# ПРИМЕНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ИНТЕРЕСАХ ТЕРРИТОРИАЛЬНОЙ ОБОРОНЫ РОССИИ

THE USE OF ARTIFICIAL INTELLIGENCE IN THE INTERESTS OF RUSSIA'S TERRITORIAL DEFENSE

**УДК 378.01(045)**

**Машнич Александр Сергеевич**, начальник 43 кафедры, Военная академия связи, г.Санкт-Петербург

**Иванов Андрей Анатольевич**, доцент 43 кафедры, Военная академия связи, г.Санкт-Петербург

**Киргизова Наталья Петровна**, старший научный сотрудник научно-исследовательской лаборатории №5, Военная академия связи, г.Санкт-Петербург

**Mashnich A.S.** mals08@mail.ru

**Ivanov A.A**. a-a-iv@yandex.ru

**Kirgizova N.P.** natalya-kirgizova@yandex.ru

**Аннотация**

Статья посвящена поиску направлений повышения эффективности территориальной обороны Российской Федерации за счет применения информационных технологий, в частности – искусственного интеллекта. Рассмотрены основные направления использования искусственного интеллекта для решения задач территориальной обороны. В статье приведены основные программные продукты в сфере искусственного интеллекта, решающие аналогичные задачи в бизнесе. Авторами предложены

рекомендации по организации территориальной обороны с использованием искусственного интеллекта, совершенствованию системы военного образования в сфере информационных технологий.

**Annotation**

The article is devoted to the search for ways to improve the effectiveness of the territorial defense of the Russian Federation through the use of information technologies, in particular, artificial intelligence. The main directions of using artificial intelligence for solving problems of territorial defense are considered. The article presents the main software products in the field of artificial intelligence that solve similar problems in business. The authors offer recommendations for organizing territorial defense using artificial intelligence, improving the system of military education in the field of information technology.

**Ключевые слова**: информационные технологии, искусственный интеллект, военное образование, территориальная оборона, организация территориальной обороны, угрозы Российской Федерации.

**Keywords**: information technologies, artificial intelligence, military education, territorial defense, organization of territorial defense, threats to the Russian Federation.

Анализ современных форм и способов реализации национальных интересов зарубежных стран с применением силы показывает, что в настоящее время и в обозримой перспективе важными средствами воздействия на критические инфраструктуры государства-жертвы рассматриваются силы специальных операций (ССО), отряды незаконных вооруженных формирований (НВФ), частные военные компании (ЧВК), террористические организации (ТО). Проведением диверсионных и террористических действий, еще до начала военных действий, они способны нарушить функционирование жизненно-важных систем (коммуникационных,

коммунальных, энергетических, транспортных, управления, банковских и др.), обеспечивающих деятельность населения и организаций. Опыт военных конфликтов на Северном Кавказе Российской Федерации, в Ливии и Сирии демонстрирует наличие тенденции на увеличение масштаба комплексного применения военных и невоенных формирований по единому плану и под единым управлением.

Учитывая вышеназванные тенденции, в Стратегии национальной безопасности РФ в качестве основных угроз безопасности закреплены следующие [1]:

разведывательная и иная деятельность спецслужб и организаций иностранных государств, отдельных лиц, наносящая ущерб национальным интересам;

деятельность экстремистских и террористических организаций, направленная на насильственное изменение конституционного строя РФ, дестабилизацию работы органов гос. власти, уничтожение или нарушение функционирования промышленных и военных объектов, транспортной инфраструктуры, объектов жизнеобеспечения населения, устрашение населения, в том числе путем завладения оружием массового поражения, отравляющими, токсичными, радиоактивными, химически и биологически опасными веществами, совершения актов ядерного терроризма, нарушения устойчивости функционирования и безопасности критической информационной инфраструктуры РФ.

Данные угрозы непосредственно связаны с внутренними военными опасностями и основными военными угрозами, закрепленными в Военной доктрине Российской Федерации [2].

В первую очередь внутренними военными опасностями рассматриваются:

деятельность, направленная на… дезорганизацию функционирования органов государственной власти, важных государственных, военных объектов и информационной инфраструктуры РФ;

деятельность террористических организаций и отдельных лиц, направленная на подрыв суверенитета, нарушение единства и территориальной целостности РФ.

Основными военными угрозами определены:

воспрепятствование работе систем государственного и военного управления РФ, нарушение функционирования ее стратегических ядерных сил, систем предупреждения о ракетном нападении, контроля космического пространства, объектов хранения ядерных боеприпасов, атомной энергетики, атомной, химической, фармацевтической и медицинской промышленности и других потенциально опасных объектов;

создание и подготовка НВФ, их деятельность на территории Российской Федерации или на территориях ее союзников.

В этой связи возрастает актуальность совершенствования военной организации государства для обеспечения своевременного выявления существующих и перспективных военных опасностей и угроз, сбалансированного развития компонентов военной организации, а также оснащения ВС РФ, других войск, воинских формирований и органов современными вооружением, военной и специальной техникой, инновационного развития оборонно-промышленного комплекса России.

При этом такое совершенствование должно учитывать комплексное применение субъектов военной организации государства при решении задач территориальной обороны с единой системой управления и информационного взаимодействия.

В сущности, территориальная оборона Российской Федерации рассматривается как «система осуществляемых в период действия военного положения мероприятий по охране и обороне военных, важных

государственных и специальных объектов, объектов, обеспечивающих жизнедеятельность населения, функционирование транспорта, коммуникаций и связи, объектов энергетики, объектов, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, по борьбе с диверсионно-разведывательными формированиями иностранных государств и незаконными вооруженными формированиями, по выявлению, предупреждению, пресечению, минимизации и (или) ликвидации последствий их диверсионной, разведывательной и террористической деятельности в целях создания благоприятных условий для функционирования указанных объектов и применения Вооруженных Сил Российской Федерации, других войск, воинских формирований, органов и создаваемых на военное время специальных формирований» [3, ст.22].

Таким образом, можно сделать вывод, что для осуществления территориальной обороны в границах военного округа, или государства в целом, требуется создать межведомственную систему, способную осуществлять ситуационную и прогнозную оценку обстановки по действиям противника и своих сил, планирование применения разнородных сил и средств военной и гражданской принадлежности на большой территории с большим количеством охраняемых и обороняемых объектов в условиях слабо формализованного обмена информации.

Анализ учений по территориальной обороне, показал, что основными требованиями к работе должностных лиц при управлении силами и средствами являются оперативность обработки поступающей информации, точность прогноза о деятельности диверсионно-террористических сил, своевременность уточнения решения по применению своей группировки и доведения его до потребителей. При этом проблемным вопросом является то, что на вооружение органов управления силами и средствами территориальной обороны пока не приняты какие-либо программно-

аппаратные комплексы, универсальные расчетно-аналитические программы и модели, системы поддержки принятия решений, позволяющие обеспечить выполнение вышеназванных требований.

Для устранения данной проблемы предлагается рассмотреть существующие возможности информационных технологий с применением искусственного интеллекта (ИИ).

Сфера ИИ относится к когнитивным наукам, связанным с приобретением (сбором, накоплением, восприятием) знаний, способностью к обучению (самообучению). Это характеризуется способностью систем ИИ быстро обучаться работать со структурированными, неструктурированными и нечётко структурированными данными, позволяющей замещать деятельность должностных лиц при решении большого количества когнитивных задач, что полностью отвечает формату работы при выполнении мероприятий территориальной обороны.

По мнению экспертов [4], для обеспечения систем ИИ учёным пришлось разрабатывать технологии «представления знаний», что позволило создать так называемые экспертные системы (ЭС), которые при использовании баз знаний помогают в принятии решений. Большую важность для ИИ приобрела разработка методов самообучения машин, появились интеллектуальные обучающие системы, в том числе в виде искусственных нейронных систем с реализацией аналогов работы нервной системы человека.

В бизнесе технологии искусственного интеллекта уже применяются для решения конкретных задач. Анализ перспектив их применения проводится различными организациями, в том числе для вложения инвестиций. Один из вариантов востребованности технологий ИИ представлен аналитиками Сбербанка России (рис.1), который подтверждает тезис, что для систем государственной безопасности высокую

востребованность вызывают интеллектуальные технологии поддержки принятия решений.

| Суб-СЦТ | Рыночные сектора | Инфраструк-турные сектора | Социальная сфера | Госуправление и безопасность |
|---|---|---|---|---|
| Компьютерное зрение | Высокая | Высокая | Средняя | Средняя |
| Обработка естественного языка | Высокая | Средняя | Средняя | Средняя |
| Распознавание и синтез речи | Высокая | Средняя | Средняя | Средняя |
| Рекомендательные системы и интеллектуальные системы поддержки принятия решений | Высокая | Высокая | Высокая | Высокая |
| Перспективные методы развития технологий ИИ | Средняя | Низкая | Низкая | Низкая |
| Нейростимуляция и нейросенсинг | Средняя | Низкая | Высокая | Низкая |
| Нейропротезирование и нейроинтерфейсы | Высокая | Низкая | Высокая | Средняя |

Низкая востребованность | Средняя востребованность | Высокая востребованность

Рис. 1. Востребованность технологий искусственного интеллекта

Для адаптации применения технологий ИИ в интересах территориальной обороны необходимо рассмотреть мероприятия [5] и задачи (таблица 1, 2) [6], выполняемые разными федеральными органами исполнительной власти.

При подготовке и ведении территориальной обороны, в соответствии с «Положением о территориальной обороне», проводятся следующие мероприятия.

1. По охране и обороне военных, важных государственных и специальных объектов, объектов, обеспечивающих жизнедеятельность населения, функционирование транспорта, коммуникаций и связи, объектов энергетики, объектов, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды.

2. По борьбе с диверсионно-разведывательными формированиями иностранных государств и незаконными вооруженными формированиями.

3. По выявлению, предупреждению, пресечению, минимизации и (или) ликвидации последствий их диверсионной, разведывательной и террористической деятельности.

Таблица 1

Задачи Федеральных органов исполнительной власти по охране и обороне объектов территориальной обороны

| Формирования ВС РФ | Территориальные органы МВД России | Войска национальной гвардии России | Органы ФСБ России |
|---|---|---|---|
| осуществление охраны и обороны военных объектов | осуществление охраны объектов, подлежащих обязательной охране полицией | осуществление охраны объектов, подлежащих обязательной охране войсками национальной гвардии; осуществление охраны важных государственных объектов и объектов на коммуникациях | осуществление охраны важных объектов, находящихся в ведении ФСБ |

Таблица 2

Задачи федеральных органов исполнительной власти по борьбе с диверсионно-разведывательными формированиями иностранных государств и незаконными вооруженными формированиями

| Формирования ВС РФ | Территориальные органы МВД России | Войска национальной гвардии России | Органы ФСБ России |
|---|---|---|---|
| проведение войсковых мероприятий по блокированию и ликвидации ДРГ, НВФ; огневое поражение крупных НВФ, блокирование и оцепление районов проведения специальных, оперативно-боевых и иных мероприятий | анализ оперативной обстановки в районах ответственности, розыск, в том числе путем проведения оперативно-розыскных мероприятий, и задержание террористов, диверсантов и их пособников, а также участие в проведении специальных, оперативно-боевых и иных мероприятий по ликвидации НВФ | проведение специальных, оперативно-боевых и иных мероприятий по пресечению деятельности ДРГ и НВФ вблизи охраняемых объектов | осуществление контрразведывательных и оперативно-розыскных мероприятий по борьбе с ДРГ и НВФ, противодействию их диверсионной, разведывательной и террористической деятельности, участие в специальных, оперативно-боевых и иных мероприятиях по борьбе с ДРГ и НВФ |

Задачи по выявлению, предупреждению, пресечению, минимизации последствий диверсионной, разведывательной и террористической

деятельности выполняются силами и средствами разведки, оперативными органами и специальными формированиями всех федеральных органов исполнительной власти заблаговременно в мирное время и продолжаются в ходе и после завершения диверсионно-террористических действий противника. Важной особенностью эффективного выполнения данных задач является правильная организация применения разноведомственных сил и средств, иррегулярных формирований (казачества, общественных и патриотических организаций и т.п.) осуществляющих добывание, сбор, обработку, анализ и оценку информации о действиях ССО, НВФ, ЧВК и ТО, а также установление общепринятых форматов и категории срочности передаваемых в информационной системе сведений (данных).

Опыт Великой Отечественной войны продемонстрировал большую роль иррегулярных формирований в решении задач (обеспечении мероприятий) территориальной обороны СССР. Для борьбы с диверсантами и десантами противника создавались истребительные батальоны под руководством командиров воинских частей войск НКВД, оперативных работников или начальников отделений милиции. К концу июля 1941 г. было сформировано 1 755 истребительных батальонов, а их численность составила 328 тыс. человек. Более 300 тыс. человек работали в группах содействия истребительным батальонам, выполняя задачи по информированию командования обо всех случаях появления десантов и диверсантов противника в районе действий истребительного батальона [7].

Таким образом, рекомендуется применение ИИ в интересах организации и ведения территориальной обороны рассматривать в соответствии с выполняемыми мероприятиями и задачами.

В мероприятиях охраны и обороны важных объектов искусственный интеллект способен обеспечить следующие задачи:

1. Минимизацию влияния человеческого фактора и эффективное прогнозирование воздействия на объекты территориальной обороны по времени (очередности) и масштабу с определением их важности.

2. Автоматизацию и достоверность оценки уязвимости объектов за счет использования ретроспективных данных, экспертных систем и моделей.

3. Прогнозирование поведенческой модели диверсионно-террористических групп (ДТГ) по воздействию на объекты территориальной обороны, распределение группировки противника по всему перечню охраняемых объектов.

4. Расчет достаточности привлекаемых наших сил и средств для каждого объекта, группы объектов в зоне (районе) территориальной обороны, их оснащенность вооружением и специальной техникой.

5. Определение оптимальных способов применения сил и средств обороны объектов с учетом прогнозных моделей действий ДТГ противника.

6. Расчет оптимальной структуры системы управления для гарантированного сбора сведений о противнике и своих силах, оповещения и информационного обмена в зоне, районе территориальной обороны, военном округе и в стране в целом.

7. Оценку эффективности выполняемых задач по охране и обороне важных военных объектов с учетом укомплектованности и сроков подготовки подразделений территориальных войск различной категории.

8. Расчет ресурсного обеспечения сил и средств территориальной обороны, потребность в резервах, восполнении потерь, их перераспределение при уничтожении обороняемого объекта.

Для повышения эффективности мероприятий борьбы с диверсионно-разведывательными формированиями (ДРФ) иностранных государств и незаконными вооруженными формированиями технологии ИИ могут обеспечить следующие задачи:

1. Расчет оптимальных маршрутов заброски и вывода ДРГ, НВФ, их перемещения к объектам воздействия, учитывая прогнозы транспортных коридоров (уровень охраны государственной границы, территории, физико-географические и погодные условия) и характеристик транспортных средств.

2. Прогнозирование районов (мест) размещения пунктов базирования и другой инфраструктуры НВФ, ССО, ТО за счет оценки вероятного характера их действий и факторов, влияющих на выполнение ими задач и живучесть.

3. Оценку возможностей НВФ, ТО по восполнению потерь, наращиванию рекрутской базы, переброске и подготовке боевиков.

4. Расчет оптимального состава нашей группировки для уничтожения ДРГ, НВФ, ее размещение на местности при подготовке и в ходе специальных мероприятий.

5. Определение потребности в использовании беспилотных транспортных средств, средств высокой проходимости, оружия на новых физических принципах.

6. Оптимизацию работы подразделений тылового и технического обеспечения за счет автоматизированного учета номенклатуры вооружения, военной и специальной техники межведомственной группировки, скорости расходования ресурсов, а также роботизации складов и другой тыловой инфраструктуры.

Обеспечение технологиями ИИ мероприятий по выявлению, предупреждению, пресечению, минимизации и (или) ликвидации последствий диверсионной, разведывательной и террористической деятельности, как наиболее объемному по привлекаемым силам и средствам, времени и ресурсам блоку задач, позволит обеспечить:

1. Оптимизацию распределения привлекаемых ресурсов на основе деятельности требующих наблюдения объектов противника в реальном времени и анализа прогнозной нагрузки.

2. Рекомендации в области необходимых инвестиций по строительству сетевой инфраструктуры за счет оценки потребностей информационной сети и выполнении требований по защите информации.

3. Прогноз тенденций масштаба деятельности противника с учетом реализации нами превентивных мероприятий по уничтожению (ликвидации) террористических формирований, разведывательных сетей.

4. Определение уровня достаточности расходов при создании и развитии системы защиты объектов территориальной обороны.

5. Совершенствование форм и способов применения Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов с учетом тенденций изменения характера современного вооруженного противоборства в мирное и военное время.

6. Определение условий для наиболее полной реализации боевых и специальных возможностей сил и средств территориальной обороны.

7. Выработку требований к перспективным формированиям, новым способам и средствам вооруженной борьбы, применяемым в интересах территориальной обороны.

С учетом содержания рекомендуемых задач ИИ для повышения эффективности подготовки и ведения территориальной обороны, основными подходами к созданию технологий ИИ, на наш взгляд, могут рассматриваться: «машинное обучение», «глубокое (глубинное) обучение», «онтологическое моделирование».

При этом «машинное обучение» предлагается рассматривать как совокупность алгоритмов и методов, позволяющих научить компьютеры делать выводы на основании имеющихся данных. Данный подход наиболее полезен для обеспечения задач по оптимизации структур, известных процессов в системе территориальной обороны и расходов на нее.

«Глубокое (глубинное) обучение» применяется для обучения искусственных нейронных сетей (ИНС), использующих больше одного

скрытого слоя (формально «глубинный» указывает на многослойную архитектуру нейронной сети). В этом случае компьютер сам находит признаки, позволяющие отделить один класс объектов от другого, и структурирует их иерархично: из более простых складывает более сложные. Таким образом, компьютер учится на примерах и своём собственном опыте.

Наиболее распространенным примером этой технологии является программа AlphaGo, которая сумела обыграть в игру «го» её абсолютного чемпиона Ли Седоля. Это было достигнуто за счет того, что после участия в обучении программы AlphaGo людей – профессиональных игроков, две копии программы включили в игру друг с другом. Добавляя новые партии в обучающую выборку и сыграв миллионы партий, программа AlphaGo научилась оценивать наиболее выгодное положение «камней» на доске для достижения победы.

Этот подход наиболее применим в решении задач охраны и обороны объектов территориальной обороны. Большинство объектов являются стационарными, с известными физико-географическими условиями, статистическим набором сведений о погодных условиях и оперативно-тактических возможностей сил и средств обороны и диверсионно-террористических сил.

Онтологическое моделирование является одним из самых сложных подходов для создания технологий ИИ. В его основе лежит описание наиболее полной совокупности данных о той или иной предметной области и логических взаимосвязей между ними. Следовательно, данный подход позволит обеспечить развитие форм и способов применения сил и средств территориальной обороны, определить условия для максимальной реализации их возможностей, а также требования к перспективным формированиям.

При создании программно-аппаратных продуктов ИИ следует учесть уже имеющиеся разработки, среди которых можно выделить интеллектуальные системы «Smart Projects» и «Aurora». «Smart Projects» – отечественная система управления проектами с поддержкой полного цикла

для построения сложных систем планирования и управления. «Smart Projects» использует такие технологии как мультиагентные системы, онтологии и сетецентрический подход. «Aurora» предназначена для создания оптимальных календарно-сетевых графиков проектов. Она использует технологии искусственного интеллекта для сохранения и применения правил и знаний планирования. «Aurora» может быть эффективна для создания крупных проектов со сложными ограничениями и требованиями к ресурсам.

Для реализации изложенных в статье рекомендаций требуется участие высокопрофессиональных специалистов в сфере обороны государства, информационных технологий, со знанием особенностей применения зарубежных ССО, современных форм гибридных и асимметричных действий против России с участием ЧВК, НВФ и террористических организаций.

Наибольшую озабоченность вызывает состояние обучения когнитивным наукам, недостаточное количество квалифицированных преподавателей и качество учебных программ в этом направлении.

В этой связи необходимо принятие централизованных мер по совершенствованию системы военного образования в сфере информационных технологий с прагматической направленностью на формирование знаний, умений и навыков по созданию систем ИИ в интересах обеспечения поддержки принятия решений во всем множестве форм применения и задач Вооруженных Сил Российской Федерации в мирное и военное время. Также в деятельности военных учебных заведений следует уделять большое внимание обобщению опыта военных конфликтов, кризисных ситуаций с участием вооруженных формирований, результатов проводимых мероприятий оперативной и боевой подготовки наших войск (сил) и иностранных армий. Внедрить в учебный процесс в качестве базовых дисциплин «Вооруженные силы иностранных государств», «Основы информационно-аналитической работы» и «Информационные технологии военного назначения». Это позволит достичь одинаковой базовой подготовки будущих защитников отечества и обеспечить

их профессиональную компетентность в вопросах строительства и развития современных высокотехнологичных систем, в том числе в сфере территориальной обороны государства.

**Литература**


1. Указ Президента РФ от 31 декабря 2015 г. N 683 "О Стратегии национальной безопасности Российской Федерации". [Электронный ресурс] URL: https://base.garant.ru/71296054/ (дата обращения: 16.08.2020).
2. Военная доктрина Российской Федерации (утв. Ук. Президента РФ от 25 дек. 2014 г. № Пр-2976) [Электронный ресурс]. – URL:https://www.rg.ru/2014/12/30/doktrina-dok.html. (дата обращения 16.08.2020).
3. Об обороне: федер. закон от 31 мая 1996 г. № 61-ФЗ (с изм. от 26 июля 2017 г.) [Электронный ресурс]. – URL:https://base.garant.ru/135907/94f5bf092e8d98af576ee351987de4f0/ (дата обращения: 16.08.2020).
4. Злата Заболотских. Искусственный интеллект для бизнеса. Мифы, реальность и стратегия использования. [Электронный ресурс]. – URL:https://ecm-journal.ru/list.aspx?Search=autor::Zlata-Zabolotskikh, 2019 г.
5. Положение о территориальной обороне Российской Федерации (утв. Ук. Президента РФ от 1 июля 2014 г. № 482). [Электронный ресурс]. – Режим доступа: http://base.garant.ru/71296054/(дата обращения: 16.08.2020).
6. Кардаш И.Л. Развитие нормативно-правовой базы территориальной обороны Российской Федерации в современных условиях. –М.: Вестник военного права. – 2018. с.32-38.
7. Органы государственной безопасности в Великой Отечественной войне. – Т. 2. – Кн. 1. – М.: Русь. – 2000. – 724 с.

**Literature**


1. Decree of the President RF of December 31, 2015 N 683 "on the national security Strategy of the Russian Federation". [Electronic resource] URL: https://base.garant.ru/71296054/ (accessed: 16.08.2020).
2. Military doctrine of the Russian Federation (approved by the decree of the President RF from 25 Dec. 2014 no. PR-2976) [Electronic resource]. - URL:https://www.rg.ru/2014/12/30/doktrina-dok.html. (accessed 16.08.2020).
3. About defense: Feder. law of may 31, 1996 No. 61-FZ (with amendments) from July 26, 2017) [Electronic resource]. - URL:https://base.garant.ru/135907/94f5bf092e8d98af576ee351987de4f0/ (accessed: 16.08.2020).
4. Zlata Zabolotskikh. Artificial intelligence for business. Myths, reality, and usage strategy. [Electronic resource]. - URL:https://ecm-journal.ru/list.aspx?Search=autor::Zlata-Zabolotskikh, 2019
5. Regulations on the territorial defense of the Russian Federation (approved by the decree of the President RF of July 1, 2014 no. 482). [Electronic resource]. – Mode of access: http://base.garant.ru/71296054/(accessed: 16.08.2020).
6. Kardash I. L. Development of the legal framework of territorial defense of the Russian Federation in modern conditions. - Moscow: Bulletin of military law. - 2018. pp. 32-38.
7. Organs of state security in the great Patriotic war. - Vol. 2. - Book 1. - Moscow: Rus. - 2000. - 724 p.