DOI 10.37539/2949-1991.2026.36.1.025
УДК 004.8

**Марцинкевич Вячеслав Юрьевич,**
президент клуба,
Спортивно-патриотический клуб "Дмитрий Донской"

**Махмудов Закир Махмудович,**
Аспирант, СибАДИ

**Соловьев Анатолий Алексеевич,**
профессор, СибАДИ

**Угрюмов Сергей Витальевич,**
канд. эконом. наук, профессор,
Институт новых химических технологий

# ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ ДЛЯ РАЗВЕДЫВАТЕЛЬНЫХ СЛУЖБ

**Аннотация.** В статье анализируется тенденции финансирования и развития искусственного интеллекта в военной и разведывательной сферах, с акцентом на опыт технологически развитых государств. Рассматриваются ключевые направления применения искусственного интеллекта, включая анализ больших массивов данных, кибербезопасность, автономные системы и обработку информации из открытых источников.

**Ключевые слова:** Искусственный интеллект, военные технологии, информационная безопасность, цифровизация оборонной сферы, анализ больших данных, автономные системы в военной сфере.

Доля финансирования исследований в области математических и компьютерных наук для нужд в Министерства обороны США значительно расширяются.

Информационно-коммуникационным технологиям, отведена четверть финансирования прикладных исследований и финансирование этой сферы будет непрерывно возрастать по таким направлениям как кибербезопасность, искусственный интеллект и человеко-машинный симбиоз, в рамках которых разрабатываются технологии искусственного интеллекта, позволяющие машинам функционировать в качестве надежных партнеров для операторов-людей. ИИ сможет понимать человеческий язык, собирать и классифицировать информацию, а также разумно (критично) реагировать на новые и непредвиденные события.

Разрабатываемые технологии позволят: военнослужащим принимать более эффективные решения в сложных условиях боя; аналитикам разведывательных служб разбираться в массивной, неполной и противоречивой информации; беспилотным и полуавтономным системам безопасно и надежно выполнять критически важные миссии. К настоящему времени предусмотрено изучение потенциала языковой обработки ИИ для обеспечения абстрактных рассуждений, начало разработки методов, обеспечивающих прозрачную и логичную коммуникацию между людьми и моделями искусственного интеллекта. Летом этого года Пентагон заплатит Google, OpenAI, Anthropic и xAI по 200 млн долларов за внедрение ИИ в военной сфере.

Новые, прорывные технологии дают стратегическое преимущество над соперниками. Очередные ожидания такого рода связывают с искусственным интеллектом *(ИИ, Artificial*

*Intelligence, AI)*. В быту ИИ широко применяется последние несколько лет, а в военной и тем более в разведывательной сферах подобные наработки появились и используются достаточно давно.

Действительно, первые попытки создания и применения ИИ в разведке отмечены в конце 1970-х, когда в США появилась частная компания IRIS *(International Reporting Information Systems)*, которая позиционировала себя ни много ни мало как информационный центр ЦРУ. Ее основатели заявляли, что их аналитическая система способна ежедневно обрабатывать порядка 15 тыс. политических экономических событий в различных уголках мира, причем делать это сразу на восьми языках, но это оказалось, как бы, сейчас сказали, фейком, инвестиционным пузырем. Действительно, первые попытки создания и применения ИИ в разведке отмечены в конце 1970-х, когда в США появилась с военнослужащими-мужчинами, чат-бот находит тех, кто нарушает инструкцию, согласно которой военные обязаны блокировать все сообщения с неизвестных номеров.

Более серьезно американцы подошли к этому вопросу в 2000-х годах после терактов 11 сентября. Тогда Агентством перспективных оборонных исследований (DARPA) был запущен проект TIA *(Terrorism Information Awareness)*, нацеленный на поиск потенциальных террористов путем анализа больших объемов на связанной между собой информации из открытых источников. TIA стал фундаментом для многих последующих разработок в этой сфере. С 2021 года он переведен на платформу ИИ, и доступ к его мощностям, помимо Пентагона, получили американские разведывательные ведомства. В 1980-е в стенах Первого главного управления (внешняя разведка) КГБ СССР родилась аналитическая система «Сплав». Ее создатели обучили машину выявлять в информационных потоках признаки разведывательной деятельности. В начале 2000-х в разведывательном секторе России появилась система «Тренд», принцип действия которой состоял в сравнении текущих событий с эталонными значениями. Эти разработки дали старт новой эпохе использования компьютерных технологий в работе с большими объемами данных в разведывательной сфере.

Произвел ли ИИ революцию в разведке, прежде всего в области анализа и обработки информации? Эффективен ли при выполнении рутинных и трудоемких задач, которые вызывают у людей скуку и нередко приводят к ошибкам? Ответ не столь однозначен. Не секрет, что в наши дни почти каждое государство имеет в арсенале армии и спецслужб набор инструментов на основе ИИ. Известно, например, что израильские военные разработали алгоритмы, которые успешно применяются для выявления целей для авиаударов. Они анализируют данные из всех доступных источников, включая спутниковые снимки, кадры с дронов, фотографии и переписку в мессенджерах, и выдают целеуказание. Как заявляют в ЦАХАЛ, часть атак уже наносится в автоматическом режиме без человеческого контроля.

Индийские разработчики сообщали о программе AI-Honey, которая помогает выявлять в армии неблагонадежные элементы. Общаясь под видом девушки в мессенджере WhatsApp. Собственные наработки и решения в сфере ИИ есть в Южной Корее, Японии, у ряда европейских государств, Китае и России.

Значительней многих в этом вопросе продвинулись США. В 2023 году частная разведывательная компания Palantir Technologies представила для американской военной разведки новейшую платформу AIP (Artificial Intelligence Platform), которая способна собирать разведданные и в режиме реального времени следить за ситуацией на поле боя через соцсети, используя метод геолокации. В том же году эта технология уже была применена на СВО против российской армии.

А ЦРУ сообщало, что его аналитики намерены использовать популярную во всем мире программу ChatGPT для сбора и анализа данных из открытых источников. На сегодняшний день стоят задачи усиления направления OSINT (Open Source Intelligence), учитывая, что

объем доступной в Сети информации год от года увеличивается буквально в геометрической прогрессии, а также широкого внедрения ИИ в работу разведки. Реализация этих задач возложена на Open Source Enterprise (OSE), входящую в состав Управления цифровых инноваций ЦРУ. Таким образом, во всех технологически развитых странах сложилось устойчивое представление о том, что за ИИ будущее. Учитывая, что уже сейчас машина может видеть, слышать и понимать человека, отвечать ему на нескольких языках в режиме реального времени, в разведывательном сообществе ожидают, что скоро у оперативников и аналитиков появятся умные роботы-ассистенты, которые объединят в себе энциклопедии и поисковые системы. Они будут помогать составлять отчеты о деловых поездках, вносить правки в служебные документы, отслеживать новостные ленты, напоминать о встречах и корректировать их расписание и подобные перспективы кажутся вполне реальными. Вместе с тем важно понимать, что в столь чувствительной сфере, как разведка, ИИ может выполнять только такие, сугубо вспомогательные функции. Облегчить аналитику сбор первичной информации – безусловно, но принимать за него решение – крайне сомнительно.

Практически любой вопрос, который является предметом разведывательного анализа, характеризуется неполнотой данных. Из-за этой неопределенности аналитики вынуждены оперировать не только фактами, но и пытаться понять, что находится в «серых зонах» – между правдой и вымыслом. В таких ситуациях генеративные ИИ неприменимы, поскольку они не умеют отделять истину от лжи. И хотя они могут служить мощным инструментом выявления корреляции и скрытых связей между отдельными событиями и даже способны генерировать новые идеи, в разведанализе их использование должно быть ограничено.

Представьте, будто вы собираете мозаику, но кто-то незаметно для вас время от времени убирает со стола ее элементы, а иногда подменяет частями из другого набора, из-за чего вам никак не удается сложить картину целиком.

Примерно так можно описать работу аналитика с разведданными. Никакими техническими средствами ее не сделать. Любые алгоритмы будут неизбежно давать сбой ввиду бесконечно возникающих новых вводных. Но это полбеды. Уже сейчас информационные потоки переполнены контентом, созданным самим ИИ, что сильно искажает реальную картину. В будущем эта проблема только усугубится: обмануть станет проще, а аналитикам все сложнее будет дать точную оценку возможностей и намерений противника.

На данный момент никто не может до конца быть уверенным в том, какое будущее ждет технологии ИИ и как они повлияют на наш мир. Даже программисты и инженеры не знают всех потенциальных ограничений и скрытых недостатков того, что они создают. Очевидно, что ИИ таит в себе и новые возможности, и серьезные риски. Для разведки и других структур, отвечающих за государственную безопасность, крайне важно не спешить с делегированием полномочий машине. Отдавать на откуп бездушному железу решения, от которых зависят судьбы живых людей, а порой и целых народов, не просто опасно, но и преступно.

*Список литературы:*

1. Кобзарь Е.П., Соловьев А.А., Стругов Ю.Ф. Математическое обоснование большой войны. Вестник Сибирского Отделения Академии Военных Наук. 2022. № 65. С. 68-73.

2. Настоящее и будущее применения ChatGPT / Д. В. Балагин, С. А. Зырянова, А. А. Соловьев, О. А. Филимонова. – Текст : непосредственный // Вестник Сибирского отделения Академии военных наук. – 2024. – № 72 : С. 120-129.

3. О пресыщении интернетом и информационные пустоты = About Internet saturation and information voids / Н. Я. Гарафутдинова, А. А. Соловьев, Л. А. Поступинских, Т. А. Юрина. – Текст : непосредственный // Вестник Сибирского отделения Академии военных наук. – 2024. – № 72 : С. 213-217

4. Корабельников А.А., Поступинских Л.А., Соловьев А.А. Искусственный интелект в системах управления войсками и оружием. В сборнике: Цифровизация и кибербезопасность: современная теория и практика. Сборник научных трудов по материалам II Международной научно-практической конференции. Отв. редактор З.В. Семенова. Омск, 2022. С. 74-77.

5. Аппельганц А.В., Пятакова О.И., Соловьев А.А. Групповое управление роботами военного назначения. В сборнике: Повышение качества образования, современные инновации в науке и производстве. Сборник трудов Международной научно-практической конференции. 2019. С. 562-568.