Национальная безопасность / nota bene
Правильная ссылка на статью:
Тиханычев О.В. Информатизация поля боя: некоторые возможности и возможные проблемы // Национальная безопасность / nota bene. 2024. № 2. DOI: 10.7256/2454-0668.2024.2.36142 EDN: BSVOXP URL: https://nbpublish.com/library_read_article.php?id=36142

Информатизация поля боя: некоторые возможности и возможные проблемы

Тиханычев Олег Васильевич

ORCID: 0000-0003-4759-2931

кандидат технических наук

заместитель начальника отдела управления перспективных разработок, ГК "Техносерв"

111395, Россия, г. Москва, ул. Юности, 13

to.technoserv@gmail.com

Статья из рубрики "Оперативное реагирование и тактика действий"

DOI:

10.7256/2454-0668.2024.2.36142

EDN:

BSVOXP

Дата направления статьи в редакцию:

21-07-2021

Аннотация: Предметом исследования является информатизация в военном деле, объект исследования – возможные способы управления противником через намеренное и целевое искажение информации о своих войсках, целях и условиях ведения действий. Автор подробно рассматривает такие аспекты современных военных действий, как многодоменность, с существенным смещением акцентов в сферу информационного противоборства. Как показывает опыт локальных войн и вооруженных конфликтов последнего десятилетия, формы их ведения существенно отличаются от "классических" войн, ведшихся до конца XX столетия. Информатизация поля боя позволила перейти к такой форме применения войск (сил) как сетецентрические действия. Но расширение возможностей, совершенствование технологий ведения войны, в соответствии с законами диалектики, порождает и определённые уязвимости. Эти уязвимости проявляются в той же сфере, где находятся сильные стороны – в области информатизации военных действий. Исходя из этого, особое внимание уделяется оценке влияния информатизации на адекватность принимаемых решений, в первую очередь – в

части возможных уязвимостей процесса управления. С использованием общенаучных методов исследования: анализа и синтеза, автором, на основе анализа основных тенденций современного вооруженного противоборства, синтезировано описание возможных уязвимостей при использовании систем автоматизированного управления, сформулирована задача разработки математического аппарата формирования и оценки достоверности информации о противоборствующих системах. Речь идёт не о физическом изменении информации в автоматизированных системах управления противника: эта задача технически сложна, но относительно проста с точки зрения алгоритмизации. И не о тривиальном введении в заблуждении человека, принимающего решения, как это многократно делалось ранее. В статье рассматривается ситуация управления принятием решений через управление направленной подачей информации с использованием уязвимостей её автоматизированной обработки в АСУ. Проблема в данной постановке поднимается впервые.

Ключевые слова:

информатизация поля боя, автоматизация управления, намеренное искажение информации, целевое информационное воздействие, информационное противоборство, управление войсками, принятие решений, современные военные концепции, управление через информацию, введение в заблуждение

Введение

В соответствии с законами диалектики, принципы ведения военных действий меняются под воздействием вновь появляющихся факторов, по мере развития науки и техники. В наше время к таким факторам относятся информатизация военных действий, непрерывный рост защищенности и индивидуальных огневых возможностей отдельных военнослужащих с одновременным повышением точности и могущества действия дальнобойных средств поражения, кардинальное повышение доли высокоточного оружия в боевых действиях [1] и появление нового его типа, который можно определить как «избирательное» или «прецизионное» оружие, поражающего не просто объект, а конкретный его элемент, да ещё осуществляя это по заданной траектории, роботизация поля боя и ряд других. Данные факторы существенно расширяют возможности противоборствующих сторон, повышают динамичность ведения боевых действий, увеличивают эффективность применения войск (сил) и оружия, изменяют требования к логистике и системе управления [2,3,4]. Особенно явно всё это проявляется во влиянии фактора информатизации, являющегося основой для развития большинства вышеперечисленных новаций. В то же время, как показывает исторический анализ, любые новшества, как правило, служат и источником новых проблем и угроз, тем больших, чем больше масштаб этих новшеств [5,6]. Такая ситуация делает актуальным выявление возникающих угроз для формирования возможных путей их локализации.

1.Некоторые особенности влияния информатизации на управление военными действиями

Итак, одной из наиболее очевидных особенностей организации современных военных действий является информатизация поля боя, влияющая практически на все аспекты ведения боевых действий и даже сформировавшая отдельную их сферу – войну в киберпространстве. Сложившаяся в результате расширения сферы действий

многодоменная структура боя (Multidomain battle, MDB) наглядно показывает сущность и содержание возможных преимуществ и потенциальных проблем ведения боевых действий в современных условиях. Как показывает анализ, существенная часть этих проблем определяется процессами получения и обработки информации.

В наиболее явной форме проявление влияния информатизации проявляется в следующих процессах:

- автоматизация сбора данных и обработки информации техническими средствами разведки и управления;

- обобщение и агрегирование данных на основе информации, получаемой от средств разведки, а также систем общего и двойного назначения [7] с использованием технологий больших данных;

- автоматизация выработки управленческих решений и прогнозирования последствий их реализации.

На практике это влияние определяется следующими факторами.

Во-первых, получение информации о противнике и внешних условиях при ведении современных боевых действий, в значительной мере, осуществляется техническими средствами, а обработка данных всё чаще осуществляется программно, с минимальным участием человека. Если раньше практически вся информация, даже полученная без участия человека, обрабатывалась операторами, то с взрывным ростом объёма и динамики получаемых данных, большая часть информации обрабатывается и агрегируется программно-техническими комплексами, которые выдают оператору только результаты анализа. В большинстве случаев - без объяснения алгоритмов выбора и формирования предпочтений.

Во-вторых, само формирование «виртуальной модели» районов боевых действий, представляемых лицу, принимающему решения (ЛПР), осуществляется соответствующими группами штабов (например, в армиях НАТО - Visual Display unit, VDU) с использованием программно-технических комплексов, включающих средства автоматизированного сбора, программного анализа, создания, визуализации и поддержания в актуальном состоянии модели управляемых систем и среды их функционирования на самых разнообразных интерфейсах. Используемые при этом алгоритмы визуализации остаются скрыты от пользователя.

В-третьих, всё больше технических средств разведки и ударных средств, чаще всего беспилотных, оснащаются собственными системами технического зрения, обеспечивающими их применение как в управляемом, так и автономном режиме. Системами, которые построены на собственных, достаточно сложных и, соответственно, потенциально уязвимых алгоритмах.

Все указанные системы и средства, как отмечено ранее, обрабатывают полученную информацию по заранее заданным алгоритмам, выдают её операторам или используют в качестве исходной при расчётах и моделировании для выработки решений. Динамичность современных боевых действий, объём поступающей информации и сложность контроля источников её получения, порождают потенциальную проблему – информация может искажаться, случайно или намеренно. Случайные искажения и возникающие из-за них ошибки – это практически норма в технических системах, неизбежное зло, с которым можно достаточно успешно бороться, для чего имеется

широкий спектр математических методов. А вот намеренное искажение данных, осуществляемое целенаправленно, это проблема, которая может быть тем сильнее, чем больше информации получается от программно-технических средств. Намеренные искажения могут быть неочевидны, что затрудняет противодействие им. Более того, потенциально, эта проблема может создать возможность управлять поведением противостоящей стороны через целенаправленное искажение информации.

Рассматриваемая проблема отражается в форме двух составляющих процесса управления, определяемых степенью участия человека в процессе управления:

- управление техническими системами, как автономное, так и с участием человека-оператора, осуществляемое, как правило, на поле боя и в районах применения;

- управление крупными человеко-машинными системами, разнородными воинскими формированиями и группировками войск.

Оба этих направления нетривиальные и недостаточно исследованы на настоящий момент.

Но если по первому из них ведутся активные исследования в рамках развития робототехники, в первую очередь автономной, то по второй сведений в открытой печати намного меньше, что служит показателем её слабой исследованности. В то же время, данная составляющая процесса управления тоже крайне актуальна, что определяется активным внедрением в управление человеко-машинными (эргатическими) системами компонентов искусственного интеллекта (ИИ).

В статье предлагается рассмотреть именно второй аспект обеспечения надёжности управления в условиях намеренных искажений информации, а именно, управление человеко-машинными системами, реализуемое с применением автоматизированных систем управления (АСУ).

2.О потенциальной возможности управления подачей информации

Ещё раз напомним, что в статье рассматривается не проблема искажения информации путём реализации программно-аппаратных воздействий на автоматизированные системы управления специального назначения (АСУ СН), приводящие к уничтожению или модификации информации в них. Это тема отдельного исследования, очень важного и актуального, но не рассматриваемого в рамках данной статьи [8]. В статье предлагается рассмотреть не менее сложный, но и не менее эффективный вариант целенаправленного искажения информации, являющейся для системы управления входящей, добываемой с целью формирования обстановки, необходимой для дальнейшей оценки и принятия решения, без реализации непосредственного вмешательства в работу компонентов АСУ противостоящей стороны.

Для начала стоить отметить, что большинство перечисленных в первом разделе подходов к добыванию и обработке информации в ходе управления военными действиями применялись и раньше. Например, об использовании дополнительной информации из сторонних источников для принятия решений упоминает ещё генерал Штеменко в книге «Генеральный штаб в годы войны». В июне 1941 года, при отсутствии достоверной информации о продвижении Вермахта, офицеры оперативного управления Генштаба обзванивали директоров колхозов, чтобы по ответам или отсутствию связи определить, хотя бы в общем виде, конфигурацию линии боевого соприкосновения.

В то же время, даже до внедрения компьютеров в управление войсками, использовались

и математические методы агрегирования разведданных и прогнозирование развития обстановки.

Искажение информации, разработка мер введения противника в заблуждение тоже использовались в рамках планирования военных действий довольно давно, с самого начала зарождения военного искусства. Ещё в V веке до нашей эры известный философ Конфуций отмечал, что «война, это путь обмана».

Отличие состоит в том, что на начальном этапе развития военного искусства, речь шла о тактическом обмане противника, использовании разного рода ложных действий для введения его в заблуждение. В дальнейшем, с ростом масштабов боевых действий, когда полководец уже не мог лично обозревать поле сражения, способы введения противника в заблуждение становились всё более разнообразными:

- формирование ложных объектов;

- маскировка объектов и их действий в различных сферах и диапазонах;

- имитационные действия и т.п.

Таким образом, методы введения противника в заблуждение на всех этапах развития военного искусства определялись, в первую очередь, состоянием средств разведки и маскировки, зависели от применяемых методов управления войсками. Пока поле боя можно было обозревать визуально, они были более простыми по содержанию и однозначными по объекту воздействия. С ростом масштабов боевых действий, командующему и штабу пришлось строить виртуальную модель управляемой группировки, группировки противника и среды противоборства на основе сбора данных обстановки. Соответственно, появлялись новые методы противодействия и обмана, по содержанию и объекту развивающиеся от маскировки на поле боя, к оперативной маскировке.

Но, что важно в рамках рассматриваемой проблемы, все эти методы разрабатывались исключительно человеком и против человека.

Реализация указанных методов достаточно наглядно описана в руководящих документах ВС США по методологии планирования введения противника в заблуждение (Military Deception Planning Methodology), которая базируется на структуре типового цикла управления (цикле Бойда в американской терминологии) [9]. Цикл OODA (петля управления Observe - Orient - Decide - Act) в рамках данной концепции модифицирован до формы двухконтурной взаимоувязанной «петли» (рис.1):

- контур управления противником: оценка реакции (See), предположение (Think), воплощение замысла (Do);

- контур действий противника на основе получаемой им информации: регистрация (See), размышление (Think), действие (Do).

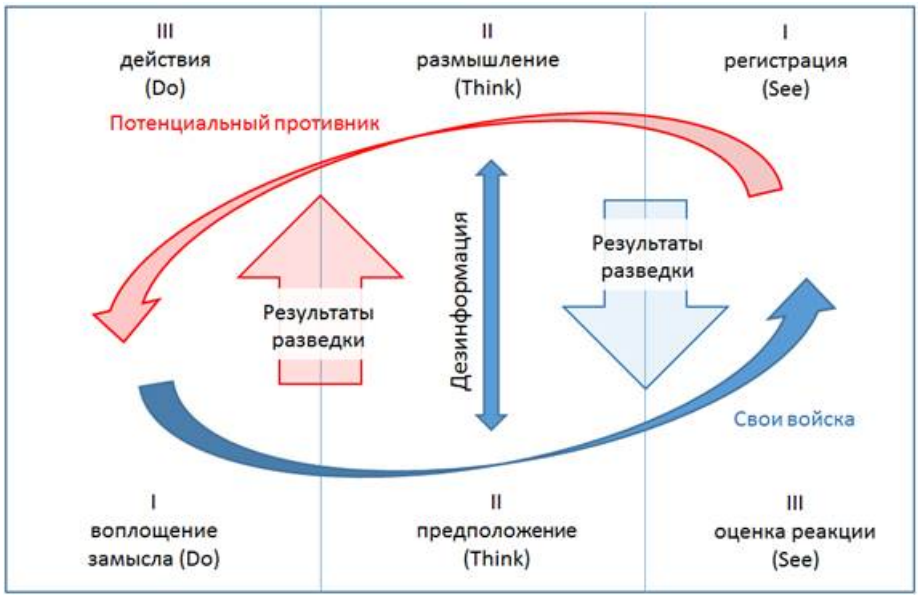

Рис.1. Двухконтурная «петля управления» действиями через дезинформацию

При наличии подтверждённой практической эффективности, отображенный на рисунке 1 алгоритм не в полной мере обеспечивает эффективное использование факторов, возникающих в результате тотальной информатизации поля боя.

Во-первых, в нём, на всех этапах (дезинформация, прогноз и оценки степени соответствия противника замыслу дезинформации), для всех применяемых методов (ложные маневры, демонстративные действия, привлечение внимания и показные действия, влияние через СМИ и социальные сети), рассматривается исключительно воздействие на человека, на управленцев противостоящей стороны, как собирающих, так и анализирующих информацию, принимающих на её основе решения.

Во-вторых, для выработки решений в реализуемом данным алгоритмом, используются субъективные логико-аналитические методы, реализуемые человеком, а не программными средствами поддержки принятия решений.

Документы НАТО, реализующие в практике управления данную методологию[8,9], определяют одним из основных составляющих противоборства информационную борьбу, частью которой являются когнитивные воздействия на ЛПР.

В то же время, обеспеченное информатизацией повышение динамичности военных действий, координированное применение распределённых сил и их усилий в рамках сетецентрических действий, определяют более жесткие требования к оперативности всех этапов цикла управления (петли OODA в терминологии противника): сбора данных, их обработки, планирования, доведения команд, контроля их выполнения [10,11,12]. Это, в свою очередь, ведёт к повышению степени автоматизации управления, к разработке новых, более эффективных, алгоритмов преобразования информации с всё меньшим участием в них человека, как самого медленного звена в процессе обработки данных.

Примером может служить использование специализированных нейронных сетей военного назначения в ВС ведущих в военном отношении государств, например, в армии Израиля. В открытых источниках появилась информация, что в настоящее время в ЦАХАЛ используется система распознавания обстановки и целераспределения на основе ИИ «Евангелие» (она же «Хабзарой» или «Благая весть», ивр. החדשות הטובות), а также программа для планирования ударов авиации Fire Factory. Эти системы не только

выявляют и определяют цели ударов, но и обеспечивают расчёт боекомплекта и формирование графика ударов, что повышает их эффективность. Это, теоретически, расширяет возможность случайного и намеренного искажения информации, служащей исходной для применения таких систем. В последнем случае – для использования с целью управления действиями противостоящей стороны в своих интересах.

Таким образом, по мере информатизации боевых действий и автоматизации управления ими, развитии технических средств разведки, сбора и обработки данных, появляются и новые возможности введения в заблуждение: объектом воздействия которых был уже не только человек, но и технические и программные средства поддержки принятия решений, элементы их информационного и алгоритмического обеспечения.

Исходя из этого, необходим новый методический аппарат планирования информационного воздействия, учитывающий современные особенности информатизации военных действий.

При разработке нового методического аппарата, учитывая развитие АСУ и ИИ в военном деле, нелогично не предусматривать методы воздействия на поддерживающие принятие решений компоненты ИИ, потенциально не менее уязвимые, чем мышление человека.

Ситуация определяется тем, что с расширением использования в АСУ компонентов искусственного интеллекта, потенциально расширяется возможность и диапазон методов ведения противника в заблуждение, дополняясь методами обмана интеллектуальных алгоритмов. Расширение использования в АСУ компонентов ИИ потенциально обеспечивает ещё один фактор уязвимости – как правило, ядро ИИ разработчик АСУ не создаёт, используя готовую «заготовку». Перечень этих заготовок не так велик. Например, для работы с нейросетями это сетевые сервисы: ChatGPT разных версий, Gemini, Baidu ENRIE, YOU, Midjourney, YaLM 100B, Open-Assistant, GitHub Copilot, Aimyvoice, ruDALL-E, Brax, Imagen и другие, каждый из которых предназначен для решения своего класса задач: поиска информации, формирования текста, звука, картинок или видео. В результате возникает потенциальная проблема, о которой уже упоминалось – любая нейросеть работает на статистических данных, обрабатывая их, интерпретируя и формируя на их основе новый результат. Но статистику знает не только планирующая сторона, но и противоборствующая. То есть, эта «игра» может быть двухсторонней: знание особенностей функционирования подобных программ потенциально позволяет, имея некоторую выборку, понять принципы работы алгоритмов, используемых в «движках» ИИ, потенциально реализуемых программным обеспечением АСУ противника. Такая ситуация не делает поставленную задачу тривиальной, а наоборот – актуальной, пусть и сложной, в первую очередь, за счёт неопределённостей в исходных данных.

Но, несмотря на сложность, эта задача решаема. Уже известны отдельные практические разработки по созданию средств введения в заблуждение компонентов искусственного интеллекта. В данном аспекте имеется пример разработки специальных рисунков на основе анализа уязвимостей нейросетевых алгоритмов распознавания изображений, за счёт реализации которых объект, нормально различимый человеком, не распознаётся аппаратно-программными комплексами наблюдения [13].

Более того, в сети Интернет уже сейчас можно найти предложения, содержащие готовые запросы-команды (Prompt) в формате, например, ChatGPT, автоматически переводящие эту нейросеть в другие режимы работы. Более простой и «прямой» вариант воздействия на искусственный интеллект продемонстрировали протестующие из организации Safe

Street Rebel в США – они заставляли остановиться беспилотные автомобили, размещая на их капотах дорожные конусы: программное обеспечение беспилотников воспринимало ситуацию как затор и глушило двигатель.

Это наглядные примеры некоего аналога «нейролептического программирования» для нейросетей. А также, прямое подтверждение того, что технологии дистанционного управления формированием выводов ИИ, без вмешательства в программный код, технически возможны.

Всё перечисленное – частные случаи, но вполне показательные. Существует вероятность, что аналогичные меры могут быть реализованы в более крупном масштабе. И это накладывает дополнительные требования как по защите алгоритмов, так и по разработке подобных средств.

С учётом сложившейся ситуации, сейчас и в обозримой перспективе, с ростом информатизации и роботизации поля боя, для осуществления подобных воздействий открываются новые возможности, они могут принимать совсем другой масштаб и содержание:

- с одной стороны, растёт вероятность получения техническими средствами намеренно искаженной информации и принятия её за истинную;

- с другой стороны, программные средства и методы обработки «больших данных» (Big Data) порождают всё новые возможности по формированию таких искажений.

Ещё раз напомним, речь в статье идёт не о «классическом» введении в заблуждение, а о новых технологиях, потенциально позволяющих через управление подачей информации, используемых программно-техническими комплексами сбора и обработки данных, формировать намеренные искажения обстановки. Искажение точно рассчитанное, обеспечивающие принятие противником заранее спланированных неэффективных для него решений.

3.Общая формулировка задачи

Таким образом, в условиях тотальной информатизации военных действий возникает двуединая научно-практическая задача

Управления информацией, поступающей на вход систем ИИ, используемых в АСУ.

Данная задача логично делится на ряд частных подзадач:

оценки и управления собираемой информацией о составе и действиях противостоящих сторон, решение которой должно обеспечивать:

1) в рамках ведения информационного противоборства, при планировании и принятии решений на его веление:

- спрогнозировать содержание информации, которую может знать противник о наших войсках (силах) и на основании которой им принимаются решения;

- сформировать предложения по намеренному искажению информации, поступающей к противнику по различным каналам, обеспечивать его побуждение к заранее заданным действиям;

- прогнозировать результаты реализации сформированных предложений.

2) в рамках защиты собственной системы управления, в интересах оценки поступающей информации – определять корректность поступающей информации о противнике, своих войсках и условиях ведения боевых действий, оперативно и непрерывно анализировать её на непреднамеренные и намеренные искажения;

Конкретное содержание каждой из задач зависит от уровня, на котором она решается;

- на поле боя, тактическом уровне, основным объектом воздействия будут технические и человеко-машинные средства управления, системы разведки и другие средства добывания информации. Методы воздействия будут преимущественно визуальные, в том числе с применением средств дополненной реальности (augmented reality, AR);

- на уровне ведения операций, где основным объектом информационного воздействия будут штабы, обеспечивающие обработку полученной информации и формирование на её основе решений, представляемых ЛПР, то есть информационно-управляющие системы, с учётом особенностей используемых в них технологий и алгоритмов;

- на стратегическом уровне к указанным методам дополняется воздействие подачей специально подготовленной информации через средства массовой информации, социальные сети и другие компоненты сети Интернет.

В части непосредственно воздействия на ИИ на тактическом уровне, существует, например, задача по введению в заблуждение ЛПР подачей ложной информации с генерацией (подменой) голоса, изображения, а также обратная задача защиты от подобных действий. Можно отметить, что в обычной жизни такие ситуации уже встречаются и известны как «дипфейки» (*deepfake*). Созданы и программные средства для их реализации, такие, например, как нейросеть имитации голоса OpenVoice. Вполне логично и ожидаемо интерпретировать подобные технологии в военную область. Можно отметить, что при достаточно высокой технической сложности, с методологической точки зрения указанные задачи являются тривиальными. Более того, для их решения уже сейчас имеются готовые технологии.

С учётом этого, при всей важности таких задач, в рамках данной статьи они не рассматриваются.

Намного более сложной с методологической точки зрения представляются задачи управления действиями противника через подачу модифицированной информации на оперативном и стратегическом уровне. Данная нетривиальная задача естественным образом делится на подзадачи по формированию выдаваемой информации, прогнозу её влияния на противника и анализу результатов, которые могут быть решены как эвристическими методами, так и с использованием точных математических методов, в том числе известных в настоящее время, хотя и не используемых для решения задач в сформулированной постановке.

Можно ещё раз отметить, что методы повышения достоверности информации об объектах и действиях противника давно известны и используются. Как и методы введения противника в заблуждение. Но, следует заметить, что существующие методы обеспечивают работу с информацией, поступающей от людей, и предназначенной для людей, которая в современных концепциях определяется как «когнитивное воздействие» [9]. В условиях тотальной информации и роботизации этого становится недостаточно. И чем глубже процессы информатизации, роботизации и использования искусственного интеллекта внедряются в сферу вооруженного противоборства, тем менее эффективными становятся существующие методы воздействия на информацию, что делает

сформулированную научно-практическую задачу крайне актуальной. Указанная задача должна быть решена в обязательном порядке любой армией, претендующей на эффективность в современном мире.

Как, в перспективе, может использоваться подобная методология? Представляется вероятным минимум два направления её применения:

- разработка «цифрового портрета» системы противоборствующих сторон и среды противоборства в интересах решения задач, методов модификации информации и управления ей;

- формирование системы противодействия аналогичным действиям противника.

Обе составляющие сформулированной проблемы являются весьма сложными в практической реализации.

Вторая составляющая сформулированной проблемы, на первый взгляд кажущаяся простой и давно решаемой, на самом деле не так тривиальна. Да, она уже сейчас решается проверенными методами: определение достоверности информации подтверждением из нескольких независимых источников, математическими методами фильтрации информации: от простейшего отсечения аномальных результатов до вычислительных методов, например, с использованием коэффициентов конкордации. Но, для работы с намеренно и сложно искажаемой информацией эти методы с высокой вероятностью могут не работать. Тогда для решения проблемы может потребоваться использование более современных подходов, например, на основе искусственного интеллекта. На практике подобные подходы уже используются и апробированы в других областях деятельности. Примерами могут служить интеллектуализированная обработка изображений с использованием состязательных моделей, таких как Clipped BagNet и ResNet, эффективность которой неоднократно подтверждена в теории и на практике, подходы с использованием атак состязательными наклейками различного формата [14] или регуляризацией поступающей информации на основе интерпретируемости [15]. Подходов для обеспечения устойчивости к атакам на компоненты искусственного интеллекта существует достаточно много и, вполне вероятно, что любой из них или их комбинации могут быть реализованы для эффективного противодействия управлению через искажение информации. Самое главное, относительно тематики, рассматриваемой в статье, что такие подходы существуют и развиваются, задача состоит в выборе наиболее эффективных и интерпретации их к условиям применения.

Более сложным представляется вопрос по реализации *первой составляющей сформулированной проблемы,* для которой необходимы принципиально новые подходы к работе органов управления и новые (доработанные) математические методы, то есть нужна разработка методик его применения и выбор или разработка специализированного инструментария.

С точки зрения постановки задачи, в рамках применения подобной методики, необходимо решать обратную задачу: зная или предполагая алгоритм действий противника как «черный ящик», сформировать такой набор входных данных, чтобы получить требуемый набор выходных, определяющих поведение противника.

Собственно, для решения сформулированной задачи может быть использован достаточно широкий спектр имеющегося математического аппарата – от итерационного до оптимизационного. Главной проблемой является формализация ситуации, позволяющая выбрать и использовать для решения задачи необходимый математический аппарат.

Для обеспечения формализации, как один из наиболее очевидных вариантов, может быть использован подход с так называемой «тройкой Хоара», которая описывает предусловия и постусловия, обеспечивающие работу любого конечного алгоритма:

$$\{P\}Q\{S\},$$

где P - предусловия, должные выполняться перед запуском задачи на решение Q;

R - постусловия, истинные после завершения работы реализующей алгоритм задачи, то есть искомое решение

В контексте решения задачи управления действиями противника через информацию, множество Q, это совокупность алгоритмов технических средств разведки и управления противника, обеспечивающие формирование «цифрового портрета» группировки наших войск в условиях её функционирования. А множество P – это матрица данных, состоящая из неизменной части и массива информации, который необходимо сформировать для создания «цифровой модели», обеспечивающей необходимое поведение противника. Результатом решения сформулированной задачи является формирование переменной части множества R.

Впрочем, это лишь один из возможных подходов к формализующих процесса поиска решения, вполне возможен выбор любого другого, подходящего по параметрам.

Далее, как отмечено ранее, при наличии алгоритма, важной частью решения такой задачи является выбор инструментария для её реализации.

Анализ требований к подобному инструментарию показывает, что основными его свойствами должны быть:

- обеспечение оперативность получения решений;

- возможность работы с неполной информацией;

- оперативный учёт быстро меняющихся факторов.

Такими свойствами обладают программно-технические системы, построенные на основе предикативной аналитики, основанные на сборе статистики предыдущих состояний (сценарного анализа, Scenario analysis) и на технологиях машинного обучения (Machine Learning - ML). Указанные технологии могут реализовываться, например, на основе математического аппарата нейросетей, обучаемых с учителем, либо самообучаемых (Unsupervised Learning). Выбор возможного инструментария достаточно широк, выбор конкретного – определятся требованиями пользователя и предпочтениями разработчика.

Таким образом, можно отметить, что уже в настоящее время, сформулированная задача имеет варианты решения, соответствующие методы и инструментарий, не решена только проблема их оценки и выбора.

Определившись с теоретической возможностью решения задачи воздействия на ИИ в составе АСУ, вновь напомним, что ведение противника в заблуждение всегда было частью тактики, оперативного искусства, стратегии.

В истории войн и военного искусства имеются близкие по характеру, но пока ещё планируемые на интуитивном уровне примеры управления информацией: информационная компания по неготовности ВС коалиции к нападению на Ирак в 1991 году [16]. Возможно, имеются признаки применения подобных технологий в ходе ведения

«гибридных» конфликтов последнего десятилетия, но пока конкретно судить рано.

Впрочем, как уже отмечено, это примеры действий, направленных на обман человека или группы людей, хоть и осуществляемые через использование информационных технологий. В статье ставится более «многослойная» задача, воздействие на технические средства добывания, обработки и доведения информации, которые должны формировать нужную информационную картину для своих пользователей.

Задача, как и предполагаемые подходы к её решению, сформулирована впервые и описана в статье в самом общем виде.

И если раньше обман противника был искусством, рассчитанным на человека и направленным на человека, то теперь это может стать наукой, формирующей на основе специализированных методик данные для человека (ЛПР) через воздействие на программные и информационные компоненты управляющих систем, в первую очередь – использующие ИИ. А «классические» методы, разумеется, будут использоваться и впредь. Более того, их эффективность потенциально может возрасти за счёт синергетического эффекта, при использовании в комплексе с предлагаемым в статье подходом.

Подтверждением актуальности сформулированной задачи могут служить изменения в процессе информационного противоборства, которые находят отражение в разрабатываемых концептуальных документах НАТО по развитию вооруженных сил и ведению боевых действий: NATO Warfighting Capstone Concept (NWCC), NATO Artificial Intelligence Strategy, Joint Intelligence, Surveillance and Reconnaissance (JISR) и других. В рамках данной тенденции, например, в ВС НАТО происходит переформирование частей и соединений РЭБ в части «кибер-борьбы», что подразумевает более широкий функционал, переход от воздействия на каналы обмена данными к затруднению использования информации, воздействия непосредственно на неё. Следующий логический шаг в развитии этого процесса – появление функционала по модификации информации, управлению её подачей. Пока этот шаг ещё не сделан, но готовность к появлению новой ситуации должна формироваться уже сейчас.

Исходя из этого, сформулированная в статье задача не только актуальна, но и крайне своевременна.

Заключение

Современный мир активно меняется, эти изменения закономерно отражаются и на ведении вооружённого противоборства. Ориентироваться в сложившихся условиях на использование когнитивных методов информационного противоборства, нацеленных только на принятие решений человеком – значит заранее обречь себя на поражение.

Исходя из этого можно сделать вывод об актуальности сформулированной задачи, основанной на комплексном использовании следующих методов информационного противоборства:

- когнитивные, но не «классические» прямые, а воздействием на промежуточные программно-технические средства обработки информации - «посредники», управлением информацией, обрабатываемой средствами автоматизации управления и ИИ, которые, в свою очередь, готовят информацию для принятия решения человеком;

- информационные, но направляемые не на человека, а воздействующие на управляющие системы на основе ИИ;

- использование классических методов введения в заблуждения с учётом результатов применения двух вышеперечисленных.

Что породит внедрение предлагаемых методов: изменение содержания ведения операций, появление нового вида боевого обеспечения или указанные особенности просто изменят некоторые составляющие существующих форм вооруженной борьбы? А может быть, появится способ преодоления «позиционного кризиса» в современной войне, определяемого многими специалистами как следствие кардинального повышения информационной осведомлённости противоборствующих сторон? Вероятно, сделать окончательный вывод поможет практика.

Впрочем, рассмотренные в статье примеры далеко не исчерпывают приложения методов управления через модификацию информации. Теоретически, они могут использоваться в любой сфере, где есть противоборство: вооруженное, экономическая конкуренция, информационное противоборство и других.

В любом случае, сформулированная в статье научно-практическая задача и предложения по варианту её решения являются важными и актуальными, а решение указанной задачи обеспечит, в том числе, ответы на современные вызовы, порождаемые информатизацией поля боя, а также выработку возможных вариантов действий по ним.

Библиография

1. Литвиненко В., Долматов В. Высокоточные артиллерийские средства огневого поражения // Армейский сборник. 2023. № 7. С. 26-33.
2. Мацуленко В.А. Оперативная маскировка войск (по опыту Великой Отечественной войны). М.: Воениздат. 1975. 200 с.
3. Орлянский В.И. Оперативная маскировка или обман противника // Военная мысль. 2007. № 7. С. 38-45.
4. Бекетов А.А., Белоконь А.П., Чермашенцев С.Г. Маскировка действий подразделений сухопутных войск, М.: Воениздат, 1976. 149 с.
5. Grassegger H., Krogerus M. Ich habe nur gezeigt, dass es die Bombe gibt. Das Magazin. URL: https://www.dasmagazin.ch/2016/12/03/ich-habe-nur-gezeigt-dass-es-die-bombe-gibt/?reduced=true (дата обращения 11.06.2018).
6. Brown Moses How I Accidentally Became An Expert On The Syrian Conflict. Sabotage Times. Jul 20, 2013. URL: https://sabotagetimes.com/life/how-i-accidentally-became-an-expert-on-the-syrian-conflict (дата обращения 11.06.2018).
7. Тиханычев О.В. Интернет-разведка, как одна из угроз информационной эпохи // Вопросы безопасности. 2019. № 2. С. 24-33. DOI: 10.25136/2409-7543.2019.2.26787.
8. Williams Brad D. NSA Renews Focus On Securing Military Weapons Systems Against 'Capable' Rivals. Breaking Defense. October 07, 2021. https://breakingdefense.com/2021/10/nsa-ups-focus-on-securing-weapons-systems-amid-capable-multipolar-rvials/
9. JP 3-13.4 Military Deception. Joint Chiefs of Staff , 2017. 108 p.
10. Чекинов С. Г., Богданов С. А. Эволюция сущности и содержания понятия «война» в XXI столетии // Военная Мысль. 2017. № 1. С. 30-43.
11. Бартош А.А. Модель гибридной войны // Военная мысль. 2019. № 5. С. 6-23.
12. Першин Ю.Ю. Гибридная война: много шума из ничего // Вопросы безопасности. 2019. № 4. С. 78-109. DOI: 10.25136/2409-7543.2019.4.30374.
13. Тиханычев О.В, Тиханычева Е.О. Обеспечение скрытности объектов при ведении вооруженных конфликтов различной интенсивности, как важный аспект их защиты: история, состояние, развитие процесса // Вопросы безопасности. 2023. № 4. С.126-151.

DOI: 10.25136/2409-7543.2023.4.39371.
14. Курденкова Е.О., Черепнина М.С., Чистякова А.С., Архипенко К.В. Влияние трансформаций на успешность состязательных атак для классификаторов изображений Clipped BagNet и ResNet. Труды ИСП РАН, том 34, вып. 6, 2022 г., стр. 101-116. DOI: 10.15514/ISPRAS-2022-34(6)-7.
15. Chistyakova A., Cherepnina M., Arkhipenko K., Kuznetsov S., Oh C.-S. and Park S., "Evaluation of interpretability methods for adversarial robustness on real-world datasets," *2021 Ivannikov Memorial Workshop (IVMEM)*, Nizhny Novgorod, Russian Federation, 2021, pp. 6-10. DOI: 10.1109/IVMEM53963.2021.00007.
16. Горохов Р.Ю. Развитие теории и практика маскировки в вооруженных силах США // Военная мысль, 2022. № 8. С. 147-156.

Результаты процедуры рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.
Со списком рецензентов издательства можно ознакомиться здесь.

Статья представляет собой глубокий анализ влияния информационных технологий на современные военные действия, с акцентом на их преимущества и потенциальные риски. Автор использует комбинацию исторического анализа, современных примеров и теоретического обсуждения для исследования эволюции военных тактик под влиянием технологических достижений, включая интеграцию искусственного интеллекта и больших данных в военную стратегию. Тема актуальна в современном цифровом мире, особенно в контексте пересечения информационных технологий и военных операций. Статья выделяется научной новизной, предлагая оригинальный взгляд на преимущества информатизации и критически оценивая потенциальные уязвимости и вызовы. Стиль академический, структура хорошо организована, а содержание подходит для научной аудитории. Обширная библиография отражает глубокое погружение автора в тему. Автор эффективно рассматривает возможные контраргументы, особенно касающиеся надежности и безопасности технологий в войне. В статье приводится интересный анализ модификации цикла OODA в рамках современной военной стратегии. Автор адаптирует традиционную концепцию OODA (Observe - Orient - Decide - Act) к условиям информационной войны, представляя ее в форме двухконтурной взаимоувязанной "петли". Первый контур описывает управление противником через оценку его реакции (See), формирование предположений (Think) и воплощение замысла (Do). Второй контур отражает действия противника, основанные на получаемой им информации, включая регистрацию (See), размышление (Think) и выполнение действий (Do). Эта модификация цикла OODA подчеркивает сложность и взаимосвязь информационных войн в современном мире. Кроме того, автор затрагивает крайне актуальную тему уязвимости систем автоматизированного управления (АСУ) в контексте использования компонентов искусственного интеллекта (ИИ). Он глубоко анализирует, как расширение использования ИИ в АСУ может привести к новым методам обмана и введения в заблуждение, как со стороны противника, так и в плане защиты. Это освещение потенциальных уязвимостей, вызванных ограниченным выбором базовых компонентов ИИ, представляет собой значительный вклад в понимание современных военных стратегий и информационной безопасности. Такой анализ подчеркивает сложность и многогранность проблемы, делая исследование особенно ценным и актуальным. Выводы подчеркивают необходимость постоянной адаптации военной стратегии для преодоления вызовов, связанных с информатизацией, что делает статью интересной для читателей, интересующихся военной стратегией, информационными технологиями и

исследованиями безопасности. В качестве развития данной работы можно предложить интеграцию дополнительных реальных примеров использования искусственного интеллекта в военных целях, что укрепит аргументацию и предоставит более глубокий анализ. Освещение конкретных технологий ИИ в военных системах автоматизированного управления усилит понимание их роли в военной стратегии. Важным аспектом также станет исследование стратегий противодействия угрозам, связанным с ИИ. Включение этических и социальных аспектов применения ИИ в военной сфере обогатит работу с точки зрения мультидисциплинарности. Кроме того, описание потенциальных будущих тенденций и сценариев в военных технологиях на основе ИИ поможет читателям лучше понять возможные последствия их применения. В целом, статья представляет собой продуманный анализ пересечения технологий и военных операций, выделяя важные аспекты для современной стратегии ведения войн.