ISSN 2658-5014 (Print) СИИТ ISSN 2686-7044 (Online)
http://siit.ugatu.su 2026. Т. 8, № 2(26)
СИСТЕМНАЯ ИНЖЕНЕРИЯ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ
Научная статья

УДК 004.8 DOI: 10.54708/SIIT-2026-no2-p144 EDN: HNJSBF

Интеллектуальные методы конкурентной разведки в обеспечении национальной безопасности

Л. Н. Родионова

Уфимский университет науки и технологий

Современные методы конкурентной разведки являются симбиозом методов военной разведки, расширением и диверсификацией методического обеспечения исследования рынка и конкурентов в маркетинге, дополненные самыми современными исследованиями в области информационных технологий. Управление корпорациями, предприятиями, что означает в совокупности и оптимизацию финансовых потоков, и решение задач управления персоналом, и формирование запасов ресурсов – становится сложной задачей, когда конкуренция вышла за рамки отдельных государств и стала глобальной. Но основная проблема современного управления компаниями заключается не в поиске достоверных данных о рынке, конкурентах и потребителях, а в донесении любых входящих данных, связанных с компанией и рынком, до руководителя, который и производил фильтрацию и обработку данных. Сейчас ситуация резко изменилась. В статье рассмотрены методы конкурентной разведки, которые можно использовать совместно с разработанными нейронными сетями, методами искусственного интеллекта (ИИ) в целях обеспечения национальной безопасности государства для совершенствования сложной технической продукции, в том числе оборонного комплекса. Проведен анализ возможности использования различных нейронных сетей для задач технической разведки и представлены рекомендации по их применению.

Конкурентная разведка; национальная безопасность; технологический суверенитет; искусственный интеллект.

Введение

Из всех функций управления менеджеры высшего эшелона оставляют себе только две стратегические функции: постановку цели и контроль, то есть задачу стратегического прогнозирования и управления, что, в свою очередь, требует не только и не столько поиска информации, которая формирует знания о настоящей ситуации, а поиска так называемой прогностической информации, которая определяет вероятность реализации и успеха предлагаемых сценариев, а также оценку тенденций изменений ситуации на рынке. Это определяет актуальность использования методов конкурентной разведки в современном мире. В статье используются основные подходы и методы, представленные в составленном автором учебном пособии [Род24]. Многочисленные исследования зарубежных ученых в области конкурентной разведки (в основном бывших сотрудников Центрального разведывательного управления США (ЦРУ) и Федерального бюро расследований (ФБР) в Российской Федерации были дополнены легальными методами и нашли отражение в трудах ученых и специалистов-практиков: Е. Ющука, А. Кузина [Ющу07, Ющу08, Куз09], Н. Баяндина [Бая02], Ю. Воронова [Вор07], Б. Джилада [Джи10], А. Доронина [Дор07], Ю. Каторина [Кат00], И. Нежданова [Куз09],

Рекомендовано к публикации программным комитетом XI Международной научной конференции ITIDS’2025 «Информационные технологии интеллектуальной поддержки принятия решений», Уфа, 13–15 ноября 2025 г.

Родионова Л. Н. Интеллектуальные методы конкурентной разведки в обеспечении национальной безопасности // СИИТ. 2026. Т. 8, № 2(26). С. 144-153. DOI: 10.54708/SIIT-2026-no2-p144. EDN: HNJSBF.

Rodionova L. N. “Intellectual methods of competitive intelligence in ensuring national security” // SIIT. 2026. Vol. 8, no. 2(26), pp. 144-153. DOI: 10.54708/SIIT-2026-no2-p144. EDN: HNJSBF. (In Russian).

Г. Лемке [Лем07], Г. Мелтона [Мел09], Е. и В. Рудометовых [Руд10], С. Шушкевича [Шуш05] и др.

Внедрение в науку и практику рыночного хозяйствования методов искусственного интеллекта (ИИ) актуализируют известные методы конкурентной разведки, что позволяет не только получать более достоверные данные, но и совершенствовать полученные результаты с помощью ИИ.

Предпосылка № 1. В одном из своих выступлений на конференции А. И. Масалович – один из самых известных профессионалов и методологов конкурентной разведки [Мас22] – процитировал проф. А. П. Ершова, который еще в 1987 году на научном форуме в Академгородке г. Новосибирска, посвященном технологическому суверенитету, указал, что отставание по отдельным элементам складывается в вектор, тот в свою очередь – дает направление; и это «…направление показывает, что мы идем не туда».

Предпосылка № 2. В середине июня 2025 года состоялось очередное заседание Бильдербергского клуба (англ. *Bilderberg Club)* – ежегодного закрытого форума, созданного в 1954 году. Достоверных сведений о заседании нет, но то, что просочилось усилиями журналистов по итогам редких интервью в прессу, заставляет задуматься. На этом заседании кроме международных банкиров около трети присутствующих составляли технические директора по ИИ корпораций, которые выполняют оборонные заказы, как например, Palantir, Microsoft IAM и пр., а также военные самого высокого ранга.

Все выступающие благодарили Украину за то, что предоставила идеальный полигон для испытаний технологий будущей войны. Говорили, что эти технологии нужно усовершенствовать и поставить на боевое дежурство. На это все отводится 24–36 месяцев. Самые богатые люди планеты брали на себя обязательства инвестировать $ 2,3–2,5 млрд в неделю (!) на создание «Цифрового НАТО» (рис. 1).

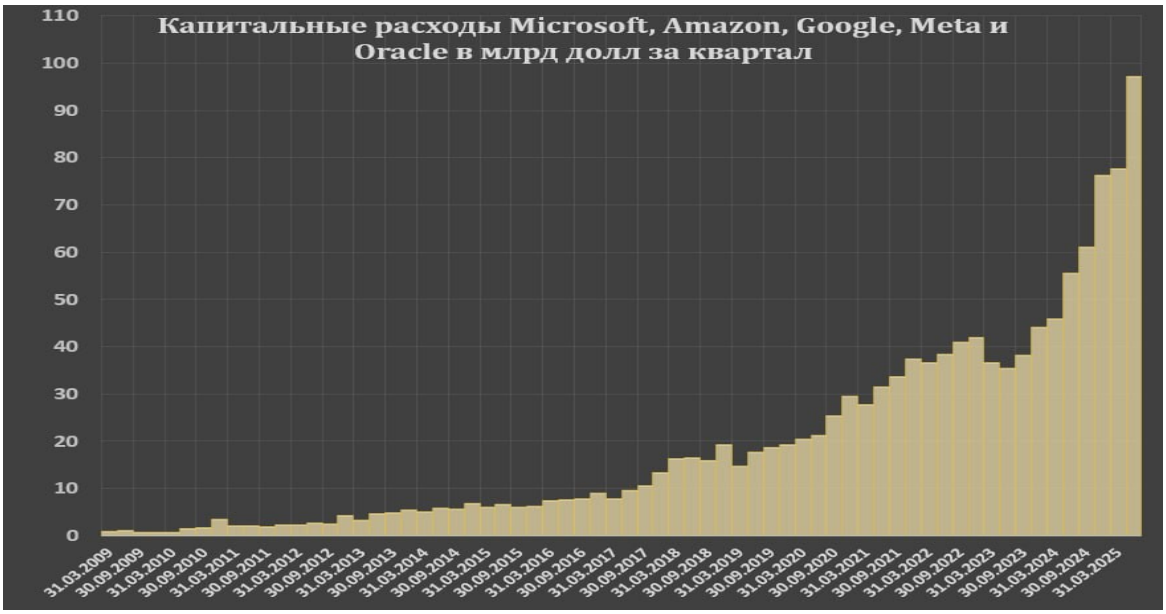

Рис. 1 Капитальные расходы ведущих IT-компаний

Предпосылка 3. ЦРУ начало интегрировать ИИ в свои операции не вчера, и даже не в 2023 г., когда об этом было заявлено официально, а в 2012 г. Состоялось внедрение ИИ-инструментов во все 18 разведывательных агентств США, где действует специальный чат-бот, созданный по заказу правительства, задача которого – обеспечить сотрудников быстрым доступом к информации и помочь в выполнении повседневных операций в закрытых системах.

Самые развитые компании типа Amazon, Web Services, Microsoft Azure и Google Cloud разработали версии своих платформ, прошедшие сертификацию для работы с государственными

данными. Эти решения позволили создать так называемые «секретные регионы» – отдельные зоны в облачной инфраструктуре, предназначенные для защиты критически важной информации.

Вторая зона, получившая название AWS Top Secret-West, была анонсирована ещё в 2021 году. На её запуск ушло четыре года.

Сейчас спецслужбы США разрабатывают программу для получения и анализа разведданных по аналогии с чат-ботом с искусственным интеллектом ChatGPT.

Все это вкупе с нагнетанием международной напряженности в отношении России требует обеспечения национальной безопасности как ключевой задачи государства.

Цель исследования: рассмотреть варианты использования методов ИИ в технической конкурентной разведке для решения проблемы технологического суверенитета государства в системе военно-промышленного комплекса.

Методы. В качестве методологии исследования используется системный подход, в качестве методов исследования: метод дедукции, метод анализа и синтеза, прямые и косвенные методы исследования конкурентной разведки и пр.

Нейросеть как инструмент поиска информации в конкурентной разведке

В России в 2017 году появилась Алиса, которую страна с восторгом приняла как свидетельство использования ИИ в реальной жизни. В этом же году 8 университетов США объявили о создании консорциума с ведущими оборонными предприятиями и через год выпустили 8 томов отчетов о будущей войне и ее техническом обеспечении: это дроны, системы лазерного прицеливания, системы управления роем дронов, космические «войска» и пр. Одно из обязательных направлений, которое присутствовало во всех отчетах, – возвращение технической разведки и опыта OSINT (Open-Source Intelligence, разведка на основе открытых источников)[1].

Ключевая роль технической разведки заключается не только в текущем докладе о конкурентах, а в определении и выявлении планов и намерений конкурентов.

Из всех существующих наиболее известных групп источников, которые ранее были на «вооружении» конкурентной разведки (КР): документы открытого доступа, опубликованные в официальной прессе, конфиденциальные данные, полученные от сотрудников или на выставках и ярмарках в неофициальных встречах, информация, полученная от «внешних» агентов (в том числе, увы, промышленным шпионажем), и данные специализированных на КР компаний – практически ничего нельзя использовать для всестороннего анализа уровня конкурентоспособности своих изделий и внесения изменений. Для этих целей привлекают исключительно экспертов.

Для сбора информации в [Bop07] предлагается алгоритм, который может бы представлен таблицей трехстадийного процесса конкурентной разведки[2] (табл. 1).

Конечно, великие разведчики вынуждены были решать в одиночку задачи первых двух этапов. А иногда и систематизация, и адресное распределение информации также являлись личным вкладом разведчиков. Бывшие сотрудники ЦРУ в своих воспоминаниях указывали, что практически 80–90 % информации получали из открытых источников, причем в то время, когда печатных изданий было в сравнении с современным количеством ничтожно мало, и все они проходили тщательную цензуру.

---

[1] Это методика и дисциплина, включающая в себя сбор, анализ и систематизацию информации из общедоступных источников, таких как социальные сети, СМИ, блоги, форумы и публичные базы данных.

[2] Методика сбора разведывательных данных на выставках и других массовых мероприятиях. М., 2011. 22 с. URL: http://www.rscip.ru/base/A2808271-8605775.html (дата обращения 18.09.2025).

Таблица 1

Реализация этапов конкурентной разведки [Bop07]

Этап	Задача	Действие
1	1 а. Определение потребности в сведениях	Систематизация вопросов
	1 б. Организация ресурсов для сбора информации	Систематизация источников информации
		Сбор информации
2	2 а. Обработка и оценка информации	Систематизация информации
	2 б. Анализ информации и выработка выводов	Генерация вторичной (обобщающей) информации
2	3 а. Передача информации лицам, принимающим решение	Обеспечение оперативной обратной связи с заказчиком
	3 б. Адресное распределение информации по подразделениям	Систематизация адресатов. Обеспечение конфиденциальности

Обилие всевозможных интернет-изданий, публикаций, оцифровывание журналов, которые раньше были доступны только в столичных библиотеках, означает, что не только корпорациям, но и государственным структурам, занимающимся вопросами национальной безопасности, скрывать что-то все труднее.

Во всех методических материалах по КР в соответствии с указанной на рис. 1 схемой заранее было известно, что кроме пункта 1а, части сведений пункта 1б (агентурная разведка) – все остальное намного эффективнее выполняется с помощью поисковиков, причем лицо, принимающее решение (ЛПР), должно «объяснить» компьютеру, что он ищет, то есть «составить поисковый запрос» [Bop07].

Поисковые роботы могут представить службе КР огромное количество текстов. И несмотря на предлагаемые автором [Bop07] «….работу по составлению, сопоставлению и состыковке трех классификаторов: классификатора вопросов (этап 1а), классификатора тем отобранной информации и классификатора персонала (для которого работает служба КР)», – алгоритмизации поддается далеко не каждая задача.

Все имеющиеся средства поиска информации в Интернете могут быть условно разделены на несколько подгрупп, а именно: средства поиска информации на отдельных сайтах, подборки ссылок, каталоги, поисковые системы, метапоисковые системы, системы мониторинга и контент-анализа, экстракторы объектов, событий и фактов, системы «knowledge discovery» (Data Mining, Text Mining), специализированные системы конкурентной разведки, интегрированные системы.

В чем проблема всех этих систем поиска технических решений для обеспечения высокого уровня выпускаемых изделий для оборонной промышленности:

1) поисковики либо находят бессмысленно огромное количество информации, либо вообще – ничего по данной теме;

2) в сети информация долго не хранится;

3) поисковику сложно хранить все ссылки и пр.

Но самое главное: все указанные системы и поисковики, которые лежат в основе этих систем, «не видят» ценности добываемой информации в соответствии с поставленной задачей, даже если проведена идеально ее алгоритмизация.

Таким образом, можно сделать вывод, что даже в условиях развитых традиционных информационных систем невозможно найти необходимую информацию для целей КР.

Впервые использовали практически все виды нейронных сетей, причем для целей откровенного промышленного шпионажа, китайские программисты: перцептроны, многослойные

перцептроны (MLP, для нелинейных задач), сверточные нейронные сети (CNN, для изображений), рекуррентные нейронные сети (RNN, для последовательностей), генеративно-состязательные сети (GAN, для создания нового контента), автокодировщики (для сжатия и извлечения данных) и трансформеры (для обработки текста).

Но год назад все пользователи нейронных сетей вынуждены были признать: данные для обучения нейронных сетей закончились. Спустя полгода об этом заявил И. Маск. Пытались использовать синтетические данные – но они отправляют к неверным кластерам. OpenAI на тестировании при использовании синтетических данных выявило 33–44 % «глюков» *ChatGPT,* например, *«Алиса, Земля плоская? – Да, Земля плоская».*

В декабре 2024 года китайские программисты выпустили сначала китайскую версию, а потом английскую версию нейронной сети DeepSeek (далее – Qwen AI и Kling AI). DeepSeek R1 – продвинутая языковая модель (LLM) от одноименной китайской компании, работает на основе третьего поколения их собственной технологии, значительно превосходит *ChatGPT.* Успеху DeepSeek во многом способствовала новая архитектура Multi-head Latent Attention (MLA), которая позволила сократить стоимость обучения на 90 %, игнорируя 95 % ненужных данных. *Конкретный заказчик этой сети – Китайский Фонд биржевой торговли.*

Причина создания этой сети тривиальна: США запретили ввоз видеоплат, топовых ускорителей и пр. Игра на бирже – игра с «нулевой суммой»[3] *– потребовала внедрение новых технологий.*

Что отличает DeepSeek от других сетей, почему ее лучше всего использовать для конкурентной разведки?

Преимущества DeepSeek:

1) Во-первых, наличие облака экспертов, определяющих кластеры, которые будет выбирать сеть. «Облако экспертов» может означать облачные сервисы, предоставляющие доступ к данным и вычислительным ресурсам через Интернет, либо облачную платформу, объединяющую экспертов для совместной работы и обмена знаниями[4]. В первом случае это могут быть различные типы облачных сервисов (IaaS, PaaS, SaaS), а во втором – специализированные платформы для управления проектами или работы с данными.

В результате такого анализа проводится структурированное разделение больших наборов данных на более мелкие, управляемые группы на основе общих признаков. Такой подход нашел широкое применение П в бизнесе (сегментирование рынка для целевого маркетинга), в медицине (группировка пациентов с общими симптомами) и самое главное – в научных исследованиях при анализе и структурировании больших объемов данных.

2) Во-вторых, DeepSeek – нейросеть с «рассуждалкой»; «рассуждающие» модели отвечают дольше, чем обычные, но ответ дают более осмысленный. «Такие нейросети обучались не только на датасетах с вопросами и ответами, но и на пошаговых рассуждениях, подкрепленных логикой»[3]. Благодаря этому они способны исправлять свои ошибки в процессе размышления и могут рассматривать разные пути решения проблемы.

3) В-третьих, разработчики ввели понятие «дистилляция модели», когда обученная генеративная модель – «учитель» – создает столько данных, сколько необходимо для обучения необученной или менее обученной модели «ученика».

Учитывая, что конкурентная разведка имеет дело с огромным массивом данных, которые необходимо не только проанализировать, но и выбрать самое ценное, и дополнить новыми предложениями, именно DeepSeek походит для этих целей идеально.

Рассмотрим пример.

---

[3] Игра с нулевой суммой (также антагонистическая игра) — это ситуация в теории игр, где выигрыш одного участника равен проигрышу другого, а общая сумма всех выигрышей и проигрышей равна нулю.

[4] Что такое DeepSeek и на что способна китайская нейросеть. [Электронный ресурс]. URL: https://practicum.yandex.ru/blog/nejroset-deepseek-kak-skachat-i-kak-polzovatsya (дата обращения 20.09.2025 г.).

Для оценки конкурентоспособности технического изделия и его совершенствования зададим ряд параметров, которые, по мнению экспертов, являются доминирующими для реализации заданных функций.

Будем считать, что эти прогнозируемые показатели Y_i ($i=\overline{1,M}$) будут определяться следующим образом (табл. 2).

Таблица 2

Прогнозируемые показатели

№	Подкластер 1	Подкластер 2	Подкластер 3	По всему кластеру
Y_1	f_1^1 (X1–X3, X5, X7–X11, X15–X19, X22–X40, L1)	f_1^2	f_1^3	f_1
Y_2	f_2^1	f_2^2	f_2^3	f_2
Y_3	f_3^1	f_3^2	f_3^3	f_3
Y_4	f_4^1	f_4^2	f_4^3	f_4
Y_5	f_5^1	f_5^2	f_5^3	f_5
Y_6	f_6^1	f_6^2	f_6^3	f_6

Вид функций f_i ($i=\overline{1,M}$) будем аппроксимировать нейросетью, предварительно настраиваемой на большом количестве исходных данных соответствующего подкластера.

В данных, используемых для обучения нейросетей, обязательно присутствуют искаженные результаты, так называемые «плохие» точки. Причинами появления подобных точек, помимо погрешностей, появляющихся при сборе данных, являются преднамеренные искажения. В процессе настройки нейросети формируется оператор, максимально точно аппроксимирующий зависимость между входными факторами и выходной величиной. Наличие «плохих» точек искажает результирующий оператор: при тестировании нейросети в неискаженных точках погрешность увеличивается, а в «плохих» – уменьшается, то есть ухудшаются ассоциативные свойства модели.

Удаление подобных точек позволит повысить точность нейросетевой модели. Здесь можно использовать поэтапный алгоритм исключения аномальных точек, описанный в [Бук01].

Пусть R – обучающее множество. Отбор подобных точек произведем по следующей процедуре:

1. Обучение нейросети на исходном множестве R.
2. Получение расчетных величин Y по значениям факторов из R.
3. Получение разницы Δ между расчетными величинами и величинами из $\{L\}$:

$$\Delta_r = \left| \frac{Y_r - \overline{Y}_r}{Y_r} \right|, \; r = \overline{1,R}.$$

4. Удаление из R обучающих примеров, у которых $\Delta > \Delta_{крит}$, где $\Delta_{крит}$ – критическое значение относительного отклонения, назначаемое аналитиком.
5. Обучение сети на сокращенном обучающем множестве.

Чтобы использовать полученные исходные данные при настройке нейронной сети, их необходимо разбить на три группы: обучающая выборка, выборка перекрестного подтверждения и тестирующая выборка. Для традиционных сетей при чрезмерно большом количестве обучающих примеров наступает так называемая перетренировка нейронной сети, ошибка на выходе сети начинает возрастать. С этой целью используют Statistica Neural Networks (нейросетевой модуль системы Statistica): в процессе обучения кроме примеров из обучающей

выборки через настраиваемую нейронную сеть пропускаются примеры из выборки перекрестного подтверждения, и для них отслеживается значение среднеквадратической ошибки. Если значение ошибки начинает вместо убывания возрастать, то процесс обучения прерывается. Как показывают эксперименты, желательный объем выборки перекрестного подтверждения оставляет 10–20 % обучающей выборки.

Для DeepSeek таких проблем не существует. Она будет несколько дольше настраиваться, «дискутируя» сама с собой. Но в результате получаем результаты значительно лучше.

Еще одно важное преимущество DeepSeek состоит в том, что это сеть с открытыми кодами. Ею можно пользоваться. Она заточена под изучение технических проблем.

DeepSeek позволяет через дистилляцию решить самую главную проблему: как улучшить конкурентные предложения, тем более, задачи решаются в реальном времени.

Контент-анализ и нейросети

Контент-анализ – один из базовых методов проведения анализа текста, применяемого социологами, маркетологами, политологами и …разведчиками. Он позволяет структурировать, классифицировать отдельные слова-паттерны, выделяя темы, категории и типовые единицы текста. Этот метод позволяет очень быстро и эффективно оценить и эмоциональное настроение гражданского общества, и ключевые направления политики (в предвыборной речи президентов), и даже основные направления технического развития. Отслеживаются социальные аспекты, включая доверие, признание и коммуникации как по отношениям внутри коллектива, так и на уровне государства у разных социальных групп. Ранее выполнялся либо вручную, либо с помощью обычных программ сортировки данных.

Контент-анализ включает в себя использование методов ИИ и обработки естественного языка (NLP) для понимания и извлечения содержательной информации из текста.

Применение NLP включает несколько ключевых этапов:

1) предобработка данных, когда текст освобождается от лишних символов, и выполняется токенизация (разделение текста на отдельные слова-паттерны или словосочетания);

2) векторизация, когда текст преобразуется в числовой формат, что позволяет системе проводить математические операции над ним с помощью популярных методов TF-IDF и Word2Vec;

3) моделирование, когда, используя подготовленные данные, нейросеть обучается на задаче;

4) тестирование и оценка.

Применение нейросетей для анализа текстов – в контент-анализе – находит широкое применение в различных областях:

1) в маркетинговых исследованиях и/или когда необходимо провести анализ отзывов клиентов для быстрого решения проблем сервиса;

2) в журналистике – для поиска свежих новостей и извлечения ключевых идей из больших объемов информации, для формирования специальных настроений и отношений;

3) в образовании – для оценки и формирования обратной связи с обучающимися.

В ТОП-15 нейросетей, предназначенных для контент-анализа и поиска ключевых слов входят такие, как BERT, GPT-3, RoBERTa, DistilBERT, T5 и ALBERT. Каждая из этих сетей обладает уникальными особенностями и применяется в различных задачах. Например, BERT отлично справляется с задачами контекстуального анализа, а T5 может использоваться для генерации текста. Эти модели обучаются на больших объемах данных, что позволяет им повышать свою эффективность и точность.

И опять DeepSeek лидирует, поскольку видит то, что скрыто от людей в соответствии с доминирующим принципом конкурентной разведки: «Что видимо – то не видимо». DeepSeek отличает:

1) глубокий контекстный анализ, когда система учитывает и внешние факторы (новости, соцсети);

2) автоматическая генерация гипотез: DeepSeek самостоятельно выдвигает гипотезы;

3) адаптация под нишу, когда платформа настраивается под специфику бизнеса.

При этом DeepSeek имеет уникальный ИИ-детектор аномалий – находит ошибки в данных или мошеннические схемы, которые не замечают даже опытные аналитики, работает в режиме «что, если» благодаря «рассуждалке», моделирует последствия решений.

Компании, использующие ИИ для поиска ключевых слов и структурирования текстов, получают конкурентные преимущества.

«Боевой блогинг» и нейросети

Конкурентная разведка использует различные виды «боевого» блогинга: блог-«аэростат», блог-«торпеда», блог-«пересмешник» и пр. У каждого из них свои задачи: у одного – не допустить проникновения конкурентов на свою территорию, у другого – пробить ресурсы противника, у третьего – запутать пользователей. И это приводит к тому, что: «Всё смешалось в мире контента»! ИИ-писатели без писателей, ИИ-картины без художников, и миллионы текстов, написанных машинами. Искусственный интеллект не только научился писать, но слился с блогосферой.

За годы обучения на миллионах текстов, мемов и новостных заголовков итогом стало то, что сейчас искусственный интеллект умеет не только писать заметки, но и выстраивать целые контент-стратегии, спасая службы КР от рутины.

Самые популярные нейросети для блогеров в 2025 году: для боевого блогинга в виде блога-«торпеды», когда нужно бомбить сети, штурмовать рунет есть специальные сервисы, и их количество растёт с каждым днём: Midjourney (создаёт картинки из воздуха); ChatGPT и аналоги (пишут отчеты), Jasper AI (управляет SEO и маркетингом); Copy.ai (генерирует креативные идеи, тексты, заголовки), Writesonic (создаёт длинные статьи и переводит тексты), СигмаЧат/GenAPI (следит за русскоязычными блогами в Telegram и ВКонтакте), Frase.io (оптимизирует тексты под SEO, делая их настоящими магнитами для глаз).

Искусственный интеллект может копировать стиль конкретного блогера, подделывая индивидуальные шутки и манеру обращения к фолловерам, что великолепно подходит для создания блога-«пересмешника».

Представленные отдельные методы конкурентной разведки далеко не в полном объеме раскрывают возможности ИИ для использования его в сфере разведки. Появление новых инструментов, возможность трансформации нейросети под живого человека может заменить и агентурную разведку, которая ранее не допускала даже возможности компьютерной замены.

Это позволит значительно ускорить внедрение новых технологий, сократить длительность производственного цикла и выйти на заданные объемы производства продукции ВПК к указанному сроку, предотвратив угрозы национальной безопасности.

Заключение

Современные события в сфере международной безопасности ставят на первый план задачи обеспечения технологического суверенитета и конкурентоспособности продукции военно-промышленного комплекса (ВПК) в системе национальной безопасности. По многим направлениям, к сожалению, Россия отстает в силу долгой привязки к сырьевой направленности экспорта.

Для решения проблем выравнивания ключевых позиций по базовым изделиям ВПК предлагается использование легальных методов конкурентной разведки.

Одним из самых современных методов поиска информации являются нейронные сети, и прежде всего DeepSeek. Преимущества этой сети в отличие от других известных инструментов ИИ заключается в следующем: наличие облака экспертов, определяющих кластеры, которые будет выбирать сеть; наличие «рассуждающей» модели, которая отвечает дольше, чем обычные, но ответ дает более осмысленный; наличие «дистилляция модели», когда обученная генеративная модель создает столько данных, сколько необходимо для обучения.

Важным преимуществом является то, что это сеть с открытыми кодами и заточена на исследование технических проблем.

СПИСОК ЛИТЕРАТУРЫ / REFERENCES

[Бая02] Баяндин Н. И. Технологии безопасности бизнеса. М.: Юрист, 2002.

Bayandin N. I. Business Security Technologies. Moscow: Jurist, 2002. (In Russian).

[Бук01] Букаев Г. И., Бублик Н. Д., Горбатков С. А., Сатаров Р. Ф. Модернизирование системы налогового контроля на основе нейросетевых информационных технологий. М.: Наука, 2001. 344 с.

Bukaev G. I., Bublik N. D., Gorbatkov S. A., Satarov R. F. Modernization of the tax control system based on neural network information technologies. Moscow: Nauka, 2001. (In Russian).

[Вор07] Воронов Ю. П. Конкурентная разведка: Уч. пос. М., 2007.

Voronov Yu. P. Competitive intelligence: a tutorial. Moscow, 2007. (In Russian).

[Джи10] Джилад Б. Конкурентная разведка. Как распознавать внешние риски и управлять ситуацией. СПб.: Питер, 2010. 320 с.

Gilad B. Competitive Intelligence: How to Recognize External Risks and Manage the Situation. St. Petersburg: Piter, 2010. (In Russian).

[Дор07] Доронин А. И. Бизнес-разведка. М.: Ось-89, 2007. QXGTBJ.

Doronin A. I. Business intelligence. Moscow: Os-89, 2007. (In Russian). QXGTBJ.

[Кат00] Каторин Ю. Ф., Куренков Е. В., Лысов А. В. Большая энциклопедия промышленного шпионажа. М.: Изд-во Полигон, 2000. UFPAUT.

Katorin Yu. F., Kurenkov E. V., Lysov A. V. The Great Encyclopedia of Industrial Espionage. Moscow: Polygon Publishing House. 2000. (In Russian). UFPAUT.

[Куз09] Кузин А., Нежданов И., Ющук Е. Дезинформация и активные мероприятия в бизнесе. Казань: Яналиф, 2009.

Kuzin A., Nezhdanov I., Yushchuk E. Disinformation and active measures in business. Kazan: Yanalif, 2009. (In Russian).

[Лем07] Лемке Г. Э. Конкурентная война: Нелинейные методы и стратегемы. М.: Ось-89, 2007. 464 с.

Lemke G. E. Competitive War: Nonlinear Methods and Strategems. Moscow: Os-89, 2007. (In Russian).

[Мас22] Масалович А. И. КиберДед знает. Инструкция по процветанию в турбулентные времена от ветерана отечественной интернет-разведки. М.: Изд-во Бомбора, 2022. 224 с.

Masalovich, A.I., "CyberGrandfather Knows." A Guide to Prospering in Turbulent Times from a Veteran of Russian Internet Intelligence. Bombora Publishing, 2022. (In Russian).

[Мел09] Мелтон Г., Пилиган К. Офисный шпионаж. М.: Феникс, 2009.

Melton G., Piligan K. Office Espionage. Moscow: Phoenix, 2009. (In Russian).

[Род24] Родионова Л. Н., Давлетшина С. М. Конкурентная разведка: Уч. пос. Уфа, 2024. 310 с. AHYROX.

Rodionova L. N., Davletshina S. M. Competitive intelligence: textbook. Ufa, 2024. (In Russian). AHYROX.

[Руд10] Рудометов Е. А., Рудометов В. Е. Шпионские штучки. Электронные средства коммерческой разведки. М.: АСТ, Полигон, 2010. 224 с.

Rudometov E. A., Rudometov V. E. Spy gadgets. Electronic means of commercial intelligence. Moscow: AST, Polygon, 2010. (In Russian).

[Шуш05] Шушкевич С. В. «Путь воина»: XXI век, или что такое конкурентная разведка // Маркетинговые коммуникации. 2005. № 4. С. 33–40. HUWYAL.

Shushkevich S. V. "The Way of the Warrior": The 21st Century, or What is Competitive Intelligence // Marketing Communications. 2005. No. 4. P. 33-40. (In Russian). HUWYAL.

[Ющу07] Ющук Е. Интернет-разведка. Руководство к действию. М.: Вершина, 2007. 256 с.

Yushchuk E. Internet Intelligence. Guide to Action. Moscow: Vershina, 2007. (In Russian).

[Ющу08] Ющук Е., Кузин А. Противодействие черному PR в Интернете. М.: Вершина, 2008. 248 с.

Yushchuk E., Kuzin A. Counteracting Black PR on the Internet. Moscow: Vershina, 2008. (In Russian).

ОБ АВТОРЕ | ABOUT THE AUTHOR

РОДИОНОВА Людмила Николаевна
Уфимский университет науки и технологий, Россия.
rodion@ufanet.ru ORCID: 0000-0003-2634-5579.
Проф. каф. экономики предпринимательства. Экономика и организация машиностроительного производства. Инж.-экономист (Уфимск. авиац. ин-т, 1980). Д-р экон. наук (С.-Петерб. гос. эконом. ун-т, 1998). Иссл. в обл. экономической и национальной безопасности, надежности финансово-промышленных групп.

RODIONOVA Lyudmila Nikolaevna
Ufa University of Science and Technology, Russia.
rodion@ufanet.ru ORCID: 0000-0003-2634-5579.
Prof. Dept. of Economics of Entrepreneurship. Engineer-economist (Ufa Aviat. Inst., 1980). Dr. of Economics (St. Petersburg State Univ. of Economics, 1998). Research in the area of economic and national security, reliability of financial and industrial groups).

МЕТАДАННЫЕ | METADATA

Заглавие: Интеллектуальные методы конкурентной разведки в обеспечении национальной безопасности.

Авторы: Родионова Л. Н.

Аннотация: Современные методы конкурентной разведки являются симбиозом методов военной разведки, расширением и диверсификацией методического обеспечения исследования рынка и конкурентов в маркетинге, дополненные самыми современными исследованиями в области информационных технологий. Управление корпорациями, предприятиями, что означает в совокупности и оптимизацию финансовых потоков, и решение задач управления персоналом, и формирование запасов ресурсов – становится сложной задачей, когда конкуренция вышла за рамки отдельных государств и стала глобальной. Но основная проблема современного управления компаниями заключается не в поиске достоверных данных о рынке, конкурентах и потребителях, а в донесении любых входящих данных, связанных с компанией и рынком, до руководителя, который и производил фильтрацию и обработку данных. Сейчас ситуация резко изменилась. В статье рассмотрены методы конкурентной разведки, которые можно использовать совместно с разработанными нейронными сетями, методами искусственного интеллекта (ИИ) в целях обеспечения национальной безопасности государства для совершенствования сложной технической продукции, в том числе оборонного комплекса. Проведен анализ возможности использования различных нейронных сетей для задач технической разведки и представлены рекомендации по их применению.

Ключевые слова: Конкурентная разведка; национальная безопасность; технологический суверенитет; искусственный интеллект.

Язык: Русский.

Статья поступила в редакцию 2 февраля 2026 г.

Title: Intellectual methods of competitive intelligence in ensuring national security.

Authors: Rodionova L. N.

Abstract: Modern competitive intelligence methods are a symbiosis of military intelligence techniques, an expansion and diversification of methodological support for market and competitor research in marketing, supplemented by the latest research in information technology. Managing corporations and enterprises—which collectively entails optimizing financial flows, solving human resource management problems, building resource reserves, and so on—becomes a complex task when competition has expanded beyond the borders of individual countries and become global. However, the main problem of modern company management is not finding reliable data on the market, competitors, and consumers, or communicating any incoming data related to the company and the market to the manager, who then filters and processes the data. Now the situation has changed dramatically. This article examines competitive intelligence methods that can be used in conjunction with developed neural networks and artificial intelligence (AI) methods to ensure national security and improve complex technical products, including those in the defense industry. An analysis of the possibility of using various neural networks for technical intelligence tasks was conducted and recommendations for their application were presented.

Key words: Competitive intelligence, national security, technological sovereignty, artificial intelligence.

Language: Russian.

The article was received by the editors on 2 February 2026.