2021; 51(6): 52-70 США & Канада: экономика, политика, культура / USA & Canada: economics, politics, culture

УДК 327.004.8
DOI: 10.31857/S268667300015219-0

Разведсообщество США и искусственный интеллект

Я.В. Селянин

Институт мировой экономики и международных отношений РАН.
Российская Федерация, Москва, Профсоюзная ул., 23.
ORCID: https://orcid.org/0000-0002-3802-0563 e-mail: yaroslav.selyanin@yandex.ru

Резюме: По мнению Комиссии национальной безопасности по искусственному интеллекту – КНБИИ *(National Security Commission on Artificial Intelligence),* разведсообщество – это один из главных американских государственных выгодоприобретателей от создания и практического использования технологий искусственного интеллекта (ИИ). Специальные службы США могут получить максимальный и наиболее быстрый результат, если эти технологии будут приняты на вооружение. Однако сегодня спецслужбы сталкиваются с дефицитом специалистов, проблемами технического и организационного характера. В статье рассматриваются цели, задачи и подходы американских спецслужб к организации работ в области разработки и внедрения ИИ. Даётся обзор стратегии разведсообщества в области ИИ, предписаний Конгресса и рекомендаций комиссии.

Ключевые слова: США, искусственный интеллект, машинное обучение, разведсообщество США, государственная политика США в области развития науки и техники

Для цитирования: Селянин Я.В. Разведсообщество США и искусственный интеллект. *США & Канада: экономика, политика, культура*. 2021; 51(6):52-70.
DOI: 10.31857/S268667300015219-0

U.S. Intelligence Community and Artificial Intelligence

Yaroslav V. Selyanin

Institute of World·Economy and International Relations, Russian Academy of Sciences.
23, Profsoyuznaya Str., Moscow, 117997, Russian Federation
ORCID: https://orcid.org/0000-0002-3802-0563 e-mail: yaroslav.selyanin@yandex.ru

Abstract: According to the National Security Commission on Artificial Intelligence (NSCAI), the intelligence community (IC) is one of the main U.S. state beneficiaries from the AI creation and practical use. American IC can get the maximum and fastest result from their adoption into service. However, today they face a shortage of specialists, technical and organizational problems. The article considers IC goals, objectives and approaches in the field of AI. The article contains an overview of the IC's AI strategy, congressional regulations, and NSCAI recommendations.

Keywords: USA; artificial intelligence; machine learning; U.S. intelligence community; the U.S. Public Policy in the Area of Science and Technology Development

For citation: Selyanin Y.V. U.S. Intelligence Community and Artificial Intelligence. *USA & Canada: Economics, Politics, Culture.* 2021; 51 (6): 52-70.
DOI: 10.31857/S268667300015219-0

В августе 2016 г. советник президента РФ по вопросам развития интернета Герман Клименко описал в интервью один из технически возможных методов слежки американских спецслужб за теми гражданами России, которые могут интересовать их в силу своего служебного положения [1]. Этот принцип основан на использовании данных о геолокации и тесных связях разведсообщества с ведущими ИТ-компаниями США, которые могут определять местоположение устройств под управлением операционных систем своего производства по всему миру. Поэтому для них не составляет труда получить информацию о смартфонах, которые регулярно посещают определённые точки Земного шара, где может находиться какое-либо ведомство или, например, военный объект. Если спецслужбы возьмут перемещение таких устройств по планете на контроль, то некоторые из них рано или поздно могут появиться на территории страны, у которой с США есть договор об экстрадиции [2]. Тогда в один совсем не прекрасный для хозяина такого устройства день неизвестные люди в штатском могут задать ему несколько вопросов и сделать предложение, от которого ему будет очень сложно отказаться [3]. 2020 год наглядно продемонстрировал, как эта схема будет работать на практике.

Так, в мае стало известно, что частная фирма «Орбитал инсайт» *(Orbital Insight)* проанализировала влияние режима самоизоляции, который вводился в РФ из-за пандемии ковид-19 (*COVID-19)*, на работу ряда российских оборонных предприятий [4]. Аналитики компании с использованием методов машинного обучения обработали некие «анонимные телефонные данные, полученные от различных партнёров», и «другую информацию из открытых источников». Сама по себе «Орбитал инсайт»– это не просто рядовая коммерческая фирма: во-первых, она занимается анализом «геопространственной» информации (*geospatial analytics*), «которая идентифицирует географическое положение и характеристики природных или искусственных объектов и границ на земле» [5]; во-вторых, членом её консультативного совета является Роберт Кардилло *(Robert Cardillo)*, бывший глава Национального агентства геопространственной разведки США *(National Geospatial-Intelligence Agency)*, входящего в американское разведсообщество. Эти факты позволяют сделать предположение о том, какого рода «различные партнёры» предоставили данные для анализа.

В июле того же года американские СМИ сообщили, что «группа исследователей из Университета штата Миссисипи» отслеживала перемещения по планете мобильных телефонов, которые изначально были замечены в посещении российских правительственных учреждений и военных объектов. Осуществить это позволило коммерческое программное обеспечение и различные собираемые устройствами и отдельными приложениями данные, в том числе о геолокации. Финансирование проекта обеспечили вооружённые силы США. Его целью была демонстрация современных возможностей по сбору и обработке данных из открытых источников с использованием коммерческого ПО [6].

Всё это стало возможным благодаря упрощению доступа к данным из-за развития и широкого внедрения информационно-коммуникационных технологий

и использованию методов машинного обучения, больше известных как искусственный интеллект (ИИ). Машинное обучение, по сути, заключается в том, что через алгоритм последовательно пропускают специальным образом подготовленные (размеченные) наборы данных (это тренировочные или обучающие данные) и подбирают определённые внутренние коэффициенты так, чтобы при обработке проверочных наборов данных система давала верный результат. Качество системы на основе машинного обучения напрямую зависит, во-первых, от качества обучающих и тестовых данных, а во-вторых, от их соответствия данным, с которыми искусственный интеллект работает на практике. Правда, пока речь идёт о так называемом «узком ИИ». Строго говоря, такой искусственный интеллект не имеет ничего общего с интеллектом и представляет собой алгоритм, заточенный на решение конкретной задачи, вроде распознавания лиц или речи. Однако свою эффективность такие системы уже доказали не раз.

Не удивительно, что разведсообщество США крайне заинтересовано в том, чтобы принять их на вооружение. Такой интерес к технологии демонстрирует, например, следующее обстоятельство. В 2013–2019 гг. Агентство национальной безопасности *(National Security Agency)* США ежегодно публиковало сборник материалов «Новая волна» *(The New Wave)*. Каждый раз он включал научные статьи, которые относятся к какой-либо одной новой технологии. Машинное обучение было его темой два года подряд – в 2018 и 2019 гг. [7], [8].

Как финансируется этот интерес специальных служб США, можно судить лишь по косвенным данным. Например, в стратегии разведсообщества в области ИИ указано, что финансовые ресурсы разведки скромны и не могут сравниться с ресурсами военных [9]. Однако там же указано, что члены разведсообщества имеют доступ к результатам НИОКР, проводимых в интересах вооружённых сил.

В целом, открытые данные позволяют оценить цели, задачи и проблемы в этой области. Силовые структуры в рамках работ по ИИ активно сотрудничают с технологическими компаниями и научными кругами. По понятным причинам, подробности не раскрываются или раскрываются неохотно. Однако очевидно, что политическое решение о широком внедрении ИИ в разведсообществе, как и в случае вооружённых сил, принято и будет реализовываться независимо от реальной готовности к этому самих технологий.

ПОЛИТИКА РАЗВЕДСООБЩЕСТВА В ОБЛАСТИ ИИ

Свою стратегию в области искусственного интеллекта разведсообщество приняло ещё в январе 2019 г. Почти на месяц раньше, чем президент Трамп подписал указ о государственной стратегии США в этой сфере [10], [Селянин Я.В. 2020a: 140-163], а Министерство обороны опубликовало в открытом доступе краткое содержание собственной стратегии в области ИИ [12], [Селянин Я.В. 2020b].

Название документа – «Целевая инициатива: стратегия усиления интеллекта/разведки с помощью машин» (*The AIM Initiative. A Strategy for Augmenting*

Intelligence Using Machines) – не содержит словосочетания «искусственный интеллект», но отражает суть интереса разведсообщества к данным технологиям [9].

Он заключается именно во взаимном дополнении способностей человека и вычислительной техники в области анализа данных и, как следствие, в более полном извлечении информации из них. Искусственный интеллект, автоматизация процессов и «дополнение способностей личного состава разведслужб с помощью технологий» (*Artificial intelligence, process Automation, and IC officer Augmentation», AIM AAA technologies, AAA*) – три кита, которые, как рассчитывают спецслужбы, выведут информационно-аналитическое обеспечение процесса принимаемых решений на качественно иной уровень [9].

В целом подходы, задачи и проблемы разведсообщества в области использования ИИ схожи с таковыми в Министерстве обороны (МО), а важность этих технологий для спецслужб обосновывается аналогичным МО образом: «Наши противники – особенно Россия и Китай – также признают потенциал ИИ для военных и разведывательных операций и активно финансируют работы в этой сфере» [9].

Однако, чтобы полноценно использовать искусственный интеллект в своих интересах, разведсообществу придётся решить значительное количество проблем. Стратегия разделяет их на несколько категорий и устанавливает определённые временные рамки их преодоления с учётом приоритетности и технических возможностей.

Безотлагательного решения требуют задачи в таких областях, как подготовка и использование данных; доступ разведсообщества к вычислительным мощностям; повышение эффективности научно-технической разведки *(Science and Technical Intelligence)* в области ИИ; получение специалистами спецслужб фундаментального понимания особенностей и уязвимостей этих технологий.

Данные – это то сырьё для работы ИИ, перерабатывая значительные массивы которого он даёт результат. Для обучения и проверки качества работы алгоритмов также нужно огромное количество данных, специальным образом отобранных и подготовленных. Причём они должны быть того же типа, как и те, с которыми системам придётся работать на практике. В контексте задач разведсообщества это часто трудно реализовать. Поэтому стратегия требует организовать внутри сообщества общий доступ служб к учебным и тестовым наборам данных и к «базам экспертных знаний, которые содержат неявные знания специалистов в области разведки». Интересно, что авторы документа учли существование конкуренции между службами и особо предупредили их, что соблюдение мер по защите информации не является основанием для «неоправданного ограничения» её обмена внутри сообщества.

Большие вычислительные мощности – второе условие, необходимое для реализации и эффективного использования систем с ИИ [Селянин Я.В. 2019a: 179-201], [Селянин Я.В. 2019b: 137-166]. В связи с этим стратегия предполагает развитие соответствующей цифровой инфраструктуры разведсообщества *(IC Information Technology Enterprise)*, включая «завершение создания системы высокопроизводительных вычислений» (то есть собственных суперкомпьютеров).

Возможно, речь идёт о вычислительных мощностях, создававшихся в Форт-Мид *(Fort Meade)*, где находятся штаб-квартиры Агентства национальной безопасности и Киберкомандования США. Так, в оборонном бюджете США на 2012, 2013 и 2014 фин. гг. было одобрено финансирование по теме «Центр высокопроизводительных вычислений» в Форт-Мид. Во всех трёх документах названия программ отличались друг от друга (в 2012 фин. г. – *High Performance Computing Capacity*; в 2013 фин. г. – *High Performance Computing Center Inc 2*; в 2014 фин. г. – *High Performance Computing Capacity Inc 3*), однако, по всей видимости, речь идёт о трёх этапах работ на одном и том же объекте. Стоит также добавить, что данный проект был предусмотрен законом о расходах на военное строительство на 2012 фин. г. *(Military Construction Authorization Act for Fiscal Year 2012)*, а в оборонном бюджете США на 2016 фин. г. министр обороны был уполномочен в рамках расширения программы строительства Центра высокопроизводительных вычислений *(High Performance Computing Center)* в Форт-Мид построить генерирующие мощности производительностью до 60 МВт для того, чтобы обеспечить резервный источник электроэнергии для соответствующей нагрузки [12], [13], [14], [15].

С учётом опасений в использовании ИИ противником, разведсообществу ставится задача усилить работу по линии научно-технической разведки *(S&TI)* для оценки потенциала иностранных государств и принятия мер по противодействию таким угрозам.

Всё это уже на самых ранних этапах работы требует иметь подготовленный личный состава. Здесь разведсообщество, как и иные госструктуры, испытывает нехватку специалистов. Дефицит кадров настолько велик, что спецслужбы опасаются даже внутренней конкуренции за квалифицированных сотрудников.

В краткосрочной перспективе разведсообщество намерено принять на вооружение решения на основе «узкого ИИ», включая как коммерческие, так и с открытым исходным кодом. Однако стратегия предостерегает ведомства от внедрения ИИ «ради галочки» и требует оценки того, удовлетворяют ли принимаемые системы нужды спецслужб и отвечают ли их стандартам в области безопасности.

Дело осложняется тем, что ИИ сегодня имеет проблемы не только с надёжностью, кибербезопасностью и «объяснимостью». Стоит отметить, что сами разработчики не понимают логику даже хорошо работающего ИИ и не могут объяснить, почему система принимает то или иное решение. Корни проблемы кроются в фундаментальных принципах работы самой технологии. Другую характерную исключительно для ИИ и более опасную угрозу создают так называемые атаки с использованием состязательного обучения *(adversarial learning, adversarial AI, adversarial ML)*. Они нацелены на уязвимости не в программном или аппаратном обеспечении системы, а на особенности работы самого алгоритма. Идея состоит в том, чтобы через изменение («отравление») обучающих, тестовых и рабочих наборов данных, создать у владельца системы ложное впечатление о её качестве работы либо заставить систему выдать нужный атакующим результат. Это может иметь катастрофические последствия для эффективности системы. Поэтому в качестве «ценных активов» службы отныне рассматривают не

только собираемые данные, но и алгоритмы для их обработки [Kegelmeyer W.P. 2019: 10-14], [Whyte C. 2020: 2015-232], [9].

Опасность состязательных методов ИИ *(adversarial AI techniques)*, с точки зрения США, усугубляется тем, что многие страны имеют необходимые для их применения инструменты, наборы данных и специалистов. Причём последние могли обучаться в тех же университетах, что и американские специалисты.

Всё это вынуждает США создавать методы и средства обеспечения надёжности систем с ИИ и противодействия любым типам атак, включая проведения их испытаний для выявления возможностей и ограничений. Это очень непростая задача, поскольку большие сложности вызывает даже просто определение контрольных показателей *(benchmarks)*, которые позволят адекватно оценивать успешность хода работ по созданию системы и определять её итоговое качество. В случае коммерческого ПО стратегия предписывает разработать порядок его допуска к эксплуатации в интересах разведсообщества, в том числе в закрытых сетях. Общедоступные решения с ИИ предполагается дорабатывать под конкретные нужды служб.

Аналогично военным, которые создали Объединённый центр искусственного интеллекта *(Joint Artificial Intelligence Center, JAIC)*, разведсообщество намерено учредить свою специальную организацию *(AIM Center)*. Её штат должен быть укомплектован специалистами в области ИИ и машинного обучения из разведсообщества и ИТ-индустрии. Планируется наладить сотрудничество с такими структурами, как Агентство перспективных исследований в сфере разведки, Управление перспективных исследований Министерства обороны, созданная при поддержке ЦРУ венчурная компания «Ин-кью-тел» (*In-Q-Tel*) [16], национальные лаборатории Министерства энергетики, Экспериментальный отдел по оборонным инновациям МО *(Defense Innovation Unit-Experimental, DIUx)* и коммерческие компании.

В среднесрочной перспективе основная цель разведсообщества состоит в получении технических средств, которые способны работать – выявлять взаимосвязи – с разнотипными и разрозненными данными.

В долгосрочной перспективе специальные службы намерены финансировать фундаментальные исследования по созданию «сильного ИИ», который способен извлекать информацию из неполных и скудных данных, учитывая при этом контекст. Интересно, что к этой же категории отнесено решение кадровых проблем разведсообщества, разработка нормативно-правовой базы спецслужб в области использования ИИ, а также решение проблемы выявления дипфейков *(deepfake)* [17].

И если первые две задачи невозможно решить быстро из-за сложности подготовки специалистов, которая в силу сложности технологий должна начинаться со школы, то относительно проблемы выявления дипфейков нет ясности в том, возможно ли её решить в принципе.

Под дипфейками *(deepfake или machine-manipulated media)* понимаются «аудио-, видеозаписи и изображения, сгенерированные или существенно модифициро-

ванные с использованием методов машинного обучения» настолько качественно, что практически неотличимы от настоящих. Целью их создания в контексте внешней и внутренней политики может быть проведение операций по дезинформации качественно иного уровня, включая «искажение информации о каком-либо событии, искажение слов или поведения отдельных лиц, либо изображение лиц, которых на самом деле не существует» [17]. Это явление вызывает большую тревогу у разведсообщества, поскольку значительно усложняет задачу определения подлинности аудио-, видеоматериалов и графических изображений [9].

В целом разведсообщество осознаёт, что ему сложно тягаться с частными компаниями и Министерством обороны в сфере ИИ. Поэтому, чтобы избежать дублирования в разработке систем, оно намерено сосредоточиться главным образом на решении своих специфических задач, «куда частный сектор инвестирует неохотно». При этом спецслужбы, как и военные, намерены организовать широкую кооперацию и сотрудничать с другими ведомствами, ИТ-компаниями, университетами, федеральными научно-исследовательскими и опытно-конструкторскими центрами МО *(DoD's federally funded research and development centers, FFRDCs)*, национальными лабораториями и международными партнёрами. Они нуждаются во взаимном обмене данными с ИТ-индустрией и привлечении квалифицированных кадров. Однако специфика процедуры госзакупок снижает интерес коммерческих компаний к сотрудничеству с госструктурами. Для исправления этой ситуации разведсообщество намерено изменить, сделать более гибким свой подход к организации государственно-частного партнёрства.

В области международного сотрудничества спецслужбы США отдают приоритет взаимодействию со странами, которые входят в разведывательный альянс «Пять глаз» *(Five Eye)*. Цели американцев в данном случае традиционно прагматичные. Они рассчитывают на: (1) расширение своих возможностей по сбору данных; (2) повышение качества и количества последних; (3) доступ к результатам их обработки союзниками; (4) согласование в рамках альянса подходов к использованию новых технологий и обеспечение совместимости различных ИИ-систем.

Авторы стратегии фактически признают, что, несмотря на развитие в мире отрасли искусственного интеллекта, разведсообщество не готово к внедрению таких технологий и ему требуется проведение серьёзной подготовительной работы.

Тем не менее, в принятой стратегии прямо поставлена задача внедрения ИИ в специальных службах, поэтому с 2019 г. участники разведсообщества начали включать её в свои собственные стратегии. Первыми стали Национальная разведывательная стратегия США 2019 г. *(The National Intelligence Strategy of the United States of America 2019)* [18] и Национальная контрразведывательная стратегия США на 2020–2022 гг. *(National Counterintelligence Strategy of the U.S. 2020-2022)* [19], [20].

ПОЗИЦИЯ КОНГРЕССА США

Американские законодатели полностью поддерживают энтузиазм силовых ведомств относительно использования технологий искусственного интеллекта в

интересах «национальной безопасности США». Это выражается в приоритетном обеспечении законодательной и финансовой поддержки такой деятельности, несмотря ни на какие межпартийные разногласия по иным вопросам.

Так, в соответствии с предписанием закона «Об оборонном бюджете» на 2019 фин. г., для оценки достижений и определения направлений дальнейшего развития государственных работ в области ИИ была создана Комиссия национальной безопасности по искусственному интеллекту под руководством Э. Шмидта. Она начала работу в марте 2019 г., и её задачей является рассмотрение методов и средств, необходимых для развития Соединёнными Штатами таких технологий в интересах национальной безопасности. Оценке подлежал широкий спектр вопросов: конкурентоспособность США в этой области; средства и методы поддержания ими своего технологического преимущества; ситуация в мире с работами и достижениями в сфере ИИ; риски, связанные с их практическим использованием, включая проблемы применения положений международного права и влияние на развитие конфликтов; способы привлечения специалистов; а также этические вопросы [21].

В конце 2019 г. Дональд Трамп подписал закон «Об оборонном бюджете» на 2020 фин. г. *(NDAA-2020)* [17]. В этом документе большое внимание уделено вопросам развития технологий ИИ и машинного обучения в США и мире, а также потенциальным угрозам национальной безопасности.

По мнению Конгресса, технический прогресс (в том числе в области ИИ) будет только усложнять выявление мошеннических аккаунтов и материалов, которые искажают представление о реальных событиях. Серьёзные опасения у законодателей вызывают упомянутые выше дипфейки, сам факт появления которых является прямым результатом использования ИИ. Всё труднее будет выявлять «вредоносное поведение» в социальных сетях. Отмечено существование проблемы защиты самого ИИ от атак, направленных на искажение результатов его работы.

В связи с этим закон «Об оборонном бюджете» 2020 г. содержит ряд предписаний американским силовым структурам по реагированию на эти вызовы.

Задача Национальной разведки в данном контексте заключается главным образом в оценке ситуации в мире и США. Законодателей интересует: анализ потенциального влияние дипфейков на национальную безопасность; обзор существующих и потенциальных методов их использования иностранными государствами; технические возможности последних в этой сфере.

В первую очередь, речь идёт о России и Китае. Директор Национальной разведки должен предоставить: отчёт о потенциале РФ и КНР в области не только создания, но и выявления дипфейков; описание их деятельности по этому направлению; характеристику государственных и сотрудничающих с государством структур обеих стран, которые участвуют в таких работах.

Для оценки собственных возможностей директору Национальной разведки поручено:

- проанализировать основные инициативы спецслужб в области ИИ, их соответствие упомянутой стратегии разведсообщества, степень координации с работами военных и практику использования коммерческих технологий;
- подготовить обзор технологий для атрибуции и противодействия использованию дипфейков, которые могут быть или уже разработаны и развёрнуты в США в интересах государства. Документ должен включать описание деятельности разведсообщества в этой сфере;
- для стимулирования таких исследований и их коммерциализации организовать через Агентство перспективных исследований в сфере разведки соревнования среди разработчиков технологий автоматического распознавания дипфейков.

На фоне упомянутых заявлений о необходимости активизации научно-технической разведки США намерены усилить защиту своих собственных особенно важных *(sensitive)* изысканий в различных областях науки и техники. Это относится к работам вузов, которые получают государственное финансирование (в любых объёмах и на любые цели). Директор Национальной разведки должен подготовить перечень иностранных субъектов, которые в контексте таких исследований представляют шпионскую или иную угрозу национальной безопасности. В список могут попасть государства, корпорации, некоммерческие и коммерческие организации, любые дочерние или аффилированные с ними структуры. Учёту подлежат «любые известные или предполагаемые попытки иностранных субъектов оказать давление на указанные вузы, включая ограничение свободы слова, распространение дезинформации, оказание влияния на профессорско-преподавательский состав, исследователей и студентов». Для противодействия этому спецслужбам поручено организовать сотрудничество с вузами и разработать необходимые правовые или административные меры [17].

По сути, речь идёт о том, что американское государство намерено усилить контрразведывательное обеспечение деятельности своих научных кругов и взять их деятельность под усиленный контроль со стороны специальных служб. Важно отметить, что научное сообщество признаёт существование угрозы, готово к сотрудничеству с разведсообществом и, в свою очередь, ожидает от него рекомендаций по обеспечению безопасности [22].

Наконец, оборонный бюджет на 2021 фин. г. предписывает разведсообществу обеспечить информационное сопровождение ряда задач других ведомств.

Так, получила новую редакцию статья закона «Об обороне» 2019 г. о создании «Инициативы по защите учёных, работающих в интересах национальной безопасности, от неправомерного влияния и других угроз безопасности». Сама инициатива нацелена на защиту как информации о технологиях и разработках, важных для обеспечения национальной безопасности США, так и соответствующих специалистов. Она относится в первую очередь к работам в интересах военных. Поэтому за её реализацию отвечает Министерство обороны вместе с «академическими и иными образовательными и научными организациями». Среди прочего ведомство должно подготовить два списка, в работе над которыми МО будет оказывать содействие Национальная разведка.

Первый будет содержать перечень академических институтов Китая, России и иных стран, если они, по мнению США, отвечают определенным критериям. Во-первых, если они уже были замечены в «неправомерной передаче технологий, краже интеллектуальной собственности, шпионаже (в том числе с использованием киберпространства)» в области достижений науки и техники, или если есть риск таких действий с их стороны. Во-вторых, если подчиняются военным или разведывательным службам. В-третьих, если «уличены в привлечении иностранных граждан к передаче сведений для продвижения работ военных или разведки» либо «в попытках скрыть связь с ними отдельного индивида или организации» [23].

Второй список касается «иностранных программ подготовки кадров *(foreign talent programs)*, которые угрожают интересам национальной безопасности США». В этом контексте разведсообщество прямо не упоминается, однако его представители с большой вероятностью войдут в число «соответствующих государственных ведомств» *(appropriate Government agencies)*, которые должны помочь МО в составлении перечня. В него будут включены программы, которые «угрожают исследованиям, финансируемым Министерством обороны»; «содействуют или вовлечены в кибератаки, кражу, шпионаж, попытки получить права собственности или инструменты влияния на компании, либо вмешиваются в дела США иным образом». Основанием для включения в список могут стать и иные причины на усмотрение министра обороны.

Оба документа будут несекретными, хотя могут иметь секретные приложения. Закон требует от военных предоставлять их оборонным комитетам Конгресса не реже раза в год и публиковать на своём общедоступном интернет-сайте [23]. Всё это говорит о том, что предназначены они не только (а, возможно, и не столько) для защиты американской науки, сколько для использования во внешнеполитических целях, например, как основание для введения очередных санкций.

Закон «Об оборонном бюджете» 2021 г. учреждает также Национальную инициативу в области ИИ *(National Artificial Intelligence Initiative)* для координации всех государственных усилий по этому направлению. Её смысл заключается в обеспечении взаимного информирования гражданских госструктур, МО и разведсообщества о мероприятиях, предпринимаемых участниками таких работ [23].

Инициатива предусматривает создание двух структур. Первая – это Национальный консультативный комитет по ИИ *(National Artificial Intelligence Advisory Committee)*. Он будет консультировать президента США и администрацию Инициативы *(National Artificial Intelligence Initiative)*. За его создание отвечает Министерство торговли [23].

Вторая – это Рабочая группа по обеспечению необходимыми ресурсами национальных исследований в области ИИ *(National AI Research Resource Task Force)*. За неё отвечают Национальный научный фонд и Управление научно-технической политики Белого дома *(Office of Science and Technology Policy)* [23].

В обоих случаях к работе будет привлекаться Национальная разведка.

РЕКОМЕНДАЦИИ КОМИССИИ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ ПО ИСКУССТВЕННОМУ ИНТЕЛЛЕКТУ

В январе 2021 г. Комиссия Национальной безопасности по искусственному интеллекту опубликовала проект своего итогового отчёта, ради которого она и была организована. Документ содержал черновую редакцию основных выводов и рекомендаций о том, как Соединённым Штатам обустроить свою ИИ-отрасль.

В марте 2021 г., как и было предусмотрено законом «Об оборонном бюджете» на 2019 фин. г., была опубликована уже чистовая версия этого отчёта *(Final Report)*. Она дополнена детальным планом мероприятий (включая проекты текстов президентских указов и законов), которые Комиссия рекомендует осуществить для реализации своих рекомендаций. Общий объём отчёта составляет 756 страниц. Для сравнения объём черновика - только 130 страниц.

Комиссия провела действительно титаническую работу по оценке всех сфер создания и применения, как самого ИИ, так и связанных с ним технологий. Один из разделов посвящён использованию ИИ в интересах разведывательного сообщества США.

Согласно тексту отчёта, из всех направлений использования технологий ИИ в области национальной безопасности разведсообщество выиграет от их внедрения больше и быстрее остальных. Ведь основная, по мнению спецслужб и военных, задача ИИ совпадает с задачами разведки и заключается в сборе и обработке данных, объёмы которых из-за распространения информационных технологий уже выросли многократно. И этот рост продолжается. В связи с этим производительности традиционных способов обработки становится недостаточно.

Отчёт рисует прекрасное (для стран-обладателей технологии) будущее ИИ: «Машины будут просеивать массивы данных, собранных из всех источников, находить критическую информацию, выступать в качестве переводчиков, объединять наборы данных из разных областей, выявлять корреляции и связи, перенаправлять ресурсы и информировать аналитиков и лиц, принимающих решения» [24]. Конечно, к этому надо относиться со здоровой долей скепсиса. Однако, с чем современные ИИ действительно справляются хорошо, так это со сбором и обработкой информации.

Комиссия настаивает на необходимости решения государством амбициозной задачи: достичь готовности к внедрению ИИ в разведсообществе к 2025 г. *(AI-Ready by 2025)*. Это означает такое состояние последнего, при котором «личный состав членов разведсообщества имеет необходимую подготовку и обладает базовым уровнем цифровой грамотности, доступом к цифровой инфраструктуре *(IC Information Technology Environment)* и программному обеспечению, которые интегрируют ИИ в рабочий процесс ведомств на всех этапах работы» [24].

В целом основная идея внедрения ИИ в разведсообществе описана в итоговом отчёте Комиссии следующим образом. «После завершения автоматизации рабочего процесса по отдельным видам своей работы, сообществу необходимо объединить их в единый непрерывный цикл анализа разрозненных и разнород-

ных данных, поступающих из всех источников, с помощью единой архитектуры непрерывно обучающихся аналитических механизмов *(continually learning analytic engines)*». Взаимное дополнение способностей человека и машин в этом случае должно позволить извлекать из данных такую информацию, которую человек извлечь не способен. В результате должна значительно повыситься точность прогнозов о грядущих угрозах. Такой комплексный анализ должен стать новым стандартом. «С улучшением качества аналитической работы машин, им следует отдавать всё большую её часть» [24].

Интересно, что в черновике финального отчёта всё это было оформлено в виде цели, которая была сформулирована как «полноценное внедрение ИИ в разведсообществе к 2030 г.» *(The Goal: AI-Enabled Intelligence by 2030)* [25]. Однако, по всей видимости, Комиссия в итоге посчитала, что характер нерешённых технических проблем и ситуация в самих ведомствах делают вероятность достижения этой цели в указанные сроки настолько низкой, что временные рамки были убраны. Тем не менее, Комиссия рекомендует максимально внедрять автоматизацию – от обязательной первичной обработки данных машинными средствами до распространения и обработки информационных материалов разведсообщества без участия человека. Сами материалы обязательно должны иметь две версии: для человека *(human-readable)* и для машин *(machine-readable)*. Это кардинально изменит не только подходы к работе, но и инструментарий разведки – перспективные системы «должны быть оптимизированы для сбора и обработки данных с помощью ИИ». Кроме того, это с большой вероятностью приведёт к переходу разведсообщества на стандартное и унифицированное ПО.

Однако, несмотря на технические проблемы, двумя главными препятствиями остаются бюрократические препоны и дефицит кадров, которые усугубляют друг друга.

Итоговый отчёт говорит, что, несмотря на проведённую разведсообществом работу, «всё ещё много серьёзных препятствий на уровне властей/регулирующих органов, политики, бюджетов, обмена данными и технических стандартов». В первом промежуточном отчёте, опубликованном в конце 2019 г., оценка была гораздо жёстче. Тогда члены Комиссии отмечали, что и военные, и специальные службы на словах признают важность ИИ для своей работы, но на практике мало что делают для их внедрения [22].

Для исправления ситуации Комиссия рекомендует провести ряд организационных изменений и назначений, поскольку «инновации в области национальной безопасности требуют сильного лидерства, если нет стимулов вроде полномасштабной войны или террористической атаки» [24].

Во-первых, офис директора Национальной разведки должен создать Совет по управлению ключевыми рисками в области ИТ-модернизации *(IT modernization Senior Risk Management Council)* спецслужб.

Во-вторых, директор по науке и технологиям *(Director of Science and Technology) ODNI* должен быть параллельно назначен на должность главного технического

директора всего разведсообщества *(IC's Chief Technology Officer, CTO)*. Он будет отвечать за координацию всех вопросов, связанных с технологиями.

Комиссия очередной раз указывает на необходимость координации работ с военными, чтобы избежать дублирования, обеспечить совместимость систем, организовать быстрый и безопасный способ обмена данными.

Страх понести наказание за последствия ошибок работы ИИ представляет собой главное (после бюрократических препон) препятствие для внедрения таких технологий. Никто не хочет брать на себя ответственность за такие ошибки, вероятность, область появления, характер и опасность которых достоверно неизвестна. Более того, неизвестно даже, возможно ли снизить степень этой неизвестности. Поэтому Комиссия в свойственных отчёту выражениях аккуратно говорит о нахождении баланса между уровнем риска ненормальной работы новых технологий и риском отставания от противника из-за опоздания в их внедрении. По сути же рекомендуется снизить требования к безопасности и надёжности работы таких систем, чтобы максимально быстро принять их на вооружение.

Комиссия подтверждает необходимость активизировать «сбор данных по линии научно-технической разведки *(S&TI)* для правильной оценки потенциала противника». Однако тут возникает проблема недостаточного общего уровня подготовки личного состава для анализа таких данных. Для исправления ситуации и курирования этого направления директору Национальной разведки рекомендуется назначить ответственного за сбор разведданных по новым технологиям *(Emerging Technology Collection Executive)* в составе Национального совета по разведке *(National Intelligence Council)*. Решить проблему дефицита кадров гораздо сложнее, чем преодолеть бюрократию. Причина, во-первых, в очень длительном сроке подготовки технических специалистов и низком качестве образования в области точных наук *(science, technology, engineering, and mathematics, STEM)* в США, о чём Комиссия также постоянно говорит.

Во-вторых, ИТ-специалисты не очень охотно идут работать в госструктуры.

Прежде в качестве основной причины рассматривалось то, что на госслужбе оплата ниже, чем в ИТ-компаниях. Чтобы скомпенсировать это, в упомянутом первом промежуточном отчёте Комиссия рекомендовала пропагандировать важность госслужбы и упирать на гражданскую сознательность потенциальных сотрудников, показывая «притягательные способы внести свой вклад в общество, решая исключительно сложные и важные проблемы» [22]. Однако итоговый отчёт говорит, что главная причина не в этом. На госслужбе такие специалисты сталкиваются с бюрократией и, как следствие, с ситуацией, когда доступный им инструментарий успевает устареть, прежде чем они получат право использовать его для работы. К этому добавляется то, что, по мнению главного советника АНБ, «миллениалы верят, что технологии в частном секторе теперь позволяют им помочь изменить мир», хотя прежде такое желание могла удовлетворить в первую очередь госслужба [22].

При желании поступить на госслужбу специалисты сталкиваются с тем, что кадровики «играют чрезмерную роль в процессе оценки соответствия кандида-

тов требованиям и часто страдают формализмом – полагаются на неточные описания должностей, а не на понимание технических требований к должности» [22]. Сами ведомства не используют свои полномочия на применение специальных механизмов найма (включая, например, право найма специалистов без конкурса или организации стажировок и стипендиальных программ).

Комиссия отмечает, что технические специалисты в области ИИ будут составлять меньшую часть общего персонала разведсообщества. Однако оставшаяся большая часть всё равно должна понимать основы политики, функциональности и применения ИИ, чтобы эффективно использовать возможности технологий. И обязательно нужны руководители всех уровней, которые понимают особенности использования, ограничения и сильные стороны ИИ [22]. Кроме того, для понимания потенциала личного состава (включая резервистов) службам рекомендуется провести его оценку и создать систему поощрения за обладание навыками в области ИТ и ИИ [22].

На этом фоне лидерами в области ИИ-технологий были и остаются частные компании. Они развиваются быстрее госсектора из-за отсутствия столь жёстких требований по безопасности и надёжности систем. В силу лучшей оплаты труда и технической оснащённости являются более привлекательным местом работы для специалистов. Кроме того, в случае утечек данных или каких-либо иных проблем, государственные структуры всегда могут откреститься от них (по аналогии с потерями личного состава частных военных компаний), указав, что вся вина лежит на подрядчике, который не организовал работу должным образом. Возможно, последнее обстоятельство даже является одним из ключевых препятствий для внедрения ИИ в госструктурах. Руководство последних и так всё устраивает, и у него не возникает желания проявить политическую волю для реального преодоления остальных проблем. В связи с этим разведсообщество всегда будет заинтересовано в привлечении коммерческих компаний для выполнения своих задач. Подрядчики, в свою очередь, не останутся без персонала и работы. Тем более, что ИИ-системы для разведки по открытым источникам информации позволяют коммерческим компаниям добиваться настолько серьёзных результатов, что Комиссия настоятельно рекомендует спецслужбам максимально интегрировать эти методы в существующие процессы работы.

ЗАКЛЮЧЕНИЕ

Разведсообщество вместе с вооружёнными силами являются главными государственными потребителями технологий в области искусственного интеллекта в США. Сейчас они сталкиваются с серьёзными проблемами внедрения таких систем из-за недостатка специалистов, отсутствия подходящей технической инфраструктуры и организационных вопросов, включая большую инертность бюрократической системы, сопротивляющейся любым инновациям.

Тем не менее, руководством США поставлена задача внедрить ИИ в специальных службах. Конгресс, несмотря на межпартийные противоречия, также не ста-

вит под сомнение важность её решения. Для выявления проблем, "перспектив и путей развития отрасли была создана Комиссия национальной безопасности по искусственному интеллекту, в составе которой практически нет случайных людей. Подавляющее большинство её членов – это ведущие специалисты по ИИ крупнейших ИТ-компаний США. Возглавляет её Эрик Шмидт, человек, под чьим руководством «Гугл» стала той корпорацией, которую мы знаем сегодня, и тот, кто одним из первых забил тревогу по поводу развития ИИ в мире и опасности для США упустить лидерство в этой сфере. Должность его заместителя занимает Роберт Уорк, который в бытность заместителем министра обороны США дал старт первой пилотной программе использования ИИ в вооружённых силах.

Комиссия развернула активную работу и по итогам своей деятельности не просто написала отчёт с общими словами, а подготовила большое число детально разработанных мер и законопроектов. В этом видна явная заинтересованность участников в реальном достижении результата – широком внедрении ИИ на практике, в том числе в разведсообществе, несмотря ни на какое сопротивление системы. Комиссия подчеркивает, что «ИИ – это квинтэссенция технологий двойного назначения» [24] и опоздание в его внедрении крайне опасно.

Однако в отчёте прослеживается и стремление пролоббировать интересы ИТ-индустрии. Документ даёт описание максимально успешного варианта развития технологий, которые вряд ли могут оставить равнодушным высокое начальство. В то же время, признавая серьёзные технические и этические проблемы внедрения и использования ИИ, Комиссия, по сути, рекомендует любой ценой снизить требования по безопасности к таким системам. Причём при отсутствии конструктивных аргументов, она использует универсальный довод – интересы национальной безопасности США.

Сегодня в области ИИ происходит обратная конверсия: технологии, доведённые коммерческими компаниями до готовности к практическому использованию, ставятся на военно-разведывательные рельсы.

Интересно, что речь идёт о технологиях, обоснованные предостережения о возможных путях использования которых прежде вызывали обвинения в конспирологии. Например, в ответ на вопросы относительно потенциальных технических возможностей и реальных целей ИТ-корпораций говорилось, что «им не интересна политика». Защитники утверждали, что цель ИТ-бизнеса – всего лишь максимально эффективно продать вам то, что вам и так нужно.

Теперь же мир увидел, как ИТ-гиганты прямо и открыто вмешиваются в политику, не только отключая аккаунт в соцсетях президенту Трампу, но и наполняя своими людьми переходную команду Байдена [26].

О возможностях технологий (наиболее современными из которых обладают как раз американские ИТ-компании), написала в своём отчёте сама Комиссия: «рекламные технологии *(AdTech)* стали технологиями национальной безопасности *(NatSecTech)*» [24]. Речь идёт об ИИ, который представляет собой «мощный инструмент таргетирования». Прежде оно «влияло на отношения бизнеса и покупателей, теперь – на отношения между правительствами и отдельными людьми».

В связи с этим Комиссия выражает опасение, что «систематический сбор данных о компаниях, гражданах и государственных структурах США – это больше чем традиционный шпионаж». «ИИ усложняет сокрытие информации о личном финансовом положении, распорядке дня, привычках, отношениях, здоровье и даже эмоциях, если не предпринимать адекватных мер по защите информации». И новая проблема заключается в том, что «уязвимости отдельных граждан и частных компаний становятся слабостями национальной безопасности, поскольку противник может: получить характеристику людей, сетей и социальных напряжений или раскола; предсказывать их ответные реакции на различные внешние воздействия; и, в итоге, проводить моделирование вариантов наиболее выгодного ему манипулирования поведением или нанесения ущерба. Развитие и распространение этих методов является главной проблемой для контрразведки».

Интересно, что об этом же ещё в 2017 г. рассказал эксперт в области ИТ Евгений Черешнев [27]. Тогда многие восприняли его выступление как алармизм. Сегодня об этом прямо пишут ведущие специалисты – действующие и бывшие сотрудники «Гугл», «Амазон», «Оракл», «Ин-кью-тел», Минобороны США под руководством бывшего главы «Гугл» и бывшего замминистра обороны, открывшего дорогу искусственному интеллекту в американские вооружённые силы, – которые и составляют Комиссию национальной безопасности по ИИ.

ИСТОЧНИКИ

1. Разведопрос: Герман Клименко, советник президента РФ // Канал Дмитрия Пучкова на Youtube. 2016. 30 августа. Available at: https://www.youtube.com/watch?v=KjQk2_iGdMo (accessed 08.04.2021).

2. Extradition To and From the United States: Overview of the Law and Contemporary Treaties // Congressional Research Service. 2016. 4 October. Available at: https://crsreports.congress.gov/product/pdf/RL/98-958#page=39&zoom=auto,-457,786 (accessed 23.03.2021).

3. Предупреждение для граждан России, выезжающих за границу, в связи с угрозой со стороны США (1311-28-08-2020) // Официальный сайт МИД РФ. 2020. 8 августа. Available at: https://www.mid.ru/web/guest/maps/us/-/asset_publisher/unVXBbj4Z6e8/content/id/4303492 (accessed 23.03.2021).

4. Tucker P. Russian Arms Production Slowed by Coronavirus, Analysts Find // Defense One. 2020. May 1. Available at: https://www.defenseone.com/technology/2020/05/russian-arms-production-slowed-coronavirus-analysts-find/165071/ (accessed 03.05.2020).

5. 10 U.S. Code § 467 – Definitions // Legal Information Institute of Cornell Law School. Available at: https://www.law.cornell.edu/uscode/text/10/467 (accessed 09.04.2021).

6. WSJ: исследователи из США следили за военными объектами в России с помощью мобильников // ИноТВ. 2020. 19 июля. Available at: https://russian.rt.com/inotv/2020-07-19/WSJ-issledovateli-iz-SSHA-sledili (accessed 22.12.2020).

7. Machine Learning // The Next Wave. Vol. 22. No. 1. 2018. Available at: https://www.nsa.gov/Portals/70/documents/resources/everyone/digital-media-center/publications/the-next-wave/TNW-22-1.pdf (accessed 12.04.2019).

8. Machine Learning // The Next Wave. Vol. 22. No. 2. 2019. Available at: https://www.nsa.gov/Portals/70/documents/resources/everyone/digital-media-center/publications/the-next-wave/TNW_22-2.pdf (accessed 12.04.2019).

9. The AIM Initiative. A strategy for augmenting intelligence using machines // Office of the Director of National Intelligence. 2019. 16 January. Available at: https://www.dni.gov/files/ODNI/documents/AIM-Strategy.pdf (accessed 25.01.2020).

10. Maintaining American Leadership in Artificial Intelligence: Executive Order 13859 of February 11, 2019 // Federal Register. Available at: https://www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence (accessed 06.02.2020).

11. Summary of the 2018 Department of Defense Artificial Intelligence Strategy // U.S. Department of Defense. 2019. 12 February. Available at: https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF (accessed 25.01.2020).

12. H.R.1540 – National Defense Authorization Act for Fiscal Year 2012. SEC. 4601 // The official website for U.S. federal legislative information Congress.gov. Available at: https://www.congress.gov/bill/112th-congress/house-bill/1540/text (accessed 11.02.2019).

13. H.R.4310 – National Defense Authorization Act for Fiscal Year 2013. SEC. 4601 // The official website for U.S. federal legislative information Congress.gov. Available at: https://www.congress.gov/bill/112th-congress/house-bill/4310/text (accessed 11.02.2019).

14. H.R.3304 – National Defense Authorization Act for Fiscal Year 2014. SEC. 4601 // The official website for U.S. federal legislative information Congress.gov. Available at: https://www.congress.gov/bill/113th-congress/house-bill/3304/text (accessed 11.02.2019).

15. S.1356 – National Defense Authorization Act for Fiscal Year 2016. SEC. 2404 // The official website for U.S. federal legislative information Congress.gov. Available at: https://www.congress.gov/bill/114th-congress/senate-bill/1356/text (accessed 11.02.2019).

16. In-Q-Tel: A New Partnership Between the CIA and the Private Sector // Central Intelligence Agency. Available at: https://www.cia.gov/library/publications/intelligence-history/in-q-tel (accessed 23.05.2020).

17. S.1790 – National Defense Authorization Act for Fiscal Year 2020 // Congress.gov. The official website for U.S. Federal Legislative Information. Available at: https://www.congress.gov/bill/116th-congress/senate-bill/1790/text (accessed 25.01.2020).

18. National Intelligence Strategy of the United States of America // Office of the Director of National Intelligence. 2019. 22 January 2019. Available at: https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf (accessed 25.03.2020).

19. National Counterintelligence Strategy of the United States of America2020-2022 // Office of the Director of National Intelligence. 2020. 13 February. Available at:

https://www.dni.gov/files/NCSC/documents/features/20200205-National_CI_Strategy_2020_2022.pdf (accessed 19.02.2020).

20. NCSC Unveils the National Counterintelligence Strategy of the U.S. 2020-2022 // Office of the Director of National Intelligence. 2020. 13 February. Available at: https://www.dni.gov/files/NCSC/documents/features/20200207-National_CI_Strategy_Press_Release.pdf (accessed 19.02.2020).

21. H.R.5515 – John S. McCain National Defense Authorization Act for Fiscal Year 2019. Sec. 1051 // Congress.gov. The official website for U.S. Federal Legislative Information. Available at: https://www.congress.gov/bill/115th-congress/house-bill/5515/text (accessed 09.04.2021).

22. Interim Report // National Security Commission on Artificial Intelligence. 2019. November. Available at: https://drive.google.com/file/d/153OrxnuGEjsUvlxWsFYauslwNeCEkvUb/view (accessed 28.01.2020).

23. H.R.6395 - National Defense Authorization Act for Fiscal Year 2021. SEC. 1299C // Congress.gov. The official website for U.S. Federal Legislative Information. Available at: https://www.congress.gov/bill/116th-congress/house-bill/6395/text/ (accessed 08.04.2021).

24. Final Report // National Security Commission on Artificial Intelligence. 2021. March. Available at: https://reports.nscai.gov/final-report/table-of-contents/ (accessed 28.01.2020).

25. Draft Final Report, P. 57 // National Security Commission on Artificial Intelligence. 2021. 19 January. Available at: https://drive.google.com/file/d/1XT1-vygq8TNwP3I-ljMkP9_MqYh-ycAk/view (accessed 22.03.2021).

26. Селянин Я.В. Facebook и Twitter удаляют Трампа: о чём стоит задуматься демократам // Сайт ИМЭМО РАН. 2021. 22 января. Available at: https://www.imemo.ru/news/events/text/facebook-i-twitter-udalyayut-trampa-o-chiom-stoit-zadumatysya-demokratam (accessed 07.04.2021).

27. Евгений Черешнев, «человек-киборг», о влиянии технологий на жизнь обычного человека (2017г.) // Канал Форума «Следующие 20 лет» на Youtube. 2020. 13 апреля. Available at: https://www.youtube.com/watch?v=J4OMoCvMeFI (accessed 07.04.2021).

СПИСОК ЛИТЕРАТУРЫ

Селянин Я.В. 2019a. Военно-промышленная политика США в области высокопроизводительных вычислений: цели, задачи, перспективы. *Проблемы национальной стратегии*. № 3 (54). С. 179–201. Available at: https://riss.ru/documents/800/732c9e54a1754d019edad10b66ecdfe3.pdf (accessed 23.05.2020).

Селянин Я.В. 2019b. Технологическое лидерство, роль государства и неоднозначность цифр в высокотехнологичных областях на примере военно-промышленной политики США в области высокопроизводительных вычислений. *Проблемы национальной стратегии*. № 5 (56). С. 137–166. Available at: https://riss.ru/documents/827/1d677d3157534c1b81af606950fc5d91.pdf (accessed 23.05.2020).

Селянин Я.В. 2020a. Государственная политика США в области искусственного интеллекта: цели, задачи, перспективы реализации. *Проблемы национальной стратегии*. № 4 (61). С. 140–163. Available at: https://riss.ru/documents/1591/07.pdf (accessed 07.09.2020).

Селянин Я.В. 2020b. Политика США по использованию искусственного интеллекта в интересах военных. *Россия и Америка в XXI веке*. Выпуск №4. Available at: https://rusus.jes.su/s207054760013351-3-1/ (accessed 01.04.2021). DOI: 10.18254/S207054760013351-3

REFERENCES

Kegelmeyer W.P. 2019. Adversarial issues in machine learning. *The Next Wave.* Vol. 22. No. 2. P. 10-14. Available at: https://www.nsa.gov/Portals/70/documents/resources/everyone/digital-media-center/publications/the-next-wave/TNW_22-2.pdf (accessed 12.04.2019).

Selyanin Y.V. 2019a. Voenno-promyshlennaia politika SShA v oblasti vysokoproizvoditel'nykh vychislenii: tseli, zadachi, perspektivy [The U.S. Military-Industry Policy in the Area of High-Performance Computing: Aims, Objectives, Prospects] (In Russ.). *National Strategy Issues.* No. 3. P. 179–201. Available at: https://riss.ru/documents/800/732c9e54a1754d019edad10b66ecdfe3.pdf (accessed 23.05.2020).

Selyanin Y.V. 2019b. Tekhnologicheskoe liderstvo, rol' gosudarstva i neodnoznachnost' tsifr v vysokotekhnologichnykh oblastiakh na primere voenno-promyshlennoi politiki SShA v oblasti vysokoproizvoditel'nykh vychislenii [Technological Leadership, State Participation, and Ambiguity of Numbers in the Area of High Technologies: the Case of the U.S. Military-Industry Policy in the Area of High Performance Computing] (In Russ.). *National Strategy Issues.* No. 5. P. 137–166. Available at: https://riss.ru/documents/827/1d677d3157534c1b81af606950fc5d91.pdf (accessed 23.05.2020).

Selyanin Y.V. 2020a. Gosudarstvennaia politika SShA v oblasti iskusstvennogo intellekta: tseli, zadachi, perspektivy realizatsii [The U.S. National Policy in the Area of Artificial Intelligence: Aims, Objectives and Prospects for Realization] (In Russ.). *National Strategy Issues.* No. 4. P. 140–163. Available at: https://riss.ru/documents/1591/07.pdf (accessed 07.09.2020).

Selyanin Y.V. 2020b. Politika SShA po ispol'zovaniiu iskusstvennogo intellekta v interesakh voennykh [U.S. Policy of the Artificial Intelligence Using in the Interests of the Military]. (In Russ.) *Russia and America in the 21th Century.* No. 4. Available at: https://rusus.jes.su/s207054760013351-3-1/?sl=en (accessed 01.04.2021). DOI: 10.18254/S207054760013351-3

Whyte C. 2020. Problems of Poison: New Paradigms and "Agreed" Competition in the Era of AI-Enabled Cyber Operations // *20/20 Vision: The Next Decade* / The NATO Cooperative Cyber Defence Centre of Excellence. 2020. P. 2015-232. Available at: https://ccdcoe.org/uploads/2020/05/CyCon_2020_book.pdf (accessed 23.05.2020).

ИНФОРМАЦИЯ ОБ АВТОРЕ / INFORMATION ABOUT THE AUTHOR

СЕЛЯНИН Ярослав Владиславович, научный сотрудник Центра североамериканских исследований Института мировой экономики и международных отношений РАН.

Российская Федерация, Москва, 117997, Профсоюзная ул., 23.

Yaroslav V. SELYANIN, Research Fellow, Center for North American Studies, Institute of World Economy and International Relations, Russian Academy of Sciences.

23, Profsoyuznaya Str., Moscow, Russian Federation, 117997

Поступила в редакцию / Received 31.03.2021
Поступила после рецензирования / Revised 15.04.2021
Принята к публикации / Accepted 22.04.2021