последняя из которых обладает некоторой способностью перехвата МБР ближе к концу траектории полета ракеты.

Новое ядерное оружие Путина

В драматической речи в марте 2018 года Путин подчеркнул, что в российский арсенал войдут новые полуавтономные и, возможно, автономные ядерные вооружения, заявив, что они могут «достичь любой точки мира» и что Запад должен понять, что Россия не «блефует».[248]

Речь Путина и предполагаемые возможности этого оружия, включая технологии, улучшенные ИИ, подчеркивают озабоченность российского руководства противоракетной обороной США, поскольку каждое из них явно способно избежать или смягчить противоракетную оборону.

Из этих систем меньше всего сообщается о крылатой ракете с ядерным двигателем «Буревестник».

Преимуществом этой системы, с точки зрения России, является ее способность патрулировать и задерживаться в течение неопределенного времени благодаря своей ядерной двигательной установке и наносить удары по команде.

---

[247] Сидней Дж. Фридберг-Младший, «Нет Искусственного Интеллекта Для Ядерного Командования и Управления: Шанахан ДЖЕЙКА», Нарушение защиты, 25 Сентября, 2019 год, https://breakingdefense.com/2019/09/no-ai-for-nuclear-command-control-jaics-shanahan.

[248] «Путин рассказал о новейших видах российского оружия», Риа Новости, 1 марта 2018 г., https://ria.ru/20180301/1515566394.html.

Как и в других системах, основным аспектом, связанным с ИИ/автономией, согласно отчетам с открытым исходным кодом, является его система наведения.[249]

Один российский военный журналист Алексей Рамм отмечает, что способность ракеты зависать над водой в течение длительных периодов времени создает проблемы с ее руководством.

Исторически сложилось так, что крылатые ракеты полагались на различные системы наведения на большей части своей траектории полета, включая инерциальные системы, согласование контуров местности (TERCOM) и космические системы позиционирования.

Для длинных траекторий полета над водой это, как правило, означало зависимость от российской системы ГЛОНАСС или GPS. Рамм отмечает, что длительные периоды бездействия заставляют сомневаться в том, что ракета будет полагаться исключительно на ГЛОНАСС, но не дает никаких указаний относительно того, какую альтернативную систему она будет использовать для поддержания точности своего положения в течение длительных периодов времени.[250]

«Авангард» – это гиперзвуковое скользящее транспортное средство, запускаемое баллистической ракетой, которое после запуска совершает небаллистический маневренный полет к своей цели. Преимуществом такой системы является как ее скорость, так и ее способность предположительно уклоняться от систем противоракетной обороны, что еще раз подчеркивает озабоченность России противоракетной обороной США.

Одной из особых проблем гиперзвуковых скользящих аппаратов является сложность поддержания и обновления их телеметрии, учитывая экстремальное тепло, создаваемое их гиперзвуковой скоростью в атмосфере. Герберт Ефремов, ведущий дизайнер системы отмечает, что ракета рассчитывает свой путь от

---

[249] «Путин рассказал о новейших типах российского оружия», Риа Новости, 1 марта 2018 г., https://ria.ru 20180301/1515566394.html Известия, январь 2019 г., https://iz.ru/829623/dmitrii-stefanovich/avangard-i.

[250] Алексий Рамм, «Крылатый «буревестник»: Что известно о загадочном российском оружии «крылатый буревестник, Известия, 5 марта 2019 г., https://iz.ru/852592/aleksei-ramm/krylatyi-burevestnik.

фактического запуска до конечной цели, используя системы, улучшенные ИИ, и что никто на самом деле не знает, какой путь оно решило выбрать к своей цели.

«Посейдон», иногда называемый Статусом-6 или Каньон, является автономным (роботизированным в некотором смысле) аппаратом, напоминающим торпеду, предназначенным для нанесения ответного ядерного удара.[251]

Он питается от небольшого ядерного реактора, обеспечивающего ему «неограниченное расстояние», и оснащен большой ядерной боеголовкой для уничтожения прибрежной инфраструктуры.[252]

«Посейдон» будет нести переоборудованная российская атомная подводная лодка «Белгород», которая будет способна нести несколько видов оружия. В то время как «Посейдон» четко классифицируется как автономный ядерный беспилотник (или, как минимум, полуавтономный) неясно, какие элементы ИИ машинного обучения могут существовать в торпеде. Одна из возможностей, предложенных в отчетности заключается в том, что он имеет сложные алгоритмы навигации, которые помогают ему маневрировать в море.[253]

Последние две системы обладают теми же характеристиками, что и другие платформы гиперзвуковых и крылатых ракет, упомянутые ранее.

Тяжелая межконтинентальная баллистическая ракета (МБР) «Сармат» предназначена для замены более старой российской МБР SS-19 и способна нести ряд различных боеголовок. Помимо традиционных характеристик МБР, мы включаем ее сюда из-за ее способности развертывать уже упомянутую ракету «Авангард» и особых проблем, связанных с автономностью этой ракеты.[254]

---

[251] «Досье на беспилотный подводный аппарат «Посейдон», Tass.ru, https://tass.ru/info/5388731.

[252] Антон Лавров и Алексей Рамм» «Посейдон в лодке: подводная лодка готовится к испытаниям ядерных роботов», Izvestia.ru, Февраль 2021 года, https://iz.ru/1123160/anton-lavrov-aleksei-ramm/poseidon-v-lodke.

[253] В.С. Прямицкий, «Ошибка или достижение», VPK.ru, 9 июня 2019 года, https://vpk.name/news/318706_poseidon _oshibka_ili_dostizhenie.html.

[254] Стюард Рассел и Питер Норвиг, Искусственный интеллект: Современный подход, 4-е изд. (Хобокен, Нью-Джерси: Пирсон Образование, 2021); Юнпин Пан, Бэзил М. Аль-Хадити и Чэнгуань Ян, «Редакционная статья: ИИ для моделирования роботов, «Путь планирование и интеллектуальное управление», Границы (2020), https://www.frontiersin.org/articles/10.3389/frobt.2020.00019/full.

Кроме того, «Кинжал» – это запущенная с воздуха баллистическая ракета, вероятно, разработана по проекту баллистической ракеты «Искандер» наземного базирования и, как сообщается, также маневренна.[255]

Ключевые военные инициативы в области ИИ

В этом разделе рассматриваются некоторые ключевые инициативы в области ИИ, которые реализуют российские военные, поскольку они связаны с основными российскими взглядами на характер современного конфликта.

В этом разделе больше рассказывается о том, как ИИ и автономия соотносятся с существующими российскими взглядами на современную войну, и меньше о том, как технологии выводятся и характеризуются с точки зрения того, как они вписываются в область ИИ.

Управление информацией для командования, контроля и принятия решений

Российские военные пытаются внедрить системы с улучшенным ИИ, которые помогут управлять большими объемами информации из множества источников на поле боя. Это происходит от тактического до оперативного и стратегического уровней.

Во многих отношениях российские военные компенсируют серьезный недостаток управления информацией и прозрачности на поле боя на протяжении всей холодной войны. В то время как советские военные могли использовать огромную боевую мощь, им было трудно «видеть» поле боя.

Это сохранялось и было вызвано из-за плохой работы ISR во время войны в Грузии.[256]

Это в сочетании с целенаправленным обзором военных действий США, предпринятых с момента окончания холодной войны, которые

---

[255] «Кинжал», Ракетная угроза: Проект противоракетной обороны CSIS, 2021 год, https://missile threat.csis.org/missile/kinzhal.

[256] Руслан Пухов, Танки Августа, Центр анализа стратегий и технологий, Москва, http://cast.ru files/The_Tanks of_August _sm_eng.pdf.

продемонстрировали российское военное руководство потенциальное влияние информационного доминирования в современном конфликте – подчеркивается общей ссылкой на сетецентрическую войну США в их дискуссиях о войне.

На стратегическом уровне российские авторы в ведущих военных журналах отражают мнение о том, что системы ИИ в сочетании с обширными данными, доступными о текущих мировых событиях, могут помочь в анализе динамично меняющаяся геополитическая и военная обстановка.[257]

Это является частью мотивации создания NDMC, миссия которого заключается в следующем: NDMC предположительно использует ИИ в своей повседневной работе для сбора и систематизации информации.[258]

Типы информации варьируются от статуса военных подразделений и операций, особенно развернутых российских подразделений, статуса ядерной триады и международных геостратегических событий.[259]

Роль центра в оценке международных событий особенно интересна.

В декабре 2019 года министр обороны России Сергей Шойгу заявил, что в России создана система, которая позволила бы России прогнозировать начальные условия, приводящие к вооруженным конфликтам, используя специальную базу данных, которая позволяет:

– обеспечить централизованное боевое управление Вооруженными Силами Российской Федерации;

– сбор, обобщение и анализ информации о военно-политической обстановке стратегических районов мира и социально-политической ситуации в Российской Федерации в мирное и военное время.

Если мы ставим в базу данных все сведения о действиях, например, из группы военных в Югославии (сколько кораблей, сколько перевозчиков, сколько самолетов, сколько ракет, в какое время – днем, ночью, что произошло), то она действует как «будильник», который говорит: «Вы знаете, ситуация очень

---

[257] Галкин, Поляндра и Степанов, «Состояние и перспективы использования ИИ в военном деле», стр.113-124.
[258] Министерство обороны Российской Федерации, «Национальный центр управления обороной Российской Федерации», https://structure.mil.ru/structure/ministry_of_defence/details.htm?id=11206@egOrganization.
[259] «Российский национальный центр управления обороной использует искусственный интеллект».

похожа в таком-то регионе мира, потому что есть такое же количество кораблей, авианосцев, самолетов, носителей крылатых ракет и высокоточного оружия, поэтому существует высокая вероятность того, что эта часть мира может испытать то, что произошло в Югославии.[260]

Шойгу далее сказал, что система не только прогнозирует конфликты, но и рекомендует ответные меры, основанные на предыдущих ошибках. Возможно, что NDMC предполагает наличие системы с аналогичными целями ИИ DARPA, ориентированного на знания, рассуждающего над схемами (KAIROS), система, которая стремится «разработать систему ИИ на основе схемы, которая может идентифицировать сложные события и доводить их до сведения пользователей».[261]

Схемы, согласно DARPA, созданы у людей путем абстрагирования повествовательных структур, основанных на опыте реального мира. На сегодняшний день, ИИ связанных систем либо были не в состоянии соответствовать схеме в реальном мире событий или требуют чрезмерную методичку, чтобы быть практичными.[262]

Отчетности на NDMC не выявили ничего подобного, схем, указанных в KAIROS и о том, как эта система учится на ошибках и как ошибки предыдущих конфликтов кодируются. Шойгу действительно утверждал, что Министерство обороны обладает техническими возможностями для накопления и систематизации необходимой информации.

Последняя часть заявления о миссии вытекает из ранее обсуждавшийся озабоченности о том, что такие противники, как Соединенные Штаты, стремятся подорвать российские власти и создать нестабильность внутри России, чтобы подстегнуть политические перемены, что приведет к оправданию военных действий США.

---

[260] Александр Пешков, «Шойгу: у Министерства обороны есть система прогнозирования конфликтов», TvZvezda.ru, декабрь 2019 г., https://tvzvezda.ru/news/forces/content/201912161125-PViRZ.html.
[261] «Рассуждения Искусственного Интеллекта, ориентированного на знания, над схемами (KAIROS)», DARPA, 2019, https://www.darpa.mil/program/knowledge-directed-artificial-intelligence-reasoning-over-schemas.
[262] Там же.

На оперативном уровне российские военные в значительной степени сосредоточились на интеграции информации с различных платформ между военными подразделениями в попытке улучшить координацию сил и принятии более быстрых решений. Заявления и обсуждения часто относятся к различным военным автоматизированным системам, часто называемым просто автоматизированными системами управления (АСУ).

АСУ не нова, но концепция является основой для того, как российские военные концептуализируют и используют ИИ и автономию, чтобы сделать российские войска более эффективными и более смертоносными. Согласно российской военной энциклопедии, АСУ определяется следующим образом: система, которая автоматизирует такие процессы или функции управления войсками и (или) оружием (боевыми средствами), как: сбор, обработка, хранение и доставка информации, необходимой для оптимизации управления войсками и оружием.[263]

Фактическое название комплексных систем АСУ Вооруженных Сил Российской Федерации «ASU VS RS» – это общий термин для ряда систем АСУ, которые работают на разных уровнях и имеют разные цели для управления и контроля. Основой всеобъемлющей системы является «Акация-М», система оперативного уровня, которая обеспечивает командирам осведомленность о боевой обстановке в режиме реального времени. На момент подготовки настоящего доклада Россия продолжает модернизировать все свои оперативные подразделения с помощью новых систем.[264]

АСУ может быть аналогична концепции системы совместного управления всеми доменами Министерства обороны США (JADC2).

JADC2 предназначен для подключения датчиков всех служб, чтобы командиры могли лучше принимать решения за счет интеграции многочисленных источников информации, что значительно сокращает время,

---

[263] Министерство обороны Российской Федерации, «Военная автоматизированная система», в Военной энциклопедии, https://encyclopedia.mil.ru.

[264] Министерство обороны Российской Федерации, комплекс средств связи завершил перевод системы управления Ленинской мотострелковой дивизии Западного военного округа на новый уровень, 7 декабря 2020 года, https://function. mil.ru/ news_page/country/more.htm?id=12301550@egNews.

необходимое для принятия мер.[265] JADC2 явно перечисляет облачные вычисления как часть своей структуры для обмена информацией, и вполне вероятно, что российская АСУ также предусматривает облачные вычисления.[266]

В 2019 году руководитель информационных систем Министерства обороны России отметил, что российские военные находятся в процессе перехода на облачные технологии и при одновременном развитии сети передачи данных это позволит Минобороны создать единую платформу информационных услуг.[267]

Он также перечислил основные направления развития системы:

- Во-первых, создаются программные и аппаратные платформы для централизованных (облачных) вычислений вместе с децентрализованными вычислениями (так называемыми туманными) вычислениями, которые дополняют друг друга.
- Во-вторых, разрабатываются инструменты для извлечения больших массивов разнородных, неструктурированных данных.
- В-третьих, создаются программные средства для обеспечения работы с несколькими тематическими базами данных с различными правами доступа.
- В-четвертых, внедряются программные средства (информационные службы), которые выполняют различные информационные задачи в интересах функциональных подсистем.[268]

В данном случае он представляет собой взаимосвязанность «системы доставки огня артиллерийской разведки», которая связывает все элементы,

---

[265] Джон Р. Хон, Объединенное командование и управление всеми областями (JADC2), Исследовательская служба Конгресса, 2020 год, https://fas.org/sgp/crs/natsec/IF11493.pdf.

[266] Виктор Худолеев, ««Цифры» на службе в армии нового поколения», «Цифра» на службе в армии нового поколения, Красная Звезда, 2019.

[267] Там же.

[268] В. Литвиненко и С. Воронков, «Огневые и артиллерийские маневры: роль артиллерии тактических формирований нового типа в вооруженных конфликтах конца XX - начала XXI веков», Армейский Сборник, № 2 (2017), https://varb.mil.by/nauka/sbornik/Sbornik_31-2016.pdf; Лестер Грау и Чак Бартлз, Российский разведывательный огневой комплекс Достигает совершеннолетия, Управление иностранных военных исследований, Армия США, 2018, стр.3.

необходимые для поражения критических целей, с высокоточными боеприпасами большой дальности.[269]

Оперативным примером того, как российские военные внедряют среду АСУ, является 2019 год. В ходе учений Каспийского флота российские воздушные, сухопутные и морские силы были объединены в единое информационное пространство. Данные об обнаруженных целях загружались в систему в режиме реального времени и в зависимости от типа цели команда выбирала наилучшие методы атаки. Вся информация была получена в режиме реального времени и проанализирована с помощью автоматизированной системы управления и контроля с элементами ИИ, согласно сообщениям прессы.

Другим примером была имитация аэрокосмической атаки на Крымский полуостров в июне 2019 года.

АСУ интегрировала системы ПВО С-400 и «Панцирь-С» – вместе с другими радиотехническими, авиационными и черноморскими силами – для отражения внезапной атаки 70 крылатых ракет.

Военнослужащие, ответственные за операцию, утверждают, что российские военные внедряют уроки, извлеченные из Сирии, в проектирование и функционирование АСУ.[270]

В настоящее время эта АСУ функционирует с помощью человеческих операторов. Министерство обороны считает, что в будущем эта система будет оснащена ИИ, чтобы самостоятельно обнаруживать потенциальные цели и распределять ракетные удары без вмешательства человека.[271]

Во время недавней военной выставки IDEX-2021 в Абу-Даби «Рособоронэкспорт» продемонстрировал несколько новых продуктов, в том числе единую систему управления тактического уровня ESU TZ, которая

---

[269] Алексей Рам и Богдан Степовой, «Разведка морского базирования: ИИ будет направлять ракеты корабельного базирования» (Разведка с моря: искусственный интеллект будет направлять корабельные ракеты), Iz.ru, 15 июля, 2019 год, https://iz.ru/898018/aleksei-ramm-bogdan-stepovoi/razvedka-s-moria-korabelnye-rakety-napravit.

[270] «Двойной расчет: «Торнадо» и «Искандер» являются частью единого боевого контура», Известия.Ru, 10 августа 2020 г., ttps://из.ru/1046036.

[271] Людмила Гундарова, «Через трудности к «Созвездию», «через тернии к Еженедельник «Звезда», 31 марта 2021 года, https://zvezdaweekly.ru/news/202131528-TqVxx.html.

является частью более крупной АСУ «Созвездие», производимой дочерней компанией «Рособоронэкспорта» под названием «Созвездие».

В настоящее время система, представленная в Абу-Даби, позволяет артиллерийским и ракетным войскам работать в интегрированной информационной среде. В статье, посвященной этому событию, сравнивается ESU TZ с американской боевой системой будущего (FCS) и системой JADC2, утверждая, что в отличие от российской ESU TZ, FCS потерпел неудачу и США начали все сначала с JADC2.[272]

На тактическом уровне российские военные рассматривают ИИ как необходимое условие для управления большими объемами данных и принятия коротких решений. Например, при проектировании российских истребителей было выдвинуто несколько инициатив по использованию ИИ для управления потоком информации, доступной пилоту, с целью упрощения принятия решений в воздушном бою. Су-35С, тяжелый многоцелевой истребитель большой дальности, использует бортовую информационно-управляющую систему под названием IUS-35, которая состоит из нескольких отдельных компьютеров, объединяющих отдельные информационные каналы в самолете в единый информационный канал, который обеспечивает «интеллектуальную поддержку» пилоту для обнаружения цели и боевого маневрирования самолета.

Во время конфликта в Сирии система также увеличила количество вылетов, выполняемых в день, используя свою способность оптимизировать предполетную подготовку и повысить умственную выносливость пилота.[273]

Раннее предупреждение и противовоздушная оборона

Российские военные надеются, что потенциал ИИ для быстрого управления информацией из нескольких источников и выявления угроз может

[272] «Су-35», Сухой, https://www.sukhoi.org/products/samolety/256/. «Информационно-управляющая система ИУС-35 истребителя Су-35С», «BMPD, https://bmpd.live journal.com/3047341.html.
[273] Галкин, Поляндра и Степанов, «Состояние и перспективы применения ИИ в военном деле».

смягчить одну из наиболее серьезных проблем безопасности: воздушно-космическую атаку со стороны Соединенных Штатов.

Воздушно-космическая атака со стороны США будет включать залпы высокоточных боеприпасов дальнего действия с воздушных и морских платформ. Российские военные, наблюдавшие за кампаниями в Югославии, Ираке, Ливии и Афганистане, определили воздушно-космическую атаку как ключевую военную операцию, используемую Соединенными Штатами для уничтожения противника в начале конфликта. Не обладая ударной способностью, сравнимой с таковой у Соединенных Штатов, российские военные (и советские военные до этого) отреагировали асимметрично, разработав обширные IADS и автономные системы для смягчения последствий аэрокосмической атаки США.

Российские стратеги считают вычислительную мощность ИИ необходимой для ускорения скорости, с которой IADS может отслеживать, обнаруживать и реагировать на надвигающуюся воздушно-космическую атаку. ИИ лучше справлялся бы с большими объемами радарных профилей и траекторий ударных боеприпасов, перемещающихся с разной высотой и скоростью.

Военные стратеги отмечают, что задача управления информацией и требуемой для этого скоростью только усложняется в связи с растущей ролью гиперзвукового оружия. Некоторые утверждают, что только ИИ может своевременно справиться с подобными угрозами.

В 2019 году военные провели учения с использованием радиолокационной базы, в которой использовалась технология ИИ для защиты от аэрокосмической атаки.

Алгоритмы системы контролировали воздушное пространство и, когда обнаруживалась угроза, координировали системы ПВО, чтобы подобрать подходящего стрелка для цели и обеспечивали наведение российских самолетов на направление атаки.[274]

[274] Алексей Козаченко и Алексей Рамм, «Наблюдая Издалека: Силы ПВО Получили Наземные Системы ДРЛО»

Например, система ПВО «Панцирь включает технологии ИИ, которые помогают ей работать полуавтономно, определять местоположение целей, классифицировать их по степени опасности и рекомендовать оптимальные решения для поражения этих целей.[275]

Распространение беспилотных летательных аппаратов в современных боевых действиях побудило российских военных искать решения для этих низколетящих, трудно обнаруживаемых аппаратов. Эта инициатива была выдвинута в большей части благодаря российскому опыту в Сирии, где российские базы подверглись нескольким атакам недорогих роев беспилотников.

Одним из примеров использования ИИ в борьбе с угрозой беспилотников является разрабатываемая российскими военными система, которая анализирует местность, окружающую их базы, и вычисляет наиболее вероятный маршрут, по которому будет двигаться беспилотник, чтобы воспользоваться преимуществами местности и упрощение планирования обороны этих баз.[276]

Логистика, обучение, техническое обслуживание и производство

Российские военные авторы признают роль, которую ИИ может сыграть в улучшении прогнозного технического обслуживания, материально-технической поддержки и прогнозирования спроса/предложения в российских вооруженных силах. ИИ обладает потенциалом для оптимизации эффективности и затрат при одновременном повышении безопасности.[277]

Интересная статья, опубликованная в официальном журнале Военно-морского флота России «Морской сборник», описывает использование ИИ в связи с кибероперациями и военно-морской логистикой. Статья тесно

Iz.ru, 15 сентября 2019 года. https://iz.ru/918749.

[275] «Панцирь с интеллектом: система может противостоять атакам без ввода оператора», Izvetsia.ru, 28 июля 2020 года, https://iz.ru/1040704/anton.

[276] «Россия разработала систему прогнозирования маршрутов вражеских беспилотных летательных аппаратов», ТАСС, август. 2020 год, https://tass.ru/armiya-i-opk/9232665.

[277] Галкин, Поляндра и Степанов, «Состояние и перспективы применения ИИ в военном деле».

связывает кибероперации с сетецентрической войной – концепция, упомянутая ранее, связана с взаимосвязанностью военных систем, обеспечивающих более точные и быстрые операции.

В рамках сетецентрической войны одной из задач является контроль и очернение информации, связанной с «информационной логистикой», включая сохранение ложных логистических узлов, складов, отчетов о поставках и т.д.

В статье рассматривается роль программного обеспечения ИИ в создании ложной среды, предназначенной для запутывания и компрометации логистической системы противника.[278]

Автономия

Российские военные разрабатывают широкий спектр систем и платформ с определенным уровнем автономии. Инвестиции российских военных в автономные технологии проистекают из их убежденности в том, что применение автономии увеличивает боевую мощь России.

Это достигается в первую очередь за счет сохранения жизней российских солдат и более эффективного управления информацией, полученной из внешней среды поля боя, по сравнению с системами, полагающимися исключительно на действия человека.[279]

Президент России Владимир Путин публично подчеркнул важность автономии в формировании нынешнего поля боя и будущего вооруженного конфликта и это мнение разделяют военное руководство России и ключевые исследователи.[280]

В апреле 2021 года начальник Главного штаба армии Василий Тонкошуров проинформировал министра обороны России Сергея Шойгу

---

[278] А. Мухитов, Системы искусственного интеллекта в кибер-архитектуре тыла и технической поддержке Военно-морского флота, Морской сборник (июнь 2018 г.), https://morskoysbornik.ric.mil.ru/upload/site231/7Sk8VdFnhM.pdf.

[279] Сэмюэль Бендетт, «Российские наземные роботы: Откровенная оценка и пути продвижения вперед», Лаборатория Безумного ученого, Июнь 2018 года, https://madsciblog.tradoc.army.mil/63-russian-ground-battlefield-robots-a-candid.

[280] «Путин делится своим мнением о том, в чем больше всего нуждается Российская армия», Тасс, 2017, https://tass.com/defense/927489; «Использование ИИ для управления вооружением в будущем во многом определит исход битвы – Путин», ТАСС, 2020, https://tass.com/defense/927489.

о прогрессе, достигнутом в создании и испытании первого российского военного подразделения с ударными роботами. Это подразделение является экспериментальным и даст представление о том, как российские сухопутные войска будут доктринально интегрировать роботизированные подразделения в сухопутные войска России.[281]

В 2016 году Андрей Григорьев, директор Фонда перспективных исследований (ARF) – российского аналога DARPA – обсудил изменение отношений между солдатами и роботами, заявив: «Я вижу все большую и большую роботизацию, на самом деле будет война операторов и машин, а не солдат на поле боя, которые стреляют друг в друга. Военные задачи будут решаться с минимизацией потерь личного состава. Солдат постепенно превратится в оператора и уйдет с поля боя».[282] И в 2020 году заместитель директора ARF Виталий Давыдов вторил Григорьеву, заявив, что ни мы, ни какая-либо другая страна не откажемся от использования боевых роботов, если мы не хотим, чтобы люди продолжали гибнуть на поле боя.

Роботизированные «братья», которые могут действовать быстрее, точнее и избирательнее, чем люди, постепенно начнут вытеснять живых бойцов. Но человек поставит задачу и сохранит контроль над действиями роботов.[283]

В 2021 году В.Б. Зарудницкий – начальник Военной академии Генерального штаба Вооруженных Сил, рассказал о растущем технологическом спектре военных систем и ведущей роли России среди иностранных государств в этих тенденциях, включая роботизацию всех сфер вооруженной борьбы, развитие ИИ роботизированных комплексов, расширение круга задач, выполняемых роботизированными комплексами, предоставляя им возможность действовать автономно, переходя от принципа «управления роботом»

---

[281] «Российская армия создаст первое военное подразделение, вооруженное ударными роботами», ТАСС, апрель. 9 декабря 2021 года, https://tass.com/defense/1276039.

[282] «Фонд перспективных исследований считает, что роботы будут вести войны будущего» (Фонд перспективных исследований считает, что роботы будут вести войны будущего), Ria.ru, 6 июля 2016 года, https://ria.ru/20160706/1459555281.html.

[283] «Виталий Давыдов: Солдат заменят терминаторы» «Виталий Давыдов: живых бойцов заменят терминаторы», Риа Новости, 21 апреля 2020 г., стр.202, https://ria.ru/20200421/1570298909.html.

к принципу «постановки задач роботу».[284] Интересное недавнее заявление Виктора Бондарева, бывшего главы Воздушно-космических сил России, также коснулось роли, которую робототехника будет играть в отношении присутствия солдат на поле боя, заявив: Огневая мощь современных систем вооружения многократно возросла по сравнению с оружием предыдущих поколений. Понятно, что, по возможности, человека следует убрать с поля боя, чтобы заменить роботизированными системами. Кроме того, современные развитые государства, в том числе Россия, испытывают серьезные демографические проблемы. И чтобы военнослужащие и военные подразделения не попадали в засаду, теперь можно отправлять боевых роботов. Если робот поврежден и потерян, это не проблема, потому что человеческие жизни будут спасены.[285]

Сложность обсуждения инициатив, связанных с автономными системами, заключается в том, что трудно обсуждать автономию в целом, учитывая как понимание и использование этого термина варьируется в разных дисциплинах и дискуссиях. Существует множество рамок для понимания природы автономных систем и их уровня автономности, начиная с прошлого десятилетия.[286]

Возможно, в самом широком смысле с тех пор, чем большей автономией обладает система, тем меньше она зависит от знаний ее создателя.[287]

Российским военным не хватает четкой таксономии автономных систем и четкого набора официальных определений военной автономии. Например, неясно, существует ли строгое обсуждение разграничения между автономными и полуавтономными системами, как это можно было бы найти в НАТО или Соединенных Штатах.[288]

---

[284] В.Б. Зарудницкий» «Природа и содержание военных конфликтов сегодня и в обозримом будущем», Военная мысль № 1 (2021), https://vm.ric.mil.ru/Nomera.

[285] «Человек должен быть удален с поля боя: боевые роботы вытесняют солдат», Московский комсомолец, 2021, https://www.mk.ru/politics/2021/04/09/cheloveka-s-polya-boya-nado-ubirat-boevye-roboty-tesnyat - soldat.html.

[286] Эндрю Илачинский, Искусственный интеллект, Роботы и рои: Проблемы, вопросы и рекомендуемые исследования, CNA, DRM-2017-U-014796-Финал, 2017, https://www.cna.org/cna_files/pdf/DRM-2017-U-014796-Final.pdf.

[287] Норвиг, Искусственный интеллект: современный подход, стр.42.

[288] Стен Аллик, Шон Фэйхи, Томас Ермалавичюс, Роджер Макдермотт и Конрад Музыка, Появление

В российской военной энциклопедии роботизированная система перечисляется как: Система, способная воспринимать информацию из окружающей среды и, основываясь на этом, выполнять определенные действия как автономно, так и с оператором в контуре управления. Наиболее характерной роботизированной системой в армии на самом деле является беспилотный летательный аппарат с элементами искусственного интеллекта, оснащенный навигационными устройствами и манипуляторами, способными заменить действия человека. Такие роботизированные системы могут использоваться как для ведения боя (например, истребители танков) и боевой поддержки (разведка, минирование и разминирование, дезактивация и т.д.).[289]

Это определение иллюстрирует сложность точности и простоты, когда речь заходит об определении автономии, поскольку оно затрагивает множество различных аспектов автономии, но также пытается включить другие технологии, такие как ИИ или робототехника. Эта проблема определения автономии является характеристикой данной области в целом, а не просто проблемой, с которой сталкивается Россия.[290]

Кроме того, российское определение не проводит различия между автономными системами, не оснащенными оружием, и автономными системами, оснащенными оружием, в отличие от Директивы Министерства обороны 3000.09:

Автономная система вооружения – система вооружения, которая после активации может выбирать и поражать цели без дальнейшего вмешательства человека-оператора. Это включает в себя управляемые человеком автономные системы вооружения, которые предназначены переопределять работу системы оружия, но могут выбирать и поражать цели без дополнительного участия человека после активации.

российских военных роботов: теория, практика и последствия, Международный центр обороны и безопасности, 2021, стр.2, https://icds.ee/en/the-rise-of-russias-military-robots-theory-practice-and-implications.

[289] Министерство обороны Российской Федерации, «Роботизированная система», Робототехническая система, Энциклопедия МО РФ, https://encyclopedia.mil.ru/encyclopedia/dictionary/details_rvsn.htm.

[290] Д-р Винсент Буланин и Маайке Вербрюгген, Анализ развития автономии в системах вооружений, Стокгольмский международный институт исследований проблем мира, 2017, стр.5-8, https://www.sipri.org/publications/2017/other - публикации/картографирование - разработка - автономия - системы вооружения.

Полуавтономная система вооружения – система вооружения, которая после активации предназначена для поражения только отдельных целей или конкретных целевых групп, выбранных оператором-человеком.[291]

Хотя это и не российская конструкция, Эндрю Уильямс предоставляет ряд измерений, с помощью которых можно приблизиться к автономным системам, которые могут быть полезны при рассмотрении связанных с автономией разработок в Вооруженных силах России.[292]

Это не отдельные категории, в которые можно аккуратно поместить различные автономные системы – это не таксономия. Это способ понять, насколько что-то автономно по отношению к своему окружению и намерениям.

Рои роботов и российские военные

Одна из конкретных областей, представляющих интерес, связана с технологией роения.

Роботизированные рои и технология роя относятся к нескольким роботам, коллективно решающим проблемы, в данном случае связанные с военными проблемами.

Концепция основана на естественных системах, таких как рои птиц и рыб.[293] Интерес российских военных к роению связан с российскими усилиями по ускорению развития автономии, связанной с военными, во всем мире, а также с оценкой потенциала роботизированных роев для решения специфических для России проблем безопасности в физических областях. Роботизированные рои обладают потенциалом для решения проблем безопасности России в морской сфере. В то время как российская военно-морская мощь всегда занимала второе место после своей сухопутной мощи, российские подводные технологии и возможности остаются внушительными, и технология роения может дополнить эту мощь.

---

[291] Там же.
[292] Там же.
[293] Умлауфт М, Шранц М, Сенде М и Эльменрайх Ш, «Поведение роботов роя и современные приложения», Спереди Робот. AI (2020): 1, doi: 10.3389/front.2020.00036, https://www.frontiersin.org/articles/10.3389/frobt.2020.00036/full.

В статье в журнале «Военная мысль» отмечается, что ВМФ России разрабатывает самоходные беспилотные летательные аппараты для удовлетворения потребности в увеличении продолжительности пребывания в море для выполнения таких задач, как разведка, особенно в районах, более сложных для пилотируемых систем, таких как поддержание осведомленности на море в Арктике, давняя озабоченность российских военных, учитывая ее протяженную границу с Арктикой и оценки подводных возможностей США.[294]

Кроме того, автор утверждает, что эти небольшие автономные системы обеспечивают превосходство в береговой разведке, противоминной деятельности и противолодочной войне.[295]

Хотя трудно сказать, что потенциал страны с автономными системами четко отражает ее уже существующие военно-технические преимущества, российский военно-морской флот способен представлять передовые подводные системы, которые имели бы по крайней мере некоторую дополнительную ценность в деятельности передовых подводных автономных систем.

В новом отчете с открытым исходным кодом утверждается, что у Министерства обороны России есть проект по борьбе с подводными лодками с использованием беспилотных летательных аппаратов, которые смогут использовать технологию роения с поддержкой ИИ.[296]

Для размещения оружия, необходимого для преследования подводных лодок, беспилотник должен будет иметь значительную полезную нагрузку, такую как S-70 «Охотник».

---

[294] «Главный конструктор Рубина: мы создаем подводный город, чтобы добраться до арктических богатств» Центр робототехники Министерства обороны Российской Федерации: в Арктике появятся карманные микроботы, Тасс, 2017, https://tass.ru/interviews/4502372.

[295] С.М. Черкасов и М.Р. Гизитдинова» «Роль мобильных подводных роботов в решении задач военно-морского флота», Роль мобильных подводных роботов в решении задач Военно-морского флота, Военная мысль, № 1, http://military article.ru/voennaya-mysl/2008-vm/10195-rol-mobilnyh-podvodnyh-robotov-v-reshenii-zadach.

[296] Антон Лавров и Роман Крезул, «Упаковка оружия: Министерство обороны в поисках противолодочного беспилотника: Тяжелый беспилотник будет работать вместе, чтобы обнаруживать и поражать подводные лодки», Упаковка оружия: Министерство обороны в поисках противолодочного беспилотника Тяжелые беспилотники будут работать вместе, чтобы обнаруживать и поражать подводные лодки, Известия, апрель. 2, 2021, https://iz.ru/1145514 anton-lavrov-roman-kretcul/stainoe.

В статье описывается концепция «нескольких охотников» с противолодочным оборудованием обнаружения и оружием, работающими в единой сети.

Эти охотники могут быть запущены как с наземных баз, так и с кораблей.

В статье предполагается, что эти беспилотные летательные аппараты будут полуавтономными, но смогут самостоятельно поражать цели или передавать эту информацию для других платформ.

Учитывая ссылку на неясно, идет ли речь в статье о реальном «рое» или о мультироботизированной системе, содержащей относительно небольшое количество роботизированных систем.[297]

В статье также упоминается противолодочный комплекс «Ответ» в качестве одной платформы, которая будет использоваться в концепции с беспилотными летательными аппаратами.[298]

«Ответ» – это противолодочная торпеда, запускаемая с универсальной пусковой установки, установленной на большинстве новых и модернизированных российских кораблей.

В статье цитируется заявление заместителя Министра обороны Алексея Криворучко о том, что как только подводная лодка будет обнаружена «на расстоянии нескольких десятков километров», ракета «Ответ» сможет доставить торпеду за считанные секунды.

Российские официальные лица также обсудили полезность роботизированных роев для наземных операций.

Например, российские военные чиновники предусмотрели роль роев в городских войнах. Легкие и тяжелые беспилотные летательные аппараты работают совместно с роящимися ISR и боевыми беспилотными летательными аппаратами для поиска и нацеливания на солдат и платформы противника.[299]

---

[297] Илачинский, Искусственный интеллект, Роботы и рои: Проблемы, вопросы и рекомендуемые исследования.
[298] Юрий Гаврилов, «Ищите наш «Ответ» под водой», Наш «Ответ» ищите под водой, Российское оружие, 5 ноября 2020 года, https://rg.ru/2020/11/05/korabli-vmf-usiliat-novym-protivolodochnym-raketnym-kompleksom.html.
[299] Буренок, Дурнев и Крюков, «Интеллектуальное вооружение: Будущее искусственного интеллекта в военном деле».

Во время «Кавказ-2020», одного из ежегодных стратегических командно-штабных учений России, три различных типа беспилотных летательных аппаратов «Форпост», «Орлан-10», «Элерон-3» и другие были «объединены» в одну группу.[300]

Хотя в отчете не приводится информация о количестве реальных платформ, участвующих в группировке, и о том, был ли это настоящий рой, это подчеркивает заинтересованность России в том, чтобы роботизированные рои были частью ее боеспособности.

В аэрокосмической области российские военные стремятся разработать и использовать роботизированные рои для воздушной разведки, радиоэлектронной борьбы и наземных ударов.

Предполагается, что эти системы смогут работать с пилотируемыми самолетами, наземными и морскими роботизированными системами.

Конструкторское бюро Кронштадта недавно анонсировало новую концепцию роботизированного роя под названием «Молния», в которой использовались реактивные беспилотные летательные аппараты-невидимки, способные выполнять задачи воздушного перехвата и наземного удара.[301]

Автономия и конфликт

Подчеркивая важность автономии, и в частности беспилотных летательных аппаратов, в бою, начальник Генерального штаба генерал Валерий Герасимов отметил в 2018 году, что сегодняшние боевые действия немыслимы без беспилотных летательных аппаратов – их используют артиллеристы, разведчики, пилоты – все.[302]

В дополнение к основным мировым тенденциям в автономии, несколько крупных конфликтов определили, как российские военные будут использовать

[300] «Рой беспилотных летательных аппаратов, впервые используемых в учениях «Кавказ-2020» против сил противника», ТАСС, 24 сентября 2020 г., https://tass.com/defense/1204513.

[301] «Роящиеся реактивные беспилотные летательные аппараты в разработке для воздушно-космических сил России», Источник: реактивные беспилотные летательные аппараты, работающие в стае, создаются для Воздушно-космических сил, Риа Новости, 2021, https://ria.ru/20210301/bespilotniki – 1599368302.html.

[302] «Российские беспилотники во время операции в Сирии провели в воздухе более 140 тысяч часов» Официальный сайт Минобороны России, 6 июля 2018 г., http://syria.mil.ru/news/more.htm?id=12184627@egNews.

свои беспилотные и автономные военные системы – Сирия и Нагорно-Карабахская война 2020 года.

В то время как российские вооруженные силы на востоке Украины действительно использовали беспилотные летательные аппараты, в основном для разведки и обнаружения артиллерии, российские сообщения об их использовании довольно ограничены.

Однако российское военное руководство заявило о преимуществах автономии в опыте российских военных в Сирии. К июлю 2018 года число полетов российских беспилотных летательных аппаратов в Сирии превысило 23 000, что составило 140 000 летных часов.

Этим успехом мы обязаны многочисленным дронам ISR малой и средней дальности платформы. Тем не менее, в Сирии у России не было настоящего боевого беспилотника, способного поражать цели, оставляя эту роль укомплектованным артиллерийским и авиационным подразделениям.

Сегодня российский парк беспилотных летательных аппаратов расширился до более чем 2 000 беспилотных летательных аппаратов, а наземные войска летают примерно на 1 500 беспилотных летательных аппаратах.

Аналогичным образом Сирия продолжает служить важным испытательным полигоном для российской технологии беспилотных наземных транспортных средств (UGV) для таких миссий, как разминирование и ISR.

Испытанные в Сирии беспилотные Уран-6 и Уран-9 поступают на вооружение инженерных, боевых и саперных подразделений и Министерство обороны использует полученные в Сирии знания для наращивания внутреннего и международного опыта в операциях по разминированию.

В апреле 2021 года Министерство обороны объявило, что российские сухопутные войска в Сирии успешно использовали тактический уровень модернизированного носимого комплекса разведки, управления и связи (KRUS)

«Стрелец-М» – для наведения тактических ударных беспилотных летательных аппаратов «Орион» на цели террористов в ходе испытания системы.[303]

Еще одним ключевым конфликтом, который привлек внимание Министерства обороны, была недавно завершившаяся Нагорно-Карабахская война 2020 года, где атакующие азербайджанские ISR и боевые беспилотник и, бронетехника и наземные войска разгромили армянские силы всего за несколько недель.

Одним из ключевых выводов из конфликта стала сложность защиты от многочисленных небольших беспилотных летательных аппаратов.[304]

Отмечая это, Министерство обороны России заявило о необходимости использования ряда беспилотных летательных аппаратов в боевых и пассивных ролях для эффективного проникновения в противовоздушную оборону противника, нейтрализации наземных формирований и работы в роях.[305]

В качестве примера Ростех недавно объявил, что российские войска испытали два беспилотных летательных аппарата в Сирии, Kub и Lancet, и что российские военные будут иметь приоритет в их приобретении в ближайшем будущем. Министерство обороны публично заявляет о присутствии российских военных в Сирии и подробно обсудило уроки Нагорного Карабаха.

В то же время международные наблюдатели отметили и зафиксировали российские беспилотники на Востоке Украины, выполняющие задачи ISR и радиоэлектронной борьбы.

Уроки Украины, безусловно, дополняют формулировку МО оперативных концепций военной автономии. Взятые вместе, эти конфликты заставляют российских военных стремиться к увеличению потенциала ISR.[306]

---

[303] «Минобороны испытало в Сирии уникальный метод наведения боевых беспилотников» Риа Новости, 4 апреля 2021 года, https://ria.ru/20210404/siriya - 1604135512.html.

[304] Майкл Кофман, «Взгляд на военные уроки нагорно-карабахского конфликта: для великих и средних держав было бы ошибкой игнорировать нагорно-карабахский конфликт», «Москва Таймс», 21 декабря 2020 г., https://www. themoscowtimes.com/2020/12/21/.

[305] Руслан Пухов, «Вторая карабахская война: предварительные уроки», ONvo.Ng.ru, 22 октября 2020 года, https://nvo.ng.ru/realty/2020-10-22/1_1114_karabakh.html.

[306] Антон Лавров и Роман Крезул, «Разведка беспилотниками: в войсках появились беспилотники bloodhound: Новые беспилотники специализируются на обнаружении средств ПВО противника», Izvestia.ru, ноябрь 2020 года, https://iz.ru/1089566/anton - лавров-роман-креткул/разведка-дроном-в-войсках - появились-беспилотники-ищейки.

ИИ в автономных и полуавтономных системах

Министерство обороны координирует ресурсы для разработки, оценки и возможного развертывания военной автономии, при этом ИИ в настоящее время является основным компонентом в разработке и закупке таких систем.[307]

В большинстве публичных заявлений ИИ обсуждается с точки зрения командования, управления и ISR для разработки и тестирования беспилотных и автономных транспортных средств.

В частности, российские военные считают беспилотные летательные аппараты важными передовыми ISR и боевыми платформами, которые сводят к минимуму как количество необходимого персонала, так и опасность, часто связанную с разведывательными миссиями.

В ответ на настоятельную потребность Министерства обороны в боевых беспилотных летательных аппаратах отечественного производства предприятия оборонно-промышленного комплекса выпускают несколько боевых беспилотных платформ с поддержкой ИИ.

Российские боевые беспилотники дальнего действия «Сокол Альтиус-У» и С-70 «Охотник» будут оснащены элементами ИИ для управления, а также позволят им работать на некотором уровне автономии. Эти системы также смогут взаимодействовать с пилотируемыми самолетами в конфигурации «лояльного ведомого». Министерство обороны недавно объявило, что Охотник будет взаимодействовать с пилотируемым российским истребителем пятого поколения Су-57, пилот которого будет командовать БПЛА.[308]

Оба беспилотных летательных аппарата предназначены для проникновения в противовоздушную оборону противника, обнаружения и атаки важных целей, таких как ракетные установки, самолеты противника и центры управления и контроля противника. Охотник, скрытный 20-тонный

[307] Роман Бирюлин, «Интервью с Алексеем Криворучко, заместителем министра обороны Российской Федерации», Redstar.ru, 30 декабря 2020 года, http://redstar.ru/oruzhie-rossii-operezhaet-vremya.
[308] Антон Лавров, «Закрытое небо: Россия работает над инновационным воздушным боем», в России создается инновационная система воздушных боев, Известия, 24 февраля 2021 г., https://iz.ru/1127710/anton - лавров.

беспилотный летательный аппарат со смешанным крылом, первоначально был создан для конфликтов высокой интенсивности с возможностью выполнения роли перехватчика.[309]

В сентябре 2019 года Министерство обороны впервые провело первый полет лояльного ведомого, когда Су-57 и беспилотный летательный аппарат S-70 «Охотник» полетели вместе, что ознаменовало важный шаг в развитии российской автономии и «лояльного ведомого». Недавно Министерство обороны объявило, что «Охотник» может запускать гиперзвуковые ракеты при полете вместе с Су-57 – Министерство обороны утверждает, что эта конфигурация потенциально может заменить целые эскадрильи пилотируемой авиации, что побудило российских военных начать разработку совершенно новых БПЛА для использования как пилотируемой, так и в беспилотной авиации. Потенциально это может включать в себя дроны, такие как «Охотник» или «Альтиус», которые запускают свои собственные рои боевых дронов, такие как недавно анонсированная «Молния», против воздушных и наземных целей противника.

В апреле 2021 года Андрей Ельчанинов, первый заместитель председателя Правления Российской военно-промышленной комиссии, заявил, что ввод в эксплуатацию «Охотника» должен начаться в 2024 году.[310]

На данный момент не похоже, что Россия способна производить полностью военные автономные концептуальные транспортные средства, предусмотренные ARF. Тем не менее, он экспериментирует с этой технологией.

Например, ARF разрабатывает платформы, которые будут служить испытательными стендами для экспериментов.

ARF разработал проект Маркер UGV также в качестве испытательного стенда для различных отечественных технологий, имеющих военное

---

[309] «Тяжелый российский беспилотник Altius с искусственным интеллектом», TopWar.ru, марта. 27, 2020, https://topwar.ru/169438-altius-tjazhelyjrossijskij - bespilotnik-s-iskusstvennym-intellektom.html.

[310] «Российские войска, начнут получать «охотника» для атак на беспилотники в 2024 году» – ТАСС 13 апреля 2021, https://tass.com/defense/1277657.

применение, что позволяет частным и государственным компаниям налаживать отношения с Министерством обороны.

Маркер действует как универсальная платформа с модульной архитектурой для тестирования глубоких нейронных сетей для содействия принятию решений, концепций объединения пилотируемых беспилотных летательных аппаратов и взаимодействия с существующими и будущими БПЛА.[311]

Ростех также работает над созданием жизнеспособного испытательного стенда с использованием беспилотной версии нового основного боевого танка Т-14 «Армата». Разработчики «Арматы» недавно объявили, что беспилотная версия Т-14 не будет производиться серийно, но послужит демонстратором передовых робототехнических технологий.[312]

Министерство обороны намерено использовать дополнительные концепции UGV в качестве испытательных стендов для совершенствования технических возможностей и боевого применения.[313]

Развитие возможностей большей автономности с использованием существующих гусеничных и колесных платформ становится основной тенденцией как в Министерстве обороны, так и в военно-промышленном комплексе страны.

Использование существующих платформ путем преобразования их в автономный, полуавтономный или даже дистанционно управляемый режим сэкономило разработчикам, таким как Уралвагонозавод, время и деньги, поскольку им не нужно создавать новые системы с нуля, а вместо этого они могут строить на проверенных платформах танков или бронетехники.

Другим соответствующим примером того, как отечественная промышленность реагирует на потребности в военной автономии, является

---

[311] Олег Мартьянов: «Армии терминаторов не будет. Там будет целая армия маркеров» Олег Мартьянов: в будущем будет не армия терминаторов, а армия умных «Маркеров», Tass.ru, 29 июня 2020 года, https://tass.ru/interviews/8831445.

[312] «Беспилотная «Армата» не будет производиться серийно», Риа Новости, 8 февраля 2021 г., https://ria.ru/20201207 armata - 1587961052.html.

[313] «Генеральный штаб рассказал о разработке перспективных систем вооружения», в Генштабе рассказали о разработке перспективных комплексов вооружения, Tass.ru, https://tass.ru/armiya-i-opk/10644329.

разработка Ростехом автоматизированной интеллектуальной системы управления роботизированными формированиями, использующей нейронные сети.

Разработчик утверждал, что система объединяет целевую информацию, полученную из нескольких источников, таких как спутники, беспилотные летательные аппараты или радары, и передает эти данные роботизированным системам, участвующим в боевых действиях.

Ростех заявил, что новая разработка в три раза повышает эффективность боевых систем за счет минимизации участия человека в процессе командования и управления.[314]

В море российские военные успешно испытали глубоководный беспилотный подводный аппарат «Витязь» (UUV), который спустился на дно Марианской впадины, самой глубокой и неисследованной части мирового морского пространства. Команда разработчиков утверждала, что бортовой ИИ позволил улучшить ситуационную осведомленность и принятие решений.[315]

Еще одним заметным проектом является беспилотный летательный аппарат Galtel, который исследовал морское дно у порта Тартус в Сирии, в котором предположительно также имелся бортовой ИИ для принятия решений и навигации.[316]

Сегодня российское военно-морское руководство готовит службу к будущим боевым действиям, подчеркивая, что подготовка экипажа должна включать эксплуатацию современного оборудования и оружия с высокой степенью автоматизации.[317]

Военная экосистема ИИ

[314] «Российские ученые работают над созданием нейронной сети, которая будет управлять роботами во время операций по разминированию», TvZvezda.ru, 26 августа 2020 года, https://tvzvezda.ru.
[315] «Витязь стал первым «роботом», достигшим дна Марианской впадины», Риа Новости, 9 мая 2020 года, https://ria.ru/20200509/1571206567.html?in.
[316] «Российский подводный робот выполнил свою военную миссию в Сирии», Российская газета, 22 февраля 2018 г., https://rg.ru/2018/02/22/rossijskij - podvodnyj-robot-vypolnil-boevuiu-zadachu-v-sirii.html.
[317] «Главнокомандующий ВМФ России рассказал о подготовке экипажей», Flot.com, 14 января 2021 года, https://flot.com/2021/%D0%92%D0%BC%D1%841.

Российская военная экосистема ИИ и робототехники быстро развивается, и новые организации и центры объединяют существующие усилия. Крупные организации с существующими программами учета, государственным финансированием и проверенными концептуальными решениями также расширяют сферу своей деятельности.

В связи с растущим интересом Министерства обороны к разработке и применению ИИ и робототехники, ключевые участники получат все большую финансовую и логистическую поддержку.

Одной из важных тенденций для мониторинга является то, что все больше российских университетов присоединяются к исследованиям военного и двойного назначения в области военного применения ИИ и робототехники, учитывая заявления Министерства обороны на выставке «АРМИЯ-2020» о том, что должно быть больше взаимосвязей и сотрудничества между гражданскими и военными организациями.

Еще одной важной тенденцией является финансирование и поддержка работы в правительственных и государственных учреждениях между военными и гражданскими усилиями в области ИИ и робототехники.

В очередной попытке связать военные и гражданские исследования Министерство обороны совместно с Курчатовским институтом запускают межведомственный и междисциплинарный рецензируемый научный журнал под названием «Вестник военного инновационного технополиса».

По словам полковника Дмитрия Теребова, заместителя начальника Главного управления научно-исследовательской деятельности Министерства обороны России, издание журнала будет способствовать широкому освещению результатов прорывных разработок и достижений технополиса, а также объединит научное сообщество, представителей гражданского и военного секторов в целях развития научного, технологического и промышленного потенциала страны и укрепления ее обороноспособности.[318]

---

[318] «Достижения ведущих ученых страны будут опубликованы в Бюллетене Военного инновационного технополиса «ЭРА»», 2021, https://function.mil.ru/news_12349063@egNews.

Наконец, на данный момент неясно, присоединяются ли российские негосударственные компании частного сектора к этим направленным усилиям, их неуверенность в этом или их нежелание участвовать в отечественных военных исследованиях и разработках может помешать им сделать это.

ИИ и связанные с автономией российские военные платформы

Как и в любой классификации ИИ и автономных систем, между категориями существует затруднения.

Исследуя российские системы, связанные с ИИ, мы изучали те системы, возможности которых с улучшением ИИ были неясны. Во многих случаях отчетность просто утверждает, что в системе есть «компоненты ИИ» с небольшим количеством деталей, если таковые имеются. Поскольку цель этого отчета – составить карту российской экосистемы ИИ и автономии, мы сочли за лучшее включить любое упоминание об ИИ или автономии.

Например, российское правительство не раскрыло уровень ИИ или автономии с помощью своего UUV Посейдон – по сути, торпеды с ядерным наконечником для поражения прибрежных районов.

Однако были предположения, и мы включаем их там, где это кажется разумным. Там, где платформам не хватает названий, команда не смогла их найти.

Например, в отчете будет содержаться ссылка на беспилотный летательный аппарат, разрабатываемый Министерством обороны, с утверждениями о его расширенных возможностях ИИ без указания имени.

Наконец, мы надеемся, что этот список является достаточно полным на момент написания, но обратите внимание, что он отражает только системы, найденные в отчетах с открытым исходным кодом.

Выбор российских военных платформ

РБ-109 А «Былина».

Тип системы ИИ/Аспект автономности – это российская платформа радиоэлектронной борьбы (РЭБ), предназначенная для обеспечения ситуационного понимания, управления и контроля, а также возможностей подавления помех на электронном поле боя.

Система состоит из пяти грузовиков с несколькими секциями персонала и, вероятно, развернута на уровне бригады РЭБ. Согласно сообщениям из открытых источников, после развертывания система автоматически устанавливает каналы связи с вышестоящими штабами, родственными батальонами РЭБ, нижестоящими эшелонами и другими отдельными системами РЭБ, такими как «Москва-1», «Силицы-2», «Палатин» и «Тирда-2».

Система предположительно исследует электронную среду, различая различные типы излучающих платформ и указывая, являются ли они друзьями или врагами, без помощи человека-оператора.

Платформы, конкретно указанные в отчетах, включают радиостанции, системы связи, радиолокационные системы, спутниковую связь и AWCAS. Есть конкретные ссылки на способность системы находить маломощные радиостанции, используемые диверсантами – общая тема в российских репортажах, в которых часто упоминаются силы специальных операций противника, представляющие опасность для российских платформ РЭБ и C2.

Основываясь на этой ситуационной осведомленности, «Былина» якобы способна самостоятельно глушить системы противника, не создавая помех российским силам. «Былина» прошла официальное тестирование в 2017 году, кульминацией которого стало ее участие в стратегических военных учениях «Запад-17».

Развертывание началось в 2018 году и Министерство обороны заявило, что его цель – внедрить систему во все свои бригады РЭБ к 2025 году.

Галтель

Российский оборонно-промышленный комплекс разрабатывает, тестирует и оценивает широкий спектр беспилотных подводных/надводных аппаратов

(UUVS/USV), некоторые из которых, как сообщается, используют технологию ИИ.

Они варьируются от небольших концепций «планера» до больших глубоководных аппаратов, способных работать на глубине нескольких километров. Хотя в открытых источниках имеется много информации об этих испытаниях, Министерство обороны России сделало только одно официальное признание в использовании UUV в военной миссии на Ближнем Востоке.

Галтель – подводный разведывательный робот.

Система впервые была публично упомянута в 2012 году на саммите АТЭС во Владивостоке и наиболее известна своими операциями в Сирии в поддержку российских военно-морских сил там.

В 2017 году комплекс был представлен для выполнения своей первой успешной миссии, в ходе которой он патрулировал воды у российского логистического объекта Тартус и завершил подводные исследования дна океана.

В интервью «Интерфаксу» член Военно-промышленной комиссии Олег Мартьянов заявил, что в дополнение к указанным выше работам комплекс может проводить работы на инженерных сооружениях, кабельных и магистральных трубопроводах. Угрозы подводным кабелям, особенно тем, которые соединяют США и их европейских союзников, являются заметной проблемой США/НАТО.

Комплекс включает в себя две автономные необитаемые подводные лодки с предельным сроком эксплуатации 24 часа и дальностью до 100 километров, согласно российской отчетности.

В отчете также утверждается, что он может обследовать площадь в четыре квадратных километра за 12 часов. Компоненты ИИ его системы управления якобы позволяют ему самостоятельно оценивать текущую ситуацию, обходить препятствия и выбирать наилучший курс для выполнения своей миссии.

ПОМ-3 «Медальон»

Российские военные разрабатывают и, возможно, уже устанавливают передовые наземные мины, которые используют некоторые возможности ИИ.

В 2015-2017 годах появились сообщения о том, что наземная мина ПОМ-3 «Медальон» обладает новыми функциями и возможностями, ранее не встречавшимися в советских или российских наземных минах.

Поверхностные возмущения, его профиль анализируются алгоритмами и определяется являются ли они друзьями или врагами. Алгоритм использует различные сигнатуры, которые делает идущий солдат со своим снаряжением, по сравнению с идущим гражданским лицом. Когда мина определяет, что угроза вошла в ее радиус поражения, она запускает свою боеголовку на высоту от 1 до 1,5 метров, прежде чем взорваться.

Название «Медальон» происходит от формы дисков внутри боеголовки, которые разбиваются на вращающиеся треугольные фрагменты.

Наземные мины, использующие сигнатуры, не являются новыми (примером являются морские мины, использующие записи сигнатур судов), поэтому аспект ИИ мины не обязательно ясен из отчетности.

Также интересно, что мина якобы может идентифицировать классы людей – например, она может отличить фермера или туриста от солдата. Также неясно, какие предположения должна сделать мина, чтобы сделать это.

ПОМ-3 – это противопехотная осколочная мина, которая способна развертываться с многочисленных платформ и имеет предполагаемый радиус поражения 12 метров.

Научно-исследовательский инженерный институт (НИИИ) занимается разработкой взрывных устройств, в том числе оружия, с 1950 года.

НИИИ входит в состав более крупного концерна «Техмаш» (http://tecmash.ru), основное производство которого состоит из боеприпасов для российских военных.

Техмаш входит в состав более крупной оборонной компании Ростех (http://rostec.ru). ПОМ-3 также демонстрировался на военном форуме «Армия-2019», проходившем в Москве.

КАМАЗ

Лаборатория автономных транспортных систем, входящая в состав Центра технологических компонентов робототехники и механики Университета Иннополис (www.robotics.innopolis.university) разрабатывает автономный грузовик Камаз, который использует бортовой модуль воздушной разведки.

Ученые утверждают, что создали свои собственные алгоритмы распознавания, классификации и маршрутизации объектов.

По словам директора центра Салимжана Гафурова, система предположительно создает 2 048 различных траекторий для ожидаемого движения транспортного средства в течение следующих 6,5 секунд и обновляет их каждые 0,05 секунды.

Кроме того, система постоянно отслеживает 360 градусов вокруг автомобиля на расстоянии 220 метров.

С помощью бортового беспилотного летательного аппарата (хранящегося и заряжаемого на платформе грузовика) грузовик может перемещаться по местности без использования карт.

Грузовик действительно сохраняет водителя, хотя разработчики утверждают, что в нем нет определенной необходимости.

Грузовик проехал более 3 000 километров по территории комплекса Иннополис. Центр использует собственный симулятор для проверки способности транспортного средства реагировать на различные ситуации.

В онлайн-источнике не упоминаются какие-либо военные аспекты этой технологии, хотя они очевидны. Российские военные планировщики оценивают, что электронная среда современного поля боя, включая

доступность космической информации, вероятно, будет сильно скомпрометирована.

Система, подобная той, что разрабатывается в центре, соответствовала бы российским усилиям по поддержанию военного потенциала в неблагоприятных условиях.

Су-35С

В соответствии с усилиями российских военных по интеграции элементов ИИ в свои силы, российские воздушно-космические силы выделили ряд областей, в которых, по их мнению, технологии, связанные с ИИ, могут дополнить успех миссии – от управления самолетами до обнаружения и поражения целей. Российский Су-35С, тяжелый многоцелевой истребитель большой дальности, является одним из примеров, упоминаемых в СМИ как включающий ИИ.

Су-35С использует бортовую информационно-управляющую систему IUS-35 (ИУС-35), которая состоит из нескольких компьютеров БЮДЖЕТ-53-31М.

Система объединяет многие из ранее отдельных информационных каналов внутри воздушного судна в единую систему, предназначенную для объединения, автоматизации и оптимизации информации для пилота, чтобы повысить его осведомленность о ситуации.

Также система обеспечивает «интеллектуальную поддержку» пилоту посредством собственного обнаружения цели, ориентирования самолета относительно цели и подготовки его систем вооружения к бою.

С добавлением этой системы возможно увеличение числа боевых вылетов, которые Су-35С смог совершить в сирийском конфликте, до 10 в день.

Предположительно, это было сделано благодаря предполетной подготовке и более высокой выносливости пилота благодаря более интеллектуальному управлению информацией.

«Маркер»

Фонд перспективных исследований (ФПИ) и НПО «Андроидная техника» (разработчики робота Федор) совместно разрабатывают маркер беспилотного наземного транспортного средства (UGV) для Министерства обороны России, описывая его как «помощника солдата на поле боя».

ФПИ использует платформу для тестирования различных технологий UGV, включая машинное зрение, связь, автономное движение и навигацию, а также технологии группового роения.

Модульные технологии Маркера позволяют исследователям тестировать различные возможности как Маркера, так и других UGV. Компания также тестирует программное обеспечение для распознавания голоса, чтобы в конечном итоге управлять человеческим голосом.

В настоящее время ФПИ планирует пять вариантов Маркера: две гусеничные модели; две колесные модели; пятая модель, которая будет включать результаты предыдущих исследований.

Олег Мартьянов, директор Национального центра развития технологий и базовых элементов робототехники, ведущего исследовательского центра ФПИ по Маркеру, недавно прокомментировал потенциальные возможности роя Маркера.

Он описал сценарий, в котором пять платформ-маркеров выполняют определенную задачу автономно, обмениваясь информацией между собой. Он также упомянул об использовании нейронных сетей при описании технологий, задействованных в платформе маркеров.

Конечной целью, по его словам, было «научить» Маркер самостоятельно выполнять задачи на больших расстояниях от оператора.

В качестве боевой машины Маркер может использовать широкий спектр оружия, включая крупнокалиберный пулемет (12,7 мм), противотанковые управляемые ракеты и гранатометы.

Как показано в видео (ссылка ниже), солдат может обозначать цели маркером из оружия солдата.

Маркер также сможет запускать свои собственные органические беспилотные летательные аппараты (квадрокоптеры) как для разведки, так и в качестве доставки боеприпасов, способных поражать цели.

Видео, рекламирующее военные возможности Маркера, можно найти по адресу: https://fpi.gov.ru/projects/fiziko-tekhnicheskie-issledovaniya/marker/).

Комплекс «Поверхность»

Согласно российским источникам новостей, Военно-морской флот России проводит испытания и готовится к развертыванию минных полей, называемых абревиатурой «Поверхность», в которых используются элементы ИИ.

Эти системы предположительно анализируют звук, магнитное поле – магноакустический «портрет» кораблей, подводных лодок и судов на воздушной подушке.[319]

Компонент ИИ центра управления минными полями идентифицирует и решает, на какие платформы нацеливаться, и способен определять «своих» на основе сигнатуры судов.

После развертывания мины способны самоорганизовываться на основе магнитных и акустических сигнатур платформ в своем районе, используя предполагаемую способность к самообучению с поддержкой ИИ. Он также может выполнять конкретные задачи, например, избегать кораблей, обнаруживающих мины, и подстерегать для уничтожения только десантные корабли.

Бывший начальник Главного штаба военно-морского флота отметил в интервью, что, хотя военно-морские силы традиционно использовали мины в прибрежных районах для защиты военно-морских баз, эти новые технологии

[319] Алексей Рамми Алексей Козаченко, «Хорошая мина при морской: флот получит боеприпасы с искусственным интеллектом: для ВМФ готовят самообучающиеся заградительные пола», Izestia, Mar. 2019, accessed Oct. 2020, https://iz.ru/841783/aleksei-ramm-alekseikozachenko/khoroshaia-mina-pri-morskoi-igre-iskusstvennym-intellektom.

позволяют минам действовать вдали от берега, в районах предполагаемой военно-морской активности противника.

В более ранних сообщениях говорилось, что на многочисленных платформах может быть развернута противоминная система, однако в более поздних отчетах за прошлый год самолет-амфибия Бе-12 был выделен в качестве основного носителя для «Поверхности».[320]

Хотя самолет является одним из старейших в российском военно-морском флоте, модернизация сохранила его работоспособность.[321]

Самолет может вести трехчасовое патрулирование с приблизительной дальностью действия 600 км.

«Алтиус»

Новый российский беспилотный летательный аппарат «Альтиус», разрабатываемый с 2011 года, предположительно включает в себя технологии, связанные с ИИ, обеспечивающие определенный уровень автономии при проведении операций.

В 2019 году предприятие УЗГА представило модифицированную версию этого беспилотника, который получил систему спутниковой связи.

При использовании такой системы дальность полета «Альтиус» была бы ограничена только запасом топлива на борту.

Такая система позволяет этому беспилотнику вести разведку и атаковать цели на расстоянии сотен или тысяч километров от своей базы.

«Альтиус» может находиться в воздухе от 24 до 48 часов, а его максимальная дальность полета может достигать 10 000 километров, при этом беспилотник проводит разведку с высоты 12 000 метров.

---

[320] Кирилл рябов, «Комплекс «Поверхность». Умные мины для военно-морского флота» Topwar.ru, Sept. 2019, accessed Oct. 2020, https://topwar.ru/162249-kompleksposverhnost-umnye-miny-dlja-voenno-morskogo-flota.html.

[321] Алексей Рамми Алексей Козаченко ««Чайка» - носитель: самолеты Бе-12 вооружат умными минными комплексами, Амфибии смогут устанавливать самообучающиеся заградительные поля», Izvestia, Sept. 2019, accessed Oct. 2020.

В конце 2019 года Министерство обороны подписало соглашение с УЗГА о создании улучшенной версии «Альтиус», которой было присвоено обозначение «Альтиус-РУ» (разведывательный).

Эта версия должна стать основной линейкой серийного развертывания для поставок в Воздушно-космические силы России и Военно-морской флот России. «Альтиус» будет оснащен инерциальной навигационной системой SP-2, обеспечивающей БПЛА дополнительную устойчивость к наведенным помехам и способность работать в условиях радиоэлектронного противодействия противника.

«Альтиус» может поднимать до одной тонны бомб и ракет. Предполагается, что беспилотник сможет нести бомбы «Гром-2» общей массой 598 кг (масса боевой части 480 кг) и дальностью пуска 10-50 км, или управляемые ракеты «Гром-1» массой 594 кг (масса боевой части 315 кг) с дальностью пуска до 120 км.

Во время визита заместителя министра обороны по вооружениям Алексея Криворучко в июне 2020 года на объект УЗГА впервые были опубликованы фотографии обновленной модели «Альтиус».

Затем было подтверждено, что беспилотник сможет не только проводить разведывательные миссии, но и наносить удары по наземным целям противника.

Этот беспилотник будет оснащен элементами ИИ, а также сможет взаимодействовать с пилотируемыми самолетами в конфигурации MUM-T.

Предусматривается, что этот беспилотник будет работать автономно без участия оператора, а также независимо взаимодействовать с российским истребителем пятого поколения Су-57.

Предполагается, что беспилотник самостоятельно прокладывает маршрут к цели или заданному району патрулирования без помощи оператора-человека, обходя средства ПВО противника, а также обнаруживая и атакуя важные наземные цели, такие как ракетные пусковые установки, центры связи и центры управления противника.

Как и предполагалось, как только он получит координаты цели, «Альтиус» сможет составить алгоритм поиска оптимального маршрута к цели и рассчитать наиболее подходящую точку для сбрасывания бомб.

Беспилотник сможет делать все это без помощи оператора, так как БПЛА получает необходимую информацию об объектах ПВО противника в режиме реального времени, чтобы построить траекторию своего полета.

Выполнив свою боевую задачу, «Альтиус» должен иметь возможность автоматически вернуться на базу по наиболее безопасному маршруту полета или вернуться в режим патрулирования и продолжить выполнение разведывательных задач.

Стоит отметить, что операторы, работающие на всех этапах полета БПЛА, в настоящее время управляют российскими военными беспилотниками во время операций.

Центр управления национальной обороной

Одним из примеров того, как технологии с поддержкой ИИ могут быть внедрены в процесс принятия решений в российских вооруженных силах, является Национальный центр управления обороной (NDMC), «нервный центр» российских военных, которому поручено ежедневно, круглосуточно оценивать и координировать деятельность в области военной и национальной безопасности внутри страны и на международном уровне.

Согласно имеющимся данным из открытых источников, российские военные будут использовать ИИ в NDMC, но не будут передавать принятие решений на аутсорсинг системам ИИ. Вместо этого технологии ИИ будут помогать в принятии решений, включая сбор и представление всей необходимой информации, чтобы операторы-люди могли четко понимать статус российских вооруженных сил и состояние воинских частей в стране и в международных развертываниях.

Согласно официальным заявлениям, NDMC предположительно содержит самые мощные в России аппаратные и программные системы, а также мощный компьютер военного назначения. Центр был запущен 1 декабря 2014 года.

Являясь ближайшим аналогом Национального военного командного центра США в Пентагоне, этот первый в своем роде российский объект выполняет следующие официальные функции, сформулированные Министерством обороны России:

- Поддерживает централизованную систему боевого управления для обеспечения боевой готовности.
- Контролирует состояние вооруженных сил и стратегически развернутых сил и помогает им в выполнении своих боевых обязанностей.
- Информирует руководство Министерства обороны, Ситуационный центр Министерства обороны и государственных должностных лиц о военно-политической обстановке во всем мире и социально-политической ситуации на всей территории Российской Федерации.
- Контролирует и координирует полеты и воздушное движение российских вооруженных сил.
- Управляет, координирует и контролирует военно-морские силы во время боевых и международных операций, а также обеспечивает материально-техническую и программную поддержку военно-морской деятельности.

Для выполнения этих функций, NDMC состоит из трех основных департаментов:

- Центр управления Стратегическими ядерными силами управляет использованием Россией ядерного оружия и может развертывать такое оружие по решению высших военных и политических должностных лиц.
- Центр боевого управления отслеживает военно-политические события по всему миру, прогнозирует потенциальные угрозы для России и ее союзников и управляет вооруженными силами, не входящими в состав Министерства обороны, такими как Национальная гвардия.

- Центр управления повседневной деятельностью управляет снабжением, техническим обслуживанием и материально-техническим обеспечением, а также состоянием здоровья вооруженных сил страны.

На официальном открытии NDMC Министр обороны Сергей Шойгу заявил, что центр является «шагом к формированию единого информационного пространства для решения задач в интересах обороны страны». Шойгу далее заявил, что NDMC задумывался как круглосуточный механизм управления всеми сферами деятельности вооруженных сил России.

Например, он должен обеспечивать способность и готовность войск выполнять свои задачи; обеспечивать выполнение государственного оборонного заказа; распоряжаться финансовыми и материальными ресурсами, включая набор войск и подготовку личного состава; решать медицинские и жилищные вопросы; и помогать управлять международной деятельностью России.

Центр собирает ключевую информацию от региональных и территориальных командований, а также воинских частей и пунктов управления. NDMC был разработан для получения информации с самых низких уровней воинских подразделений и, после анализа и оценки, передачи данных непосредственно тем, кто находится на стратегическом уровне.

Он в кратчайшие сроки объединяет работу военного руководства, органов исполнительной власти и органов местного самоуправления, позволяя Совету национальной безопасности России, Генеральному штабу Вооруженных Сил, руководителям федеральных органов исполнительной власти и различным оборонным структурам работать вместе.

Согласно сообщениям, официальные представители NDMC утверждают, что центр отслеживает и координирует с помощью видеопотоков и в режиме реального времени все основные этапы производства и ремонта военной техники, начиная с подписания государственного контракта и запуска продукции и заканчивая доставкой конкретного оружия в конкретную воинскую часть. Для выполнения этой задачи сотрудники NDMC отслеживают

такую деятельность с помощью 700 камер на 500 военно-промышленных объектах по всей стране и их содержимое, предположительно, анализируется шесть раз за каждую смену NDMC. До создания NDMC такой обмен информацией был «немыслимым». Наиболее сложной и трудоемкой задачей для военных было заниматься сбором и анализом различных данных и информации.

По словам министра обороны Сергея Шойгу, суперкомпьютер центра, который является единственным в российской оборонной системе, может хранить 236 петабайт данных (против 12 петабайт Пентагона), а его производительность оценивается в 16 петафлопс (против 5 петафлопс Пентагона); скорость обработки информации эквивалентна 50 Библиотекам имени Ленина в секунду (Библиотека имени Ленина является Государственной библиотекой России и насчитывает 17,5 миллиона книг). Суперкомпьютер центра, разработанный российской Объединенной приборостроительной корпорацией, как сообщается, защищен от кибератак; аппаратное и программное обеспечение NDMC полностью произведено в России.

«Мста-СМ» 2С19 М2

Министерство обороны оснащает войска Южного военного округа новейшими самоходными роботизированными артиллерийскими системами Мста-СМ 2С19М2 и ожидает, что поставки будут завершены в течение одного-двух лет.

Эти системы не только обладают повышенной дальностью и точностью, но и могут использовать «умные» высокоточные снаряды.

Преимущества «Мста-СМ» заключаются в роботизации интеграции системы тактического управления – новой автоматизированной системы наведения и управления огнем для гаубиц.

В результате каждая боевая машина теперь может автоматически обмениваться информацией с командными пунктами батальонов и батарей,

а также с артиллерийскими радарами. Это включает в себя возможность получать и передавать информацию о каждом произведенном выстреле.

При необходимости «Мста-СМ» может функционировать удаленно. Возможности «Мста-СМ» также выиграют от более тесной интеграции с беспилотными летательными аппаратами «Орлан-10», которые проводят разведку и помогают координировать стрельбу по всей дальности стрельбы этих гаубиц.

Научно-исследовательский институт электронных устройств Ростеха (входит в концерн «Техномаш» Госкорпорации Ростех) также разработал боеприпасы с поддержкой ИИ, которые могут достигать цели, несмотря на радиоэлектронные средства противодействия противника.

С-500 «Прометей»

30 декабря 2020 года заместитель министра обороны России Алексей Криворучко объявил, что Россия планирует завершить испытания ракетного комплекса С-500 «Прометей» и официально приобретет его в 2021 году.

С-500 производится оборонной корпорацией «Алмаз-Антей».

Ранее заместитель Главнокомандующего Воздушно-космическими силами России генерал-лейтенант Юрий Грехов отметил, что С-500 разработан с использованием отечественных электронных компонентов и с высокой степенью автоматизации всех боевых процессов и операций.

Предлагаемая автоматизация является частью более широких усилий Министерства обороны по автоматизации множества функций в российских военных системах, которые включают боевые машины всех типов, беспилотные и автономные системы и вспомогательные комплексы, такие как С-500.

Производители утверждают, что S-500 способен уничтожать все воздушные цели в радиусе 400 километров. Кроме того, они утверждают, что он может уничтожать приближающиеся гиперзвуковые ракеты на расстоянии 600 километров.

Система также предназначена для перехвата межконтинентальных баллистических ракет (МБР) ближе к концу их траектории.

Ракеты С-500 предположительно могут достигать объектов космического базирования на низких орбитах, возможно, нацеливаясь на разведывательные и телекоммуникационные спутники.

В дополнение к противодействию угрозам МБР противника, С-500 также сможет эффективно поражать высотные беспилотные летательные аппараты, особенно с учетом опасений Министерства обороны России, что беспилотные летательные аппараты НАТО большой дальности постоянно ведут наблюдение вдоль российских границ.

1Б-75 «Пенициллин»

В декабре 2020 года российские военные начали поставки в вооруженные силы своей новейшей системы противодействия батареям «Пенициллин».

Система оснащена новыми системами обнаружения и некоторой степенью автоматизации.

Он обнаруживает как звуковые, так и оптические излучения с помощью специальных оптико-электронных модулей и наземных датчиков.

Система состоит из шести телевизионных камер и шести тепловизоров с полем зрения 70 градусов и азимутом 10 градусов.

Сигналы от этих датчиков объединяются с четырьмя наземными акустическими и сейсмическими датчиками.

Системы «Пенициллина» объединяют эти различные выбросы, чтобы точно определить источник удара. В ограниченной отчетности с открытым исходным кодом говорится, что система может обнаруживать стрельбу и удары на расстоянии до 25 километров.

В пресс-релизах концерна Vega о «Пенициллине» отмечается, что он должен быть в состоянии снизить значительную часть риска для передовых разведчиков, которые обычно предоставляют информацию

о прицеливании систем поражения противника, и что он может работать в полностью автоматизированном режиме без оператора.

Российские военные сначала установят эти системы на уровне полка и бригады, а затем предоставят их береговым войскам.

МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО

Для России ИИ становится все более приоритетной областью международного сотрудничества, выделяемой на самом высоком уровне.

Когда Владимир Путин выступал (посредством видеоконференции) на Генеральной Ассамблее ООН в сентябре 2020 года, передовые цифровые технологии, в частности ИИ, были одним из основных направлений его выступления.

Он заявил, что передовые цифровые технологии позволили адаптироваться к меняющимся обстоятельствам пандемии, в том числе посредством предоставления услуг и дистанционного обучения, и что ИИ оказался полезным в медицинской области, поскольку врачи могут более точно и быстро ставить диагнозы и выбирать идеальное лечение для отдельных людей.

В то же время Путин заявил, что цифровые технологии представляют угрозу международной безопасности и стабильности, поскольку они могут бесконтрольно распространяться и попасть в руки радикалов и экстремистов по всему миру. Он утверждал, что ООН должна серьезно рассмотреть вопросы кибербезопасности и защиты частной жизни при разработке политики в области цифровых технологий, чтобы найти баланс между стимулированием развития ИИ и осуществлением соответствующих ограничительных мер. Он выступал за коллективный подход, с помощью которого государства могли бы совместно согласовать правила, которые остановили бы потенциальные угрозы, подчеркивая не только военную и технологическую безопасность, но и угрозы традициям, праву и морали.

Эти проблемы сформировали взгляды России на регулирование развития ИИ, поскольку Россия стремится утвердиться в качестве лидера мысли по этике развития ИИ посредством участия в международных дискуссиях по установлению правил в этой области.[322]

При обсуждении ИИ с зарубежными коллегами, Российские официальные лица в целом подчеркнули желание своего правительства сотрудничать с другими странами в этой сфере. Такие беседы довольно часты, причем с широким кругом потенциальных партнеров.

Например, только в сентябре 2020 года российские официальные лица обсуждали потенциальное сотрудничество в области ИИ со своими коллегами из Беларуси, Южной Кореи и Германии, а также на форуме БРИКС. Публичные замечания, сопровождающие такие дискуссии, неизменно подчеркивают ведущую роль России в разработке новых технологий и вытекающие из этого возможности, которые международное сотрудничество может способствовать как в России, так и в потенциальных государствах-партнерах.[323]

Условно можно провести обзор отношений международного сотрудничества, связанных с ИИ в России. Страны имеют размер и разделены на три простые относительные категории малых, средних и крупных, отражающие относительный уровень сотрудничества в области ИИ.

Для каждой отдельной страны или региона показаны три типа отношений: государственные (красный), отраслевые (зеленый) и академические (синий). Толщина каждой линии представляет уровень сотрудничества ИИ в этой области относительно (жирный шрифт) других областей.

В каждой стране или регионе также есть организация, если она значима, которая фигурировала в нашем анализе отношений, например, китайская Huawei. Этот график является результатом субъективной, а не количественной оценки командой типов, веса и значимости отношений и предназначен лишь

---

[322] Президент России, «75-я сессия» Генеральной Ассамблеи ООН, 22 сентября 2020 года, http://kremlin.ru/events/president/news/64074.

[323] «Искусственный интеллект и право: есть контакт?», Garant.ru, 16 июля 2020 года, https://www.garant.ru/news1401154.

для руководства или широкого обзора международного сотрудничества России в области ИИ.

В то же время существуют некоторые правовые ограничения на сотрудничество.

Например, в апреле 2020 года был принят новый закон, устанавливающий экспериментальный правовой режим для регулирования условий разработки и внедрения технологий ИИ в России.

Он включает положение, запрещающее иностранным фирмам или совместным предприятиям с доминирующей иностранной собственностью подавать заявки на участие в режиме.[324]

Ограничения на участие России в международном сотрудничестве в области ИИ не ограничиваются такими правовыми барьерами.

Другие факторы включают поздний приход российских исследователей в эту область по сравнению с исследователями из других стран и их все еще ограниченные связи с международными сетями, работающими в этой области.[325]

Будучи поздним участником в этой области, Россия также стремилась избежать юридических ограничений на свою деятельность по разработке ИИ, как это ясно видно из ее роли в продолжающихся переговорах ООН по ЗАКОНАМ по смертоносным автономным системам оружия, подробно обсуждаемых ниже.

В целом, несмотря на сильные экономические стимулы и некоторое политическое давление с целью расширения возможностей ИИ в России за счет международного сотрудничества, партнерские отношения с иностранными

---

[324] «Рапота: Союзное государство Белоруссии и РФ должно учитывать развитие высоких технологий» ТАСС, 29 сентября 2020 года, https://tass.ru/politika/9578271, В телефонных переговорах с Муном Путин говорит, что Россия настроена на сотрудничество в области мира в Корее: Чон Ва Дэ», Информационное агентство Ренхап, 28 сентября 2020 г., https://en.yna.co.kr/view/AEN20200928013300315, «В. Тимченко: Законодательная сфера регулирования развития искусственного интеллекта в России активно развивается» Совет Федерации, 21 сентября 2020 г., http://council.gov.ru/events/news/119232/; Состоялась шестая встреча министров связи стран БРИКС, Отредактированное Министерством связи, цифрового развития и средств массовой информации Российской Федерации; «Декларация 6-го совещания министров связи стран БРИКС», БРИКС (17 сентября 2020 г.), https://eng.brics-russia2020.ru/documents.

[325] «Иностранным фирмам не разрешат участвовать во внедрении искусственного интеллекта в РФ», Интерфакс, 6 июля 2020 года, https://www.interfax.ru/russia/716123.

фирмами сыграли относительно ограниченную роль в развитии российского ИИ.

В то время как китайская фирма Huawei и южнокорейская фирма Samsung установили прочное присутствие в России, они в значительной степени являются исключениями. На российском рынке цифровых технологий нет аналогичных западных фирм с сильным присутствием. Хотя в таком положении дел легко винить санкции, которые не могут объяснить отсутствие других азиатских фирм, следующих примеру двух лидеров.

Более вероятное объяснение заключается в том, что коммерческие стимулы превосходят геополитические соображения: Россия является относительно ограниченным рынком и она не предлагает очевидных сравнительных преимуществ с точки зрения предоставления молодым предпринимателям, которые могут быть лидерами в продвижении в этой области по сравнению с Восточной Азией или Западом.

В результате большинство усилий по международному сотрудничеству, описанных ниже, являются либо разовыми коммерческими совместными предприятиями, либо усилиями российских компаний, занимающихся ИИ, по проникновению на зарубежные рынки.[326]

Позиция России на переговорах по ЗАКОНАМ

Недавняя позиция России по ЗАКОНАМ (дебаты в Организации Объединенных Наций по использованию смертоносных автономных систем оружия) состоит в том, чтобы не согласиться с необходимостью юридически обязательного регулирования и ограничения со стороны международного сообщества в отношении такого оружия или других мер.[327]

[326] Ирина Дежина, «Разбег с барьерами. Что тормозит развитие российских нейротехнологий?» Новости Поиска, 7 июня 2020 г., https://www.poisknews.ru/themes - нейротехнологий.

[327] Основными исключениями являются Huawei и Samsung, как отмечалось выше, а также сотрудничество MIT и Сколтеха, которое изначально было многообещающим, но в значительной степени угасло из-за ограничений, связанных с западными санкциями.

Россия утверждает, что ее подход мотивирован тем фактом, что механизм ИИ, способный сделать смертоносное оружие действительно автономным, все еще является теорией, а не практической реальностью в наши дни.

Россия с 2014 года является активным личным участником каждого совещания по ЗАКОНОДАТЕЛЬСТВУ по КОО (Конвенции ООН об обычных вооружениях), но продолжает выступать против юридических переговоров по ЗАКОНАМ.

Российская делегация на обсуждениях ЗАКОНОВ в 2018 и 2019 годах, состоящая из Министерства иностранных дел России, Министерства обороны и Министерства промышленности и торговли, не была склонна обсуждать существенное ограничение или полный запрет таких автономных систем.[328]

Такое противодействие стало еще более очевидным из-за того, что Россия не присутствовала на последнем совещании по КОО в сентябре 2020 года, на котором российские представители не присутствовали ни виртуально, ни лично.[329]

Кроме того, Россия попыталась перенести встречу, которая уже была отложена из-за COVID-19, на более позднее время в 2021 году.[330]

Россия занимает жесткую позицию против переговоров по ЗАКОНАМ по нескольким заявленным причинам – в законах отсутствует точное юридическое определение. Российская Федерация часто упоминает, что предстоящие обсуждения ЗАКОНОВ столкнутся с большими практическими трудностями, если стороны сначала «не согласуют основные определения ЗАКОНОВ».[331]

Российские участники переговоров считают, что, поскольку смертоносные автономные системы вооружений еще не разработаны, заранее

---

[328] Андрей Малов, советник Министерства иностранных дел ДНКВ Российской Федерации, о причинах скептического отношения Москвы к запрету на «боевых роботов» Kimmersant.ru, 16 августа 2018 года, https://www.kommersant.ru/doc/ 3714110?from=doc_vrez.

[329] Дастин Льюис, «Непреходящий тупик в области автономного оружия», Просто Безопасность, сентябрь. 28 декабря 2020 года, https://www.justsecurity.org/72610/an-enduring-impasse-on-autonomous-weapons.

[330] Янош Делкер, «Рост и развитие распознавания лиц – Фон дер Ляйен расшифровал – Запрет роботов-убийц», Политико, 23 сентября 2020 г., https://www.politico.eu/newsletter/ai-decoded/politico-ai-decoded-the-rise-and-rise-of.

[331] Заявление Российской Федерации Группе правительственных экспертов по КНО, CCW/GGE.1/2017/WP.8, 10 ноября 2017 г., https://admin.govexec.com/media/russia.pdf.

определенные и превентивные запреты могут ограничить более широкое развитие ИИ и автономных систем, в том числе полезных.

Например, Министерство иностранных дел России указало на «трудности с четким различием между гражданскими и военными разработками в автономных системах».[332]

Действующих международных правил достаточно. Российская делегация считает, что дальнейшие ограничения ЗАКОНОВ выдвигаются «радикальными государствами и неправительственными организациями», которые желают полного запрета ЗАКОНОВ.[333]

Решение России объявить усилия по ограничению ЗАКОНОВ «радикальными» подчеркивает продолжающуюся политизацию этой дискуссии в конкурирующих лагерях, при этом Россия твердо выступает за сохранение права каждой страны создавать оружие по своему выбору, рассматривая тех, кто выступает за ограничение ЗАКОНОВ, как стремящихся наложить ограничения на национальный суверенитет.

В 2018 и 2019 годах российская делегация специально указала, что действующее международное право (включая его гуманитарную отрасль) полностью применимо к ЗАКОНАМ и не нуждается в обновлении или адаптации.

Российские официальные лица указали, что их страна строго придерживается норм международного гуманитарного права (МГП), применимых к этому виду оружия, и что российское национальное законодательство содержит положения, которые могут касаться возможного ввода в эксплуатацию оружия, которое не соответствует правовым обязательствам России по МГП.[334]

Приверженность России соблюдению норм МГП в вооруженных конфликтах была вновь подчеркнута в недавнем рабочем документе, который

---

[332] «Автомат Калашникова – Россия выступает против запрета на полностью автономные боевые системы», Коммерсант, 16 августа 2018 г., https://www.kommersant.ru/doc/3714419.
[333] Там же.
[334] Там же.

она представила Группе правительственных экспертов по ЗАКОНОДАТЕЛЬСТВУ 2020 года по КОО.[335]

Аналогичным образом, Россия выступает за концепцию «значимого человеческого контроля» над будущими ЗАКОНАМИ в качестве потенциальной точки консенсуса с международным сообществом, хотя сомнительно, что критерии «значимости» можно было бы разработать без политизации.[336]

Разработка автономного оружия не является неизбежной: российские делегации в ООН официально утверждают, что обсуждение ЗАКОНОВ преждевременно, поскольку такого оружия еще не существует.

Например, в своем позиционном документе по КОО, представленном в 2017 году, Россия ссылается на маловероятность того, что смертоносное автономное оружие станет реальностью в ближайшем будущем, называя их «пока еще несуществующие системы вооружений».[337]

Однако критики указывают на лицемерный характер позиции России, поскольку российские оборонные компании являются одними из наиболее активных в продвижении разработки такого автономного оружия.[338]

Россия вложила значительные средства в исследования и разработки автономных систем вооружений и сделала военные инвестиции в ИИ и робототехнику главным приоритетом национальной обороны.[339] Возможно, это соответствует суверенному праву России осуществлять свои политические, военные и/или экономические интересы как часть ее реакции на то, что она считает мировым порядком, определяемым гегемонией США.[340]

---

[335] Российская Федерация, Заявление Российской Федерации Группе правительственных экспертов по КОО, 2017 год: Национальное осуществление Руководящих принципов по новым технологиям в области смертоносных автономных систем вооружений, 2020 год, https://reachingcriticalwill.org/images/documents/Disarmament.

[336] Там же.

[337] Там же.

[338] Дэвид Гилберт, «Российский производитель оружия Калашников разрабатывает роботов-убийц с искусственным интеллектом», Вице, 12 июля 2017 г., https://www.vice.com/en/article/vbzq8y/russian-developing-killer-ai-robots.

[339] Указ Президента Российской Федерации № 490 «О развитии искусственного интеллекта в Российской Федерации».

[340] Патрик Такер, «Россия для Организации Объединенных Наций: Не пытайтесь помешать нам создавать роботов-убийц», Defense One, 21 ноября 2017 г., https://www.defenseone.com/technology/2017/11/russia-united-

Тем не менее, России еще предстоит внести конструктивный вклад в обсуждение ЗАКОНОВ в рамках КОО и, таким образом, международное сообщество в целом рассматривает ее как некооперативный субъект в этой сфере.

И США, и Россия, среди прочего, выразили несогласие с юридически обязательными понятиями ЗАКОНОВ в дискуссиях по КОО, однако только Россия демонстрирует нежелание сотрудничать на международном уровне в дискуссиях по определению и мозговому штурму рамок ЗАКОНОВ.

До тех пор, пока автономные системы остаются бюджетным приоритетом национальной безопасности и обороны России, можно ожидать, что Россия будет продолжать выступать против дальнейшего ограничения или определения ЗАКОНОВ в любой форме и препятствовать тому, чтобы КНО ограничивала виды технологий, которые могут быть использованы на службе национальной безопасности.

Китай

За последние пять лет Китай стал ключевым партнером России в сфере высоких технологий в целом и ИИ в частности.

Это партнерство укрепилось в результате растущего согласования интересов и проблем безопасности, отчасти обусловленного взаимным ощущением того, что обе страны конкурируют с Соединенными Штатами и бросают вызов их доминирующей роли в международной системе.

Политика США в отношении обеих стран, включая санкции, экспортный контроль и тарифы, подтолкнула Россию и Китай к более тесному сотрудничеству в целях развития своих высокотехнологичных отраслей.

Эти геополитические обстоятельства усилили «решимость китайских и российских лидеров развивать местные замены иностранных, особенно американских технологий, от чипов до операционных систем и обеспечили дополнительную мотивацию для сотрудничества».

---

nations-dont-try-stop-us - роботы-убийцы зданий/142734.

Российско-китайские межправительственные инициативы в области искусственного интеллекта

История российско-китайского технологического сотрудничества в сфере ИИ подробно описана в недавнем докладе Сэмюэля Бендетта и Эльзы Кания.

Они подчеркивают происхождение современных отношений, вытекающих из государственного визита Си Цзиньпина в Москву в мае 2015 года, результатом которого стали новые соглашения о сотрудничестве в цифровой экономике.[341]

С тех пор сотрудничество в области науки и технологий стало одним из столпов стратегического партнерства двух стран.

Бендетт и Кания выделяют пять областей, в которых сотрудничество в области ИИ расширилось за последние пять лет: диалоги и обмены, совместные инвестиционные фонды, развитие промышленных научно-технических парков, совместные конкурсы и расширение академического сотрудничества.[342]

В июне 2016 года было объявлено о создании Китайско-Российского инновационного парка, финансируемого Правительством провинции Шэньси, Российским фондом прямых инвестиций и Китайско-Российским инвестиционным фондом.[343]

Он был завершен в 2018 году с участием предприятий ИИ.[344]

В 2017 году Министерство науки и технологий Китая и Министерство экономического развития России учредили Китайско-российский инновационный диалог, который с тех пор проводится ежегодно и предназначен для компаний из двух стран, чтобы продемонстрировать свою продукцию и заключить новые соглашения о сотрудничестве.

---

[341] Сэмюэл Бендетт и Эльза Кания, Новое китайско-российское партнерство в области высоких технологий, Австралийский институт стратегической политики, Отчет № 22, 2019, https://www.aspi.org.au/report/new-sino-russian-high-tech-partnership.

[342] «Китайско-российское стратегическое партнерство открывает новые горизонты», China Daily, 6 ноября 2016 г., http://www.chinadaily.com. cn/world/ 2016 liattends SCOCCEEC/2016-11/06/content_27288768.htm.

[343] Бендетт и Кания, Новое китайско-российское партнерство в области высоких технологий.

[344] Чэнь Лань, «Шелковый путь» приглашает российских бизнесменов «Российская газета», 14 июня 2018 г., https://rg.ru/2018/06/14/v-siane-otkrylsia-mezhdunarodnyj.

Первый диалог состоялся в Пекине, и в нем приняли участие более 100 китайских и российских предприятий из различных отраслей промышленности, включая нанотехнологии, робототехнику и ИИ.

Соревнование проводится с 2018 года, когда состоялся первый Китайско-Российский конкурс промышленных инноваций.

В этом конкурсе, посвященном теме «Инновации движут будущим», были освещены большие данные, ИИ и высокотехнологичное производство.

В сентябре 2019 года был создан совместный инвестиционный фонд, финансируемый правительством, с первоначальным бюджетом в 1 миллиард долларов и акцентом на финансирование исследований в области ИИ.[345]

За прошедший год обе стороны еще больше расширили все эти усилия, в том числе в рамках двухлетней инициативы, которая объявила 2020 и 2021 годы годами российско-китайского научно-технического и инновационного сотрудничества.

Хотя изначально программа предназначалась для охвата широкого спектра технологического сотрудничества, включая, в частности, ИИ и интернет вещей, пандемия COVID-19 заставила ее сместить основное внимание на здравоохранение и биотехнологии.

В рамках этих усилий две страны разрабатывают двусторонний механизм обмена научной информацией, уделяя основное, но не исключительное внимание общественному здравоохранению и биомедицине.[346]

Huawei как движущая сила сотрудничества

Ключевую роль в коммерческом сотрудничестве между Россией и Китаем в области ИИ сыграла компания Huawei, которая была названа звездным игроком в партнерстве.

---

[345] Дмитрий Саймс, «Huawei играет главную роль в новом китайско-российском партнерстве в области искусственного интеллекта», Nikkei Asia, 4 февраля 2020 г., https://asia.nikkei.com/Spotlight/Asia-Insight/Huawei-plays-star-role-in-new-China-Russia-AI-partnership.

[346] «Россия и Китай обсуждают ключевые проекты года научного сотрудничества», ТАСС, 25 декабря 2019 г., https://tass.com/science/1103515; «пресс-релиз посольства Китая в России», 22 июня 2020 г., http://ru.china-embassy.org/rus/gdxw/t1791912.htm.

Huawei открыла свои первые исследовательские институты в России в 2017 году с объектами в Москве и Санкт-Петербурге, которые были сосредоточены на разработке математических моделей для коммуникационных технологий.

Три дополнительных центра открылись в 2019 году, так как компания объявила о планах утроить свой научно-исследовательский персонал в России.[347]

Первые крупные прямые финансовые инвестиции Huawei в российские компании ИИ начались в 2019 году, когда она купила права на технологию распознавания лиц, разработанную российским стартапом Vocord, и наняла большую часть сотрудников Vocord.[348]

Позже, в том же году компания подписала соглашение о сотрудничестве со Сколково, а затем объявила о плане создания экосистемы ИИ в России к 2025 году, которая будет состоять из 20 университетов, более 100 компаний-разработчиков программного обеспечения и более 100 000 разработчиков ИИ.[349] Проекты сотрудничества Huawei основаны на стратегии для российского рынка.

Стратегия, получившая название TIGER (Технология, Промышленность, Рост, Экосистема, Надежность), предполагает совместную работу с российскими компаниями по «разработке и применению технологий, созданию промышленные решения, программы стимулирования партнеров и создания экосистемы, которые в конечном итоге приведут к развитию собственной промышленности России».

Huawei фокусируется на расширении экосистемы ИИ в России в трех областях:

---

[347] «Huawei планирует предложить около 1500 рабочих мест в исследовательских центрах в России в течение следующих 6 лет», Спутник, 15 августа 2019 г., https://sptnkne.ws/8Xfm.

[348] Алена Сухаревская, «Huawei купила технологии российской компании в области распознавания лиц, Ведомости, 3 июня 2019 г., https://www.vedomosti.ru/technology/articles/2019/06/02/803125-huawei-kupil.

[349] Ольга Иншакова, «Huawei создаст экосистему искусственного интеллекта в России», Форум по туберкулезу, 25 февраля 2020 г., https://eng.tbforum.ru/blog/huawei-will-create-an-artificial-intelligence-ecosystem-in-russia.

1) использование инновационной лаборатории Huawei OpenLab в Москве для укрепления сотрудничества с российскими партнерами в проектах ИИ;

2) подготовка российских разработчиков на основе глобального сообщества разработчиков Ascend;

3) разработка курсов, связанных с технологиями ИИ, и расширение круга российских университетов, занимающихся обучением в этих областях. Huawei инвестировала 5 миллионов долларов в партнерские отношения в России в 2020 году.

Он планирует увеличить закупки у российских поставщиков с 392 миллионов долларов в 2017-2019 годах до 800 миллионов долларов в 2020-2025 годах и увеличит количество научно-исследовательских центров в России до пяти.[350]

В рамках этой стратегии в 2020 году Российский научно-исследовательский институт Huawei открыл совместную научно-исследовательскую лабораторию для ИИ и глубокого обучения со Школой прикладной математики и компьютерных наук МФТИ.

Лаборатория будет сосредоточена на разработке нейросетевых алгоритмов для компьютерного зрения, машинного обучения и ИИ; разработка методов вычислительной фотографии и улучшения изображения с использованием математического моделирования и передовых алгоритмов; решение математически сложных задач для создания алгоритмов одновременного поиска и позиционирования.

Это была 10-я подобная совместная лаборатория, открытая Huawei с российскими учебными заведениями и научно-исследовательскими институтами.[351]

Huawei продолжает привлекать российские учебные заведения с помощью соглашений о финансировании и партнерстве, чтобы использовать

---

[350] «Huawei готова инвестировать в новые технологии для создания в РФ цифровой инфраструктуры», ТАСС, 25 июня 2020 г., https://tass.ru/ekonomika/8816823.

[351] «МФТИ и Huawei открыли совместную R&D-лабораторию по разработке технологий искусственного интеллекта», MSKIT.ru, 6 марта 2020 года, http://mskit.ru/news/n217346.

российское STEM-образование для своих собственных RDT&E (исследование, разработка, испытание и оценка). Huawei создает лаборатории ИИ и ML (машинное обучение), исследовательские гранты и соглашения о сотрудничестве, чтобы привлечь огромный пул способных студентов STEM в России.

В свою очередь, российские университеты получают столь необходимое финансирование и доступ к мировому лидеру в области высоких технологий. Ожидается, что в этом мероприятии примут участие десятки ведущих российских школ и университетов.

В рамках этого плана Huawei создала ряд академий при региональных университетах, таких как Новосибирский государственный технический университет и Уральский радиотехнический колледж имени А.С. Попова в Екатеринбурге. Эти академии недавно диверсифицировались, включив курсы по ИИ и машинному обучению.[352]

В коммерческой сфере Huawei установила широкий спектр партнерских отношений с российскими компаниями.

Он работает с российской ИИ-компанией VisionLabs. Благодаря этому партнерству опыт VisionLabs в области компьютерного зрения будет использован в серии продуктов Huawei Atlas для машинного обучения.

В качестве первого шага VisionLabs добавила поддержку Atlas 800 в свое существующее программное обеспечение Luna SDK. Luna SDK – это кроссплатформенный набор инструментов разработки с функциональностью распознавания и анализа лиц и других объектов на 2D-изображениях с использованием нейронных сетей.

Продукт был недавно признан на конкурсе NIST в США одним из самых быстрых и точных из таких продуктов.[353]

---

[352] «Huawei и УРТК выпустили первых студентов по направлению Искусственного интеллекта», Huawei.com, 15 июня 2020 года, https://e.huawei.com/ru/news/ru/2020/202006161749.

[353] «VisionLabs и Huawei объявляют о стратегическом партнерстве в области компьютерного зрения» 19 октября 2020 г., https://www.cnews.ru/news/line/2020-10.

Huawei и CDNvideo подписали меморандум о сотрудничестве, который позволит CDNvideo использовать виртуальные машины Huawei KunPeng для своих облачных серверов. Две компании изучили возможности совместной работы по предоставлению новых услуг для пользователей, включая бессерверные вычисления, управляемые базы данных и облачные хранилища. Конечная цель – создать объединенную экосистему продуктов и услуг.[354]

Huawei сотрудничает с российскими компаниями в области облачных вычислений, включая партнерство с Kaspersky, которое объединяет облачную службу безопасности последнего с облачной платформой Huawei FusionSphere. Huawei также напрямую сотрудничает со Sber для запуска собственной облачной платформы в России.[355]

Huawei также сотрудничает с Ростелекомом, крупнейшим российским провайдером междугородной телефонной связи и Интернета, для разработки домашнего Wi-Fi-маршрутизатора, специально предназначенного для игр. Маршрутизатор использует технологию ИИ для определения приоритетов доставки пакетов данных на игровые серверы и с них, без неоправданной задержки других приложений. Две компании работают вместе с 2016 года над разработкой технологии и планируют распространить ее на другие виды использования.[356]

Huawei стремится к дальнейшему расширению своих партнерских отношений.

С этой целью он недавно принял участие в конференции российского Инфофорума о будущем цифровой безопасности, в которой приняли участие российские компании (например, Мегафон, Ростелеком, Росатом и Российские железные дороги), а также от государственных учреждений (например,

---

[354] «Huawei и CDNvideo подписали меморандум о сотрудничестве в области разработки сервисов на основе ИИ, Интернета вещей и больших данных» Коммерсант, 15 октября 2020 г., https://www.kommersant.ru/doc/4531348.
[355] Лорен Дадли, «Huawei привлекает российские таланты и технологии для обеспечения будущих инноваций: Часть 2», part-two-huawei-enlists-russian-talent-and - технология - обеспечение -будущих - инноваций.
[356] «Ростелеком и Huawei представили игровой маршрутизатор с искусственным интеллектом», CNews, 17 ноября 2020 г., https://www.cnews.ru/news/line/2020-11.

администрации Президента, Министерства иностранных дел, Федерального агентства связи и Федеральной налоговой службы).

Участники конференции обсудили глобальные тенденции в области цифровых технологий, их внедрение в государственные службы и практику построения систем информационной безопасности в новой цифровой реальности.[357]

Хотя Huawei является бесспорным лидером сектора российско-китайского сотрудничества в области ИИ, коммерческие партнерские отношения между российскими и китайскими компаниями в секторе ИИ не ограничиваются Huawei.

Компания Fitsco, китайский поставщик систем сигнализации железнодорожного транзита, и Cognitive Pilot, совместное предприятие российской группы компаний Sber и Cognitive Technologies, объявили о создании стратегического альянса для обмена решениями для интеллектуального городского планирования и других транспортных сетевых технологий с поддержкой ИИ.

Это расширяет и углубляет партнерство, которое ранее существовало с конца весны, когда они начали сотрудничать над новой усовершенствованной системой помощи водителю для китайского легкорельсового транспорта.[358]

Китайская технология Dahua и российская NtechLab сотрудничают в проекте по созданию камеры с возможностями распознавания лиц. Китайский разработчик программного обеспечения Vinci Group договорился о работе над продуктами ИИ с российским ИТ-стартапом Jovi Technologies.[359]

В целом, в условиях растущей напряженности в отношениях с Соединенными Штатами Китай и Россия явно договорились о расширении

---

[357] «На международной конференции Инфофорума «Будущее цифровой безопасности. Экспертный взгляд «компания Huawei представила рекомендации по развитию цифровой экономики России», 10, 2020, https://www.vedomosti.ru/press_releases/2020/11/10/.

[358] «Fitsco и Когнитивный пилот образуют стратегический альянс для развития ITS в Азии и России», Технологии дорожного движения Сегодня, 11 сентября 2020 г., https://www.traffictechnologytoday.com/news/public-transit/fitsco-and-cognitive-pilot-form-strategic-alliance-to-develop-its-in-asia-and-russia.html.

[359] «Huawei играет главную роль в новом китайско-российском партнерстве в области искусственного интеллекта».

своего технологического сотрудничества, при этом ИИ играет ключевую роль в их планах на будущее. Некоторые аналитики полагают, что партнерство может рухнуть из-за готовности Китая возобновить отношения с Соединенными Штатами, если представится такая возможность.[360]

Однако на сегодняшний день не было никаких признаков каких-либо подобных разногласий. Напротив, отношения между Китаем и Россией продолжали расти и углубляться в течение последнего года, даже несмотря на то, что пандемия все больше смещала приоритеты в сторону биомедицинской сферы.

Южная Корея и Япония

Хотя Китай является основным направлением усилий России по международному сотрудничеству в области ИИ, Южная Корея и Япония также играют очень заметную роль в этой области.

На правительственном уровне сотрудничество с Южной Кореей в технологической сфере является обширным и получило дальнейшее развитие с подписанием плана «Девять мостов 2.0» в октябре 2020 года.

В рамках этой инициативы инновационные платформы были явно добавлены в список приоритетных направлений двустороннего экономического сотрудничества.[361]

Хотя это первое указание на явную роль ИИ в российско-корейском двусторонним сотрудничестве на государственном уровне, коммерческое сотрудничество существует уже много лет.

Несмотря на то, что Huawei является наиболее важным игроком в сотрудничестве Китая с Россией в области ИИ, ключевую роль для Южной Кореи играет Samsung.

Московский центр искусственного интеллекта Samsung играет ключевую роль в этом сотрудничестве. Он был основан в 2018 году с целью

---

[360] Там же.

[361] «Южная Корея и Россия подписали план «Девять мостов 2.0», Ситао, 29 октября 2020 г., https://www.seetao.com/details/44488/en.html.

использования российского опыта в области ИИ и использования возможностей российского центра исследований и разработок Samsung, который работает в Москве с 1993 года.

Основные направления исследований центра искусственного интеллекта включают компьютерное зрение, робототехнику и интеллектуальную помощь при вождении.

Его возможности в анализе зрения позволили ему разработать программное обеспечение, которое может превратить одно неподвижное изображение в видео, которое может имитировать выражение лица и движения человека.

В отличие от обычных «глубоко поддельных» видео, которые требуют процесса 3D-моделирования, технология, разработанная совместно со Сколтехом, может создать убедительное поддельное видео всего с одним изображением.

Эта возможность привела к опасениям, что ее технология ИИ может быть использована для создания «глубоко поддельных» видеороликов, которые могут повлиять на общественность.[362]

В дополнение к своим коммерческим усилиям в России Samsung создала образовательное подразделение под названием Samsung IT Academy. Эта академия разработала серию одногодичных курсов по ИИ, Интернету вещей и разработке мобильных приложений, которые преподаются в 34 университетах по всей России (и в Казахстане), в которых обучается более 1000 студентов. Цель состоит в том, чтобы выпускники программы помогли решить значительную нехватку персонала, ощущаемую во всем Российская ИТ-индустрия.

Хотя обучение в университетах растет, одного этого недостаточно для решения проблемы нехватки.[363]

---

[362] «Samsung Electronics запускает Центр искусственного интеллекта в России», пресс-релиз Samsung, 29 мая 2018 г., https://news.samsung.com/global/samsung-e4 мая 2019 года, https://pulsenews.co.kr/view.php?sc =30800028&year =2019.

[363] «Проект «IT Академия Samsung» начинает новый учебный год в России и Казахстане, 21 октября 2020 года, https://news.samsung.com/kz_ru/project-it.

В дополнение к организации семестровых занятий, академия также проводит обучение во время фестивалей выходного дня, таких как фестиваль, проведенный в сентябре 2020 года в рамках Международного молодежного форума «Виртуальный Байкал», в котором приняли участие 1400 участников со всей России.[364]

Академия также организует ежегодный всероссийский конкурс для выпускников своих университетских учебных программ.[365]

В отличие от Южной Кореи, Российские официальные лица только недавно начали взаимодействовать со своими японскими коллегами в области ИИ. В рамках усилий по диверсификации спектра своих высокотехнологичных партнерских отношений Россия недавно представила ряд инициатив по сотрудничеству с Японией в сфере технологических инноваций.

В июне 2020 года заместитель министра экономического развития России встретился с генеральным директором Департамента торговой и информационной политики Министерства экономики, торговли и промышленности Японии, чтобы предложить создать «дорожную карту» для сотрудничества в области высоких технологий.

В ходе встречи она заявила, что это одна из наиболее активных областей российско-японского сотрудничества, и выразила готовность к расширению совместной работы в этой сфере, в том числе в построении цифровой экономики и развитии ИИ.

Кроме того, обе стороны затронули тему сотрудничества между инновационными технопарками, инновационными регионами, фондами, институтами развития и исследовательскими университетами с целью содействия более глубокому слиянию науки и техники с промышленностью и окружающей средой в целях оптимизации инновационных экосистем обеих стран.[366]

---

[364] Эксперты «IT Академии Samsung» приняли участие в международном молодежном форуме «Байкал», Новости Samsung, сентябрь. 22, 2020, https://news.samsung.com/ru/IT.
[365] «Компания Samsung» «IT Академия Samsung».
[366] «Замглавы Минэкономразвития предложила создать «дорожную карту» взаимодействия с Японией в сфере высоких технологий», Министерство экономического развития России, 11 июня 2020 года,

Соединенные Штаты

Сотрудничество России с Соединенными Штатами в области ИИ ограничивается в основном академическим сектором и лишь несколькими коммерческими предприятиями.

Стимулы в первую очередь направлены на получение прибыли, поскольку компании стремятся выйти на крупные рынки США, такие как автомобильная, сельскохозяйственная и финансовая отрасли.

Усилия по налаживанию связей с академическими институтами являются признаком того, что россияне, активно работающие в области ИИ, признают лидирующие позиции американских ученых в этой области. Но ограниченный успех таких усилий является признаком ограничений, создаваемых общими враждебными отношениями между двумя странами и юридическими ограничениями режима санкций США.

Санкции США, которые препятствуют экспорту военных технологий и технологий двойного назначения в Россию, разрешают экспорт определенных видов оборудования, таких как некоторые компьютерные чипы, но ограничивают взаимодействие со многими крупными государственными корпорациями, которые находятся в санкционных списках.

Кроме того, многие крупные американские компании в этой сфере, такие как Google и Amazon, неохотно сотрудничают с некоторыми ключевыми российскими игроками из-за опасений, что они могут нарушить режим санкций.[367]

Взаимодействие правительств в значительной степени носит конкурентный характер. Существует устойчивое мнение, особенно в России, что Россия и Соединенные Штаты находятся в разгаре технологической конкуренции в области ИИ.

---

https://www.economy.gov.ru/.html.

[367] «Цифровая трансформация в России: сохранение конкурентоспособности», DT - Global Business Consulting, май 2019 г., https://www.bakermckenzie.com/pdf.

Со стороны США тогдашний конгрессмен США Уилл Херд в проекте резолюции о создании национальной стратегии ИИ США отметил, что Россия стремилась к лидерству в этой области. Как он выразился: «Если мы не установим правила дорожного движения для ИИ, это сделают Китай или Россия. Сам Владимир Путин сказал, что нация, которая лидирует в области искусственного интеллекта, «будет правителем мира». Я бы предпочел, чтобы будущее определялось нашими ценностями, а не их».[368]

В ответ Сергей Боярский, первый заместитель председателя Комитета Государственной Думы по информационной политике, информационным технологиям и связи, сказал: «Это новая гонка. Раньше была гонка за космос, а теперь за искусственный интеллект». Боярский сказал, что для США естественно опасаться продвижения России вперед в области ИИ, потому что технологии, основанные на ИИ, будут глубоко переплетаться с нашей жизнью в ближайшие 30-50 лет. Он заявил, что Россия готова конкурировать с США по созданию ИИ и что страны, которые не воспринимают ИИ всерьез, в конечном итоге окажутся в стороне в будущем.[369]

Академическое сотрудничество

Наиболее значимая российско-американская совместная инициатива началась более 10 лет назад, когда тогдашний президент Дмитрий Медведев запустил инновационный кластер «Сколково».

Он хотел, чтобы Сколково стало российским эквивалентом Кремниевой долины в Соединенных Штатах. Цель состояла в том, чтобы создать устойчивую экосистему предпринимательства и инноваций, создавая культуру стартапов и поощряя венчурный капитализм.

---

[368] «Моултон присоединяется к Херду, Келли в резолюции о создании национальной стратегии искусственного интеллекта», Пресс-релиз Сета Моултона, 16 сентября 2020 г., https://moulton.house.gov/press-releases/moulton-joins-hurd-kelly.

[369] «В Госдуме рассказали о гонке РФ и США по созданию искусственного интеллекта», Crimeangazette.ru, 25 сентября 2020 года, http://crimeangazette.ru/novosti/v.

С этой целью правительство предоставило участникам проекта различные налоговые льготы и более либеральные визовые правила для обеспечения занятости иностранных граждан.

Федеральное правительство также построило обширную новую транспортную инфраструктуру, чтобы соединить район с центром Москвы и местными транспортными узлами.

Сколково включает в себя пять исследовательских кластеров: ИТ, Энергетика, Ядерный, Биомедицина и Космос.

Развитие технологий ИИ является одним из основных направлений Кластера информационных технологий.[370]

Чтобы привлечь больше международных партнеров, Сколково недавно запустило программу Softlanding, который призван стимулировать иностранные стартапы в области высоких технологий базироваться в Сколково.[371]

Это двухнедельная программа, которая знакомит участников с услугами и преимуществами, предлагаемыми Сколково, и преимуществами создания стартапа там.[372]

Основная инициатива двустороннего сотрудничества в рамках Сколково состояла из Сколковского института науки и технологий (Сколтех), который является компонентом инновационного кластера Сколково.

Это частный научно-исследовательский институт для аспирантов, созданный в 2011 году в сотрудничестве с Массачусетским технологическим институтом (МТИ) для «воспитания нового поколения исследователей и предпринимателей, продвижения передовых научных знаний и развития инновационных технологий для решения важнейших проблем, стоящих перед Россией и миром».[373]

---

[370] «Что такое Сколково?», Сколково, 14 июля 2020 г., https://old.sk.ru/foundation/about/.

[371] «Программа по привлечению зарубежных стартапов запущена в Сколково», ТАСС, 25 июня 2020 года, https://tass.ru/ekonomika/6588743.

[372] «Программа софтлендинга в Сколково», доступ к которой получен 14 июля 2020 г., http://www.techno-preneur.net/Skolkovo - Softlanding 14 июля 2020 г., https://www.skoltech.ru/en/about/.

[373] «О компании», Сколтех, дата обращения 14 июля 2020 г., https://www.skoltech.ru/en/about/.

Виктор Вексельберг был важным игроком, инициировавшим это сотрудничество. Будучи президентом фонда «Сколково», он был одним из ключевых лидеры в создании Сколково и сыграл значительную роль в том, чтобы убедить МТИ сотрудничать со Сколково в создании Сколтеха, проекта, за который МТИ заплатил 300 миллионов долларов на начальном этапе разработки.

После нескольких лет сотрудничества Вексельберг был назначен попечителем МТИ в 2013 году и оставался на этой должности до 2018 года. В то время он был отстранен от этой должности в результате того, что его включили в санкционный список Министерства финансов.[374]

Сотрудничество Массачусетского технологического института и Сколтеха вступило в свою третью фазу.

Первый этап, который длился до 2016 года, состоял из помощи МТИ в запуске Сколтеха, включая участие в наборе начального преподавательского состава и приеме первых нескольких групп аспирантов.

За этот период в МТИ обучалось более 100 студентов Сколтеха, 24 преподавателя МТИ вели занятия в Москве, а в МТИ для Сколтеха было разработано 33 курса в рамках совместного плана разработки учебных программ.

МТИ также участвовал в проектировании кампуса Сколтеха, проводил обучение административного персонала и помог разработать первоначальную структуру управления Сколтеха, административную стратегию и операционные планы.[375]

Второй этап, длившийся с 2016 по 2019 год, был сосредоточен на совместной деятельности, направленной на содействие дальнейшему развитию института и Сколково в целом. На этом этапе основное внимание уделялось совместным исследовательским проектам, которые связывают

---

[374] Майк Экель, «Всемирно известный научный университет спокойно распутывается с российским миллиардером», Радиосвязь «Свободная Европа», 14 Января 2019 года, https://www.rferl.org/a/mit-quietly-untangles-itself-from - russian-billionaire/29708417.html.

[375] «История», Программа Массачусетского технологического института, 14 июля 2020 года, https://skoltech.mit.edu/node/8.

исследователей в двух партнерских институтах, совместным конференциям, а также консультациям и поддержке со стороны преподавателей МТИ в Сколтехе по исследовательским и институциональным вопросам по мере необходимости.[376]

Ухудшение политических отношений между США и Россией оказало значительное влияние на партнерство МТИ и Сколтеха, при этом персонал МТИ играет гораздо менее активную роль в управлении Сколтехом и менее непосредственно участвует в образовании. Несмотря на ограничения на сотрудничество и обмен, вызванные ухудшением политических отношений между Соединенными Штатами и Россией (в частности, из-за санкций), МТИ остается неотъемлемой частью Сколтеха, недавно подписав новое соглашение, которое расширяет партнерство на третий этап, который продлится до 2024 года и продолжит программы образовательных обменов 2-й фазы между двумя институтами.[377]

Недавние совместные проекты, объявленные программой, включают два из них в области ИИ: «Машинное обучение для квантово-усовершенствованных датчиков» и «Теоретические основы неконтролируемого глубокого обучения».

В настоящее время эти проекты являются скорее исключением, при этом основное внимание уделяется образовательному обмену, а не совместным проектам.

Коммерческое сотрудничество

Коммерческое сотрудничество между Россией и Соединенными Штатами в области ИИ остается относительно ограниченным.

Существующие партнерские отношения, как правило, являются пилотными проектами, такими как недавняя инициатива компании Synesis, базирующейся в Сколково, по использованию тепловизионных компонентов

[376] «Программа MIT Сколтех», Программа MIT Сколтех, 14 июля 2020 г., https://skoltech.mit.edu/.
[377] «Сколтех рассматривает новое соглашение с MIT как успех для российской науки в целом», ТАСС, 17 декабря 2019 г., https://tass.com/economy/1100349.

своей платформы Kipod «умный город» для измерения температуры тела клиентов и контроля норм социального дистанцирования в крупной сети аптек во Флориде.[378]

Еще один такой проект был разработан в сельскохозяйственной сфере, где российская компания по ИИ Cognitive Technologies внедряет свою пилотную автономную систему вождения Cognitive Agro для тракторов и полевых опрыскивателей в Соединенных Штатах в феврале 2021 года, в рамках лицензионного соглашения с крупным американским производителем сельскохозяйственной техники.[379] Российские компаний также участвовали в тестировании продуктов ИИ в Соединенных Штатах на ограниченной основе.

Например, летом 2020 года Яндекс объявил, что начал тестирование автомобилей без водителя в Анн-Арборе, штат Мичиган. Выбор места был обусловлен сочетанием факторов, в том числе более мягкими правовыми требованиями в Мичигане, которые позволяют компаниям тестировать автомобили без водителя и без инженера на борту транспортного средства. Первоначально Яндекс привез автомобили в Мичиган, чтобы продемонстрировать их на публичных тест-драйвах на Североамериканском международном автосалоне в Детройте. После того, как шоу было отменено из-за пандемии COVID-19, Яндекс решил воспользоваться правовым режимом штата, чтобы найти место для проведения долгосрочного тестирования транспортных средств в другой среде с точки зрения дорожных условий и правил дорожного движения.

В конце концов он остановился на Энн-Арборе, потому что это относительно большой город с большим количеством исследовательских и инженерных объектов, который также находится недалеко от автомобильного центра Детройта.

---

[378] «Интеллектуальную платформу для борьбы с коронавирусом создали в Сколково», ТАСС, 3 июня 2020 г., https://tass.ru/ekonomika/8636089.

[379] Лори Бедорд, «Российская компания хочет автоматизировать американское сельскохозяйственное оборудование», Успешное сельское хозяйство, 6 ноября 2020 г., https://www.agriculture.com/news/technology/cognitive-agro-pilot-coming.

Автомобили представляют собой беспилотные автомобили четвертого поколения, изготовленные в партнерстве с Hyundai Motors и основанные на модели Sonata. Яндекс ранее тестировал свои транспортные средства в Сколково и в Тель-Авиве.[380]

Инициатива Яндекса по беспилотным автомобилям началась как результат его отношений с Uber, после того как он фактически выкупил операции последнего в России в 2017 году. Вскоре после начала своей программы тестирования в Энн-Арборе две компании объявили, что они создали отдельную компанию, которая сосредоточится на самоуправляемых автомобилях, при этом Яндексу принадлежит 73% акций, Uber – 19%, а остальное принадлежит менеджерам и сотрудникам Яндекса.[381]

Потенциально более существенное совместное предприятие предполагает создание совместной лаборатории данных Sber и Visa, где будут изучаться анонимизированные данные кредитных карт для лучшего прогнозирования тенденций в поведении клиентов. Лаборатория, расположенная в кампусе Sber, будет использовать инструменты ИИ и машинного обучения для создания вероятностных гипотез с целью «повышения удобства и качества услуг для клиентов».

Ранее Sber и Visa сотрудничали в разработке решений для ИИ. Например, в июне 2020 года компании объединились с ритейлером Azbuka для создания круглосуточного магазина без кассира, в котором с покупателей автоматически взимается плата за покупки при выходе из здания.[382]

Сотрудничество с европейскими государствами и институтами

---

[380] ««Яндекс» тестирует беспилотные автомобили в США» 6 августа 2020 года, https://www.cnews.ru/news/top/2020-08-06_yandeks_pristupil_k_testirovaniyu.

[381] Пол Соэрс, «Uber и Яндекс объединяют свои сервисы обмена поездками, чтобы сформировать новую компанию стоимостью 3,8 миллиарда долларов, ориентированную на Россию и соседние рынки», 13 июля 2017 г., https://venturebeat.com/2017/07/13/uber-and-yandex-merge.

[382] «Сбербанк и Visa запускают в России лабораторию данных», 30 сентября 2020 г., https://www.cnews.ru/news/line/ 2020-09-30_sberbank_i_visa_zapuskayut_v.

Сотрудничество России в области ИИ с государствами-членами ЕС подвержено некоторым из тех же ограничений, что и сотрудничество России с Соединенными Штатами.

Российские лидеры указали, что, несмотря на геополитическую напряженность, ЕС остается важным экономическим партнером для России.

Недавно министр иностранных дел России Сергей Лавров выделил ИИ как одну из областей, сотрудничество в которой принесет пользу обеим сторонам.

В то же время он отметил, что сотрудничество может быть только равноправным, с учетом интересов обеих сторон. Он отметил, что Россия не будет делать никаких односторонних жестов доброй воли.[383]

Для дальнейшего развития этого сотрудничества Россия играет ключевую роль в европейских органах, которые устанавливают нормы для технологий ИИ.

Например, в ноябре 2020 года Специальный комитет Совета Европы по технологиям ИИ избрал Андрея Незнамова, исполнительного директора Центра исследований данных для государственных органов Sber, своим председателем.

Незнамов является соавтором Национальной стратегии развития ИИ и Концепции регулирования технологий ИИ и робототехники.[384]

В качестве председателя межправительственной группы до конца 2021 года он будет содействовать организации и проведению глобальных консультаций между европейскими государствами и представителями науки и бизнеса по вопросам регулирования технологий ИИ в Европе.[385]

Сотрудничество России с Европой в области ИИ сдерживается рядом факторов, в том числе западными санкциями в отношении передачи технологий

---

[383] «Россия не допустит «игры» в одни ворота» с Евросоюзом, заявил Лавров» 3 ноября 2020 года, https://ria.ru/20201103/evrosoyuz-1582872350.html.

[384] Российская Федерация является членом Совета Европы с 1996 года, и наличие должностей в различных комитетах не является чем-то необычным. Совет Европы отличается и отделен от Совета Европейского Союза.

[385] Основной задачей Специального комитета Совета Европы по ИИ является определение порядка регулирования технологий ИИ в Европе. Комитет был создан в 2019 году по решению Комитета министров Совета Европы. В него входят представители государств-членов Совета Европы, а также наблюдатели от различных международных органов и представители научных и деловых кругов», TAdviser, 9 ноября 2020 года.

в Россию: проблемы безопасности, которые заставляют обе стороны проявлять осторожность в выявлении своих уязвимостей, общее отсутствие доверия к сотрудничеству в области технологий из-за страха перед хакерскими атаками, чувство экономической конкуренции и спад в российской экономике, который сделал Россию менее привлекательной для европейских партнеров.

В то же время есть некоторые области, в которых возможен синергизм, и сотрудничество может быть выгодным для обеих сторон. К ним относится использование ИИ в меганаучных проектах, где уже существует сотрудничество, таких как физика элементарных частиц и международная космическая станция.

Исследования и разработки в области здравоохранения являются еще одной потенциальной областью сотрудничества, поскольку их можно в значительной степени отделить от более чувствительных проблем безопасности. Аналогичным образом, умные города и умная инфраструктура не так подвержены подозрениям и могут стать еще одной областью сотрудничества.[386]

Академическое сотрудничество

Как и в Соединенных Штатах, Сколтех лидирует в академическом сотрудничестве с европейскими исследователями в области ИИ.

В одном из таких проектов ученые из Сколковского института науки и технологий, французского института INRIA и японского института RIKEN используют алгоритмы ИИ для анализа мозговых волн посредством электрической активности, чтобы понять эмоциональное состояние людей и уровень психического стресса.[387]

В отдельной работе, исследователи из того же института Сколтеха работают с учеными из Университета Граца и Солнечной обсерватории

[386] Иван Данилин, «Цифровая трансформация: построение диалога ЕС-Россия (на примере ИИ)» «Краткое изложение 2, май 2019 г., http://eu-russia-expertnetwork.eu/en/analytics/euren-brief-02.
[387] «В Сколтехе компьютер обучают понимать эмоции людей» Computerworld, 29 декабря 2020 г., https:// computer world.ru/news/V-Skoltehe-kompyuter - обучают-понимать-эмоции-людей.

Канцельхоэ в Австрии над разработкой нового метода глубокого обучения для последовательной классификации и количественной оценки качества солнечных изображений с наземных солнечных обсерваторий.

Метод был разработан в Сколтехе в рамках интегрированной сетевой исследовательской группы SPRING solar physics, которая обеспечивает автономный мониторинг Солнца с использованием новейших технологий в области наблюдательной физики Солнца.

SPRING является частью проекта SOLARNET, который разрабатывает Европейский солнечный телескоп. Проект поддерживается Европейским союзом «Горизонт науки и инноваций 2020». Сколтех также участвует в инициативе и является одним из 35 международных партнеров.[388]

Академические партнерские отношения Сколтеха с западными университетами выходят за рамки государств-членов ЕС.

Партнерство с Университетом Кертина в Австралии и Университетом Калгари в Канаде работает над разработкой алгоритма, который может определять вязкость нефти без необходимости извлечения образцов путем анализа сканирования ядерного магнитного резонанса.

По мнению исследователей, аналогичные методы могут быть использованы в сельском хозяйстве и пищевой науке.[389]

Некоторые инициативы по сотрудничеству выходят за рамки Сколтеха и даже вообще за пределы Москвы.

Например, ученые из Томского государственного университета (ТГУ) и Болгарского университета Пловдива, используя грант Национального научного фонда Болгарии, объявленный 21 апреля 2020 года, будут использовать алгоритмы обработки больших данных, созданные в ТГУ, чтобы понять распространение мифов об опасности вакцинации и преимуществах гомеопатии.

---

[388] «Искусственный интеллект помогает наблюдать за Солнцем» ComNews, декабрь. 14 декабря 2020 года, https:// www.comnews.ru/digital-economy/content/212176/2020-12-14/2020-w51/iskusstvennyy.

[389] «Искусственный интеллект научился определять вязкость нефти» CNews, 3 ноября 2020 г., https://www.cnews.ru/news/line/2020-11-03_iskusstvennyj_intellekt.

На основе этой работы исследователи разработают рекомендации для сектора здравоохранения Болгарии к 2022 году.[390]

Также разрабатываются совместные академические программы, такие как магистерская программа по науке о данных и ИИ, недавно созданная в Институте экономики, математики и информационных технологий Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации (РАНХИГС) в сотрудничестве с Лондонским университетом.[391]

Аналогичная инициатива, разработанная Сибирским государственным университетом и Университетом Ульма в Германии, выиграл международный конкурс с предложением наладить долгосрочное сотрудничество между двумя университетами в области ИИ для организации обменов, стажировок и совместных исследовательских проектов.[392]

Совместные проекты в коммерческом сотрудничестве

Российские компании инициировали несколько совместных предприятий с европейскими партнерами в области ИИ. Например, совместное российско-британское предприятие использует каскадные нейронные сети для оценки личности. Партнерство осуществляется между британской коммерческой фирмой BestFitMe и Российским научно-исследовательским институтом.[393]

В другом случае российско-украинский стартап под названием Signum.ai собрал деньги для разработки приложения, которое может собирать и анализировать данные из социальных сетей, блогов, форумов и других интернет-порталов в режиме реального времени с использованием нескольких

[390] «Большие данные», FutureRussia.gov.ru, 21 апреля 2020 года, https://futurerussia.gov.ru/nacionalnye-proekty.
[391] «Наука о данных – в ВТБ рассказали о профессиях будущего и объяснили, почему их банкам нужны выпускники РАНХиГС,» Новости AI, 27 июля 2020 г., https://ai.ru/2020/07/predstaviteli_data_science_komand.
[392] «Ученым СибГУ вручили диплом за победу в конкурсе Россия и Германия: научно-образовательные мосты», NGS24, 16 сентября 2020 г., https://ngs24.ru/news/more/69469139.
[393] «Искусственный интеллект научили определять черты характера по фото» Научная Россия, 29 июля 2020 г., https://scientificrussia.ru/articles/iskusstvennyj-intellekt-nauchili-opredelyat-cherty-haraktera-po-foto.

методов, включая сетевой анализ, и позиционируется как инструмент, особенно полезный для маркетинга и продаж команды.[394]

Финско-российская фирма по цифровизации промышленности Zyfra разработала платформу цифрового управления производством, которая позволяет нефтегазовым компаниям централизовать оперативное управление с помощью ИИ. Она ориентирована на продажу своей продукции в Южной Азии и Латинской Америке.[395]

Российские компании в области ИИ стремятся продавать свою продукцию в Европейском Союзе.

Базирующаяся в Сколково компания «Диагностика-М» продала компоненты своей системы безопасности Radar-IQ клиентам в Словакии. Система использует ИИ для наблюдения за безопасными зонами, такими как порты, аэропорты, электростанции, тюрьмы и т.д.[396]

Коммерческие усилия идут в обоих направлениях, и европейские компании стремятся продавать свои продукты на основе ИИ в России.

Например, европейская компания по ИТ-услугам Atos недавно запустила русскоязычного чат-бота, включающего SAP Intelligent Robotic Process Automation (RPA), который автоматизирует повторяющиеся ручные процессы путем создания, планирования, управления и мониторинга интеллектуальных ботов, позволяя сотрудникам тратить время на выполнение важных задач, а не на рутинные операции.[397]

Инициативы в других частях мира

В то время как Восточная Азия и Европа были основными направлениями деятельности российских технологических компаний, стремящихся развивать совместные проекты в области ИИ, они также установили несколько

[394] «Стартап с русско-украинскими корнями Signum.ai привлек 500 долларов США»,7 июля 2020 года, https://www. cnews.ru/news/line/2020-07.
[395] «СП Газпрома и Zyfra по цифровой индустриализации смотрит на рынок нефти и газа Индии», Economic Times, 25 ноября 2020 г., https://m.economictimes.com/industry/energy/oil-gas/gazprom-zyfra-jcms.
[396] «Резидент ОЭЗ»Технополис Москва» разработал систему охраны периметра с применением искусственного интеллекта,17 августа 2020 года, https://safe.cnews.ru/news/line/2020-08-17_rezident_oez_tehnopolis.
[397] «Atos запустил русскоязычного бота на базе SAP Conversation AI», CNews.Ru, 7 мая 2020 года, https://www.cnews.ru/news/line/2020-05 – 07.

партнерских отношений с другими странами мира, особенно на Ближнем Востоке и в Индии.

Объединенные Арабские Эмираты и Ближний Восток

Партнерские отношения в ОАЭ включают как академические, так и коммерческие предприятия.

Что касается академической стороны, Сколтех сотрудничает с Университетом Шарджи над созданием совместной лаборатории ИИ, которая могла бы разрабатывать приложения в области медицины, энергетики и аэрокосмической промышленности.

Это предприятие основано на Меморандуме о взаимопонимании, подписанном двумя университетами в ноябре 2019 года.[398]

С коммерческой стороны, совместное предприятие Российского фонда прямых инвестиций, Группы Medscan и компании из ОАЭ под названием Group42 запустило проект по диагностике и выявлению пневмонии, в том числе COVID-19, с использованием компьютерной томографии в сочетании с технологией ИИ, разработанной совместным предприятием.[399]

VisionLabs недавно открыла офис в Дубае. Офис будет сосредоточен на продажах и оказании технической поддержки пилотным проектам в регионе в рамках стратегического плана развития компании по расширению своих позиций в регионе и более эффективной работе с партнерами и поставщиками по всему Ближнему Востоку.

Ближний Восток является вторым по величине рынком компании. На Ближнем Востоке ее наиболее популярные продукты включают биометрическую платформу LUNA для умных и безопасных городов, которая используется полицией Дубая для управления транспортными потоками

[398] «Первый совместный семинар Сколтеха и UOS посвящен приложениям ИИ и новым технологиям», Сколтех, 10 октября 2020 г., https://www.skoltech.ru/en/2020/10/inaugural.
[399] «Российский фонд прямых инвестиций запускает диагностику COVID-19 с использованием технологии искусственного интеллекта», Tass.com, 24 апреля 2020 года, https://tass.com/science/1149433.

и управления транспортными потоками, а также продукт проверки подлинности KYC для банковских операций.[400]

Неудивительно, что использование ИИ для разведки энергии является одним из основных направлений российских инициатив по сотрудничеству на Ближнем Востоке.

По словам вице-премьера России Александра Новака, Россия и энергетическая компания Саудовской Аравии Saudi Aramco обсуждают партнерство для работы в энергетических проектах в рамках двусторонней программы стратегического сотрудничества, согласованной обеими странами в октябре 2019 года.

Планы включают использование технологий ИИ для улучшения возможностей добычи нефти для обоих партнеров.[401]

Российские компании также обратились к Ближнему Востоку за финансированием своих инициатив в области ИИ.

Стартап по распознаванию лиц и компьютерному зрению NtechLab привлек 15 миллионов долларов нового финансирования, частично из источников в неназванных странах Ближнего Востока.

Компания, которая была основана в 2015, использует ИИ и нейронные сети для идентификации лиц, силуэтов и действий по видеозаписям. Финансирование предназначено для дальнейшего развития ассортимента продукции и выхода на новые рынки. NtechLab заявила, что планирует использовать инвестиции для разработки автоматического обнаружения «агрессивного поведения» и разработки программного обеспечения для распознавания транспортных средств. Финансирование также будет использовано для выхода на рынки Ближнего Востока, Юго-Восточной Азии и Латинской Америки.[402]

---

[400] «VisionLabs поможет развитию искусственного интеллекта в ОАЭ», CNews, ноябрь. 25 декабря 2020 года, https://www.cnews.ru/news/line/2020-11- 25.

[401] «Саудовская Аравия рассматривает возможность участия в проектах ИИ в России», Вести, 21 декабря 2020 г., https://www.vesti.ru/finance/article/2501550.

[402] «РФПИ и фонды Ближнего Востока вложили более 1 млрд руб. в российского разработчика NtechLab».

В других странах Ближнего Востока сотрудничеству с Израилем способствовало двустороннее соглашение 2010 года, предусматривающее расширение сотрудничества в области промышленных исследований и разработок.

С помощью этого механизма Группа РОСНАНО, российское инновационное учреждение в области нанотехнологий, и Израильское инновационное агентство создали механизм грантов для команд, состоящих как из российских, так и израильских партнеров.

Согласно веб-сайту Группы РОСНАНО, проекты должны быть связаны с областью нанотехнологий или смежными высокотехнологичными секторами, должны иметь потенциальные рынки в Израиле и России и должны планировать коммерциализацию технологии через три-пять лет. Фонд инфраструктурных и образовательных программ

Группы РОСНАНО, управляющий российской долей грантовых средств, был основан в 2010 году путем реорганизации государственного учреждения «Российская корпорация нанотехнологий».

ИИ является одним из приоритетных направлений гранта.

Российские лидеры рассматривают совместные научные исследования и разработки в качестве ключевого направления в развитии российско-израильского двустороннего сотрудничества.

Это сотрудничество рассматривается как выгодное не только с точки зрения технологических преимуществ, но и с точки зрения предоставления России доступа к ключевому посреднику на Ближнем Востоке.

Технологическое сотрудничество также обеспечивает связь с русскоязычной диаспорой в Израиле, что имеет решающее значение для экономического развития Израиля.[403]

В других частях света

[403] «Россия и Израиль начали новый отбор проектов по промышленным НИОКР,» Ведомости, 16 июля 2020 г., https://www.vedomosti.ru/press_releases/2020/07/16/r.

Усилия России по расширению сотрудничества в области ИИ в других частях мира относительно ограничены и в основном сосредоточены на маркетинге российских продуктов ИИ.

Индия – одна из стран, которая в последнее время находится в центре внимания российских усилий по расширению сотрудничества в сфере ИИ. Это только начинается, в первую очередь через организацию БРИКС.

На мероприятии, организованном Правительством России в декабре 2020 года с широким участием Индии, первый заместитель председателя исполнительного совета Sber в своих замечаниях сосредоточился на расширении сотрудничества между Россией и Индией в области исследований и разработок в области ИИ, «поскольку обе страны стремятся занять лидирующие позиции на мировом рынке».[404]

Помимо этих усилий, сотрудничество с Индией практически не осуществляется, хотя крупные российские корпорации, такие как «Газпром нефть», стремятся получить доступ к индийскому рынку решений на основе ИИ для повышения эффективности добычи углеводородов.[405]

Россия предприняла некоторые ограниченные усилия для проникновения на довольно отдаленные рынки в области ИИ, в том числе в Латинской Америке и Африке.

Латинская Америка считается потенциально очень прибыльным рынком, особенно в области приложений, которые помогают носителям испанского языка изучать английский. Российская компания разработала для этой цели приложение, предназначенное для детей, которое использует голосовой помощник на основе ИИ и продается в Мексике и Чили, с планами последующего расширения на другие страны Латинской Америки.[406]

---

[404] «Зонтик БРИКС для расширения сотрудничества Индии и России в области искусственного интеллекта», Zee News, 18 ноября 2020 г., https://zeenews.india.com/india/brics-umbrella-to-increase-india-russia-collaboration.

[405] «Совместное предприятие Газпрома и Zyfra по цифровой индустриализации смотрит на рынок нефти и газа Индии».

[406] «Старт продаж приложения Приятель в испаноязычных странах Латинской Америки», Т-Советник, 12 августа 2020 г., https://www.tadviser.ru/index.php/MyBudd.

Российские предприятия в Африке остаются относительно ограниченными, с акцентом на коммерческие продажи продуктов с поддержкой ИИ и обучение африканских студентов в российских высших учебных заведениях, ориентированных на технологии.

В сфере образования существует давняя история обучения африканских студентов в российских университетах, таких как Университет дружбы народов имени Патриса Лумумбы. Общее число африканских студентов, обучающихся в России по всем направлениям, составляет более 27 000.

Наибольший процент приходится на технические и инженерные области, включая ИИ, хотя точные цифры отсутствуют.[407]

Что касается коммерческих продаж, российские технологии ИИ особенно востребованы в горнодобывающей промышленности и других отраслях по добыче природных ресурсов в Африке.

Одним из примеров является Группа компаний Цифра, которая разработала платформу для работы с производственными данными, использующую ИИ и промышленный интернет вещи в горнодобывающей, нефтегазовой, химической и машиностроительной промышленности.

Ее продукция используется по всему миру, в том числе в ряде стран Латинской Америки и Африки. Недавно он получил 1 миллиард рублей инвестиций от WEB Ventures, инвестиционного подразделения ВЭБ РФ, с целью расширения своих продаж на международных рынках.[408]

[407] «Юрий Кукин, Ирина Мандрыкина, Вадим Белозерцев, «За знаниями и снегом: что притягивает африканских студентов в учебе в России»», ТАСС, 29 декабря 2020 г., https://tass.ru/obschestvo/10353061.
[408] «VEB Ventures инвестирует 990 млн рублей в разработчика решений для цифровизации промышленности Группу»Цифра» 23 декабря 2020 года, https://ru-bezh.ru/press-releases/38953-veb.