УДК 519.711.3

doi: 10.53816/23061456_2025_3–4_17

ОБЕСПЕЧЕНИЕ ИССЛЕДОВАНИЙ ПЕРСПЕКТИВ РАЗВИТИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ В УСЛОВИЯХ СЕТЕЦЕНТРИЧЕСКОЙ ПАРАДИГМЫ УПРАВЛЕНИЯ

PROVIDING RESEARCH ON THE PROSPECTS FOR THE DEVELOPMENT OF AUTOMATED CONTROL SYSTEMS IN A NETWORK-CENTRIC MANAGEMENT PARADIGM

Д-р техн. наук В.А. Кежаев[1], канд. техн. наук М.М. Макаров[1], канд. техн. наук А.М. Сазыкин[2]

D.Sc. V.A. Kezhaev, Ph.D. M.M. Makarov, Ph.D. A.M. Sazykin

[1]Военно-космическая академия им. А.Ф. Можайского, [2]НПО Спецматериалов

В статье рассматриваются актуальные и проблемные вопросы обеспечения исследований, касающихся перспектив развития автоматизированных систем управления. Особое внимание уделяется современным системам управления войсками и оружием, особенно в условиях сетецентрической парадигмы управления и информационного противоборства. В тексте приводятся характерные особенности функционирования системы управления в условиях информационного противоборства, а также воздействие на нее случайных факторов, которые могут существенно влиять на эффективность работы этих систем. Кроме того, предлагается один из вариантов исследования особенностей функционирования подобных систем в условиях деструктивного воздействия со стороны противника, что является важным аспектом для повышения их устойчивости и надежности.
Ключевые слова: автоматизированная система управления, сетецентрическая парадигма управления, информационное противоборство, факторы стохастической природы.

This article discusses current and problematic issues of research support related to the prospects for the development of automated control systems. Special attention is paid to modern systems of command and control of troops and weapons, especially in the context of a network-centric management paradigm and information warfare. The text presents the characteristic features of the functioning of the management system in the context of information warfare, as well as the impact of random factors on it, which can significantly affect the efficiency of these systems. In addition, one of the options for studying the features of the functioning of such systems in conditions of destructive influence from the enemy is proposed, which is an important aspect to increase their stability and reliability.
Keywords: automated control system, network-centric management paradigm, information warfare, stochastic factors.

Результаты анализа состояния вопросов обеспечения научных исследований перспектив развития автоматизированных систем управления (АСУ) в условиях сетецентрической парадигмы управления и информационного противоборства свидетельствуют о возникновении

проблемной ситуации в данной области [1–3]. Предпосылки её формирования связаны с качественными преобразованиями в военной сфере, которые происходили в последние десятилетия. В первую очередь они затронули системы управления войсками и оружием, как важнейший компонент АСУ специального назначения [4, 5]. Это обусловлено кардинальными изменениями в теории управления, вызванными бурным развитием информатизации всех областей военного дела [6].

В дальнейшем, для простоты изложения, под информационным противоборством будем понимать процесс согласованных по цели и месту организационно-технических мероприятий, которые проводятся сторонами вооруженного конфликта для взаимной дезорганизации информационного обеспечения АСУ с целью срыва выполнения боевых задач.

В частности, одной из сложных задач информационного противоборства является необходимость учета случайного характера длительности воздействия на систему управления внешних факторов, имеющих стохастическую природу [7, 8]. При этом следует учитывать, что основная трудность связана не только с определением вероятности своевременного обнаружения атаки на элементы системы управления. В первую очередь необходимо определить вероятность своевременной готовности средств её защиты к отражению несанкционированного доступа к элементам системы управления. Для этого, естественно, важно знать вероятность того, что отрезок времени от момента обнаружения до момента блокировки деструктивных действий окажется больше времени, затрачиваемого на выработку соответствующего управляющего воздействия по парированию этих действий.

Эффективность функционирования системы управления в условиях информационного противоборства и воздействия на нее случайных факторов в значительной степени зависит от множества параметров, зависящих, как правило, от особенностей состава и структуры данной системы [3]. Поэтому в процессе определения целей и задач обеспечения научных исследований перспектив развития АСУ необходимо:

– во-первых, руководствоваться принципами системного подхода [9] на всех этапах исследования;

– во-вторых, учитывать характеристики систем и особенности их функционирования в условиях сетецентрической парадигмы управления и информационного противоборства.

Поэтому рассмотрим некоторые характерные признаки АСУ, которые, на наш взгляд, в значительной степени влияют на качество и полноту научных исследований, перспектив их развития в современных условиях (табл. 1).

Таблица 1

Характерные особенности АСУ (на примере систем управления)

№ п.п.	Характерные особенности, влияющие на идентификацию систем специального назначения	Звено управления
1	Степень защищенности системы управления в значительной степени определяется интенсивностью информационного противоборства и его количественно-качественными параметрами в ходе боевых действий	Оперативное, тактическое
2	Сведения, поступающие в систему, имеют, как правило, противоречивый характер, являются разнородными по своей природе и разновидовыми	Оперативное
3	Информация, подлежащая обработке, передаче и распределению носит закрытый характер, что требует дополнительных ресурсов (вычислительных, временных, материальных и т.д.) по поддержанию такого режима во всем спектре решаемых задач управления	Оперативное, тактическое
4	Для обработки входных данных, наряду с регулярными методами, необходимо дополнительно разрабатывать специальные модели, методы и методики, позволяющие в масштабе реального времени оперативно обеспечивать информационную поддержку деятельности должностных лиц органов управления всех звеньев	Оперативное

Таблица 1 (продолжение)

№ п.п.	Характерные особенности, влияющие на идентификацию систем специального назначения	Звено управления
5	Возможность оперативного получения информации из смежных предметных областей, сфер военных действий жестко регламентирована и крайне ограничена правилами разграничения доступа к соответствующим информационным массивам	Оперативное
6	Топология связей между источниками информации, пунктами управления формирований различных звеньев управления является динамичной, в значительной степени зависящей от интенсивности боевых действий, фортификационного оборудования местности, театра военных действий (операционного направления)	Оперативное, тактическое
7	Свойства системы обычно трудно идентифицировать с достаточной степенью точности. Возникает необходимость решения проблемы анализа динамики функционирования системы. Более того, если даже удается выявить у нее свойство эргодичности, то и в этом случае такую систему оценивать с помощью классических статистических методов крайне сложно. Это вызвано тем, что статистическая выборка, как правило, оказывается очень малой	Оперативное
8	Потребность периодически выполнять мероприятия, связаные с:	
	анализом задач комплексной обработки информации различных видов (текстовой, видовой, иконографической и др.);	Оперативное, тактическое
	описанием моделей потоков информационных документов, а также основных элементов процесса комплексной обработки: селекции информационных (идентификационных) признаков, формирования совокупностей этих признаков и их дальнейшей интерпретации;	Оперативное
	модификацией методик построения информационных структур для комплексной обработки специальной информации в условиях дефицита времени	Тактическое

В случае фиксированного значения длительности воздействия T (речь идет о внешних факторах стохастической природы) на систему управления, вероятность своевременного обнаружения $P_{\text{со}}(t)$ можно определить с помощью выражения

$$P_{\text{со}}(t)=\begin{cases}1-e^{-\sum\limits_{i=1}^{k}\lambda_i P_{\text{об}i}(T-t)}, & \text{если } T>t;\\ 0, & \text{если } T\le t,\end{cases}$$

где t — время, прошедшее от момента обнаружения атаки до начала её блокировки;

T — продолжительность воздействия на систему управления;

λ_i — частота мониторинга атак на систему управления;

$P_{\text{об}i}$ — вероятность обнаружения атаки i-м средством защиты;

k — число средств, участвующих в мониторинге возможных атак на систему управления.

С учетом случайного характера длительности атаки на систему управления, вероятность своевременного обнаружения является функцией времени, определяемой в соответствии с выражением

$$P^{*}_{\text{об}i}(t)=\int_{t}^{\infty}P_{\text{об}}(t)\,\tau(t)\,dt, \qquad (1)$$

где $P_{\text{об}}(t)$ — вероятность обнаружения атаки в момент времени t;

$\tau(t)$ — длительность атаки в момент времени t.

Опыт эксплуатации систем управления позволяет утверждать, что продолжительность атаки на систему управления определяется достаточно большим количеством случайных факторов, ни один из которых не имеет превалирующего значения [7, 8]. Поэтому можно принять допущение о нормальном законе распределения случайной величины T.

Подставив в выражение (1) функцию плотности нормального закона распределения случайной величины, после преобразований получим выражение для определения вероятности

своевременного обнаружения атаки на систему управления

$$P^{*}_{\text{со}}(t) = 1 - F\left(\frac{t - m_T}{\sigma_T}\right) - \exp\Lambda\left(t + \frac{\sigma_T^2\Lambda}{2} - m_T\right) \times \left[1 - F\left(\frac{t + \sigma_T^2\Lambda - m_T}{\sigma_T}\right)\right], \quad (2)$$

где m_T — математическое ожидание продолжительности атаки на систему управления;

σ_T — среднеквадратическое отклонение продолжительности атаки на систему управления;

$F(\cdot) = \int_{-\infty}^{x} \frac{1}{\sqrt{2\pi}} e^{\frac{t^2}{2}} dt$ — табулированная функция.

Выражение (2) позволяет определять значение показателя своевременности обнаружения атаки на систему управления в любой момент времени. Важно отметить, что благодаря предложенному варианту расчета данного показателя удается сохранить связь между системой обнаружения атаки и системой блокирования (отражения) атаки.

Предлагая варианты обеспечения научных исследований перспектив развития АСУ, безусловно необходимо принимать во внимание достижения армий высокоразвитых стран в данной области. Результаты изучения и анализа доктринальных и уставных документов армий ведущих зарубежных стран позволяют сделать вывод о том, что:

– во-первых, базой для реализации современных концепций управления является сетевая информационная разведывательно-управляющая структура;

– во-вторых, все сетецентрические концепции армий ведущих зарубежных стран реализуются путем организации взаимодействия и объединения разрозненных подсистем в единую структуру через развертывание «системы сетей». Такая организация взаимодействия подразумевает не только объединение в техническом смысле, но и организацию когнитивного взаимодействия между системами и органами управления;

– в-третьих, все существующие и перспективные разработки в этой области направлены на достижение доминирования в информационном противоборстве с любым противником, обладающим высокотехнологичными системами управления.

Сравнительная оценка тенденций развития поисковых и исследовательских работ различного характера показывает, что стремление разработать научно-методические положения совместного моделирования функционирования систем управления в инфокоммуникационном пространстве и их защиты в условиях информационного противоборства становится все более очевидным [3]. Поэтому в ближайшем будущем следует ожидать появления новых проблем в области управления, связанных, в первую очередь, с необходимостью решения задач обеспечения защиты подобных систем, с учетом интенсивного информационного противоборства в режиме реального времени.

Поэтому не случайно в Военной доктрине РФ [10] ставится конкретная задача «…создание базовых информационно-управляющих систем и их интеграция с системами управления оружием и комплексами средств автоматизации органов управления стратегического, оперативно-стратегического, оперативного, оперативно-тактического и тактического уровней». Благодаря такой интеграции результаты противоборства могут быть сравнимы с результатами применения группировок Сухопутных войск.

Учитывая тенденции развития информационного противоборства, а также направления совершенствования научно-методических положений в области управления, следует ожидать кардинальных изменений в данной области. При этом достаточно сильное влияние на развитие взглядов и концепций противоборства в современную эпоху будет оказывать глубокая интеграция задач информационного противоборства и технологии моделирования процессов, реализующих сетецентрическую парадигму управления [2]. Большинство армий зарубежных государств целенаправленно делают ставку на развитие информационной составляющей в действиях конфликтующих сторон. Согласно этой концепции, основные ресурсы сосредоточиваются на разработке самых передовых, высокоэффективных технологий, способствующих созданию качественно нового потенциала у участников конфликта.

Как показывает анализ публикаций в зарубежных источниках, разрешением данных

проблем глубоко и целенаправленно занимаются военные специалисты многих стран. Об этом свидетельствует, в частности, характер и интенсивность работ, проводимых в этой области специалистами передовых в экономическом отношении стран. Так, руководство США в процессе «революционной военной трансформации» активно внедряет в практику управления перспективные информационные технологии и моделирование. Некоторые из таких примеров описаны в источниках, список которых приведен в статье [11]. Обобщая и систематизируя эти сведения, можно констатировать, что основные усилия военных специалистов сводятся к разработке:

– перспективных информационных технологий управления в прогнозируемых столкновениях конфликтующих сторон;

– высокотехнологичных комплексов, ориентированных на применение в условиях сетецентрических действий;

– инновационных принципов применения различных средств физического воздействия непосредственно на системы управления в сочетании с активизацией работ по информационному противоборству.

Учитывая степень концентрации усилий на разработке перечисленных научных направлений, необходимо в первую очередь обратить внимание на некоторые характерные аспекты технологий исследования систем управления, основные из которых представлены в табл. 2.

Перечисленные задачи активно реализуются, трансформируясь в приоритетные направления реформирования различных структур стран-участников потенциальных конфликтов. В процессе данных изменений непрерывно совершенствуются формы и способы информационного противоборства. При этом удалось обнаружить и новые тенденции, присущие сетецентрическому управлению и его влиянию на эффективность ведения информационного противоборства. Об этом свидетельствует, в частности, то, что:

– реализуется принцип поражения систем управления путем бесконтактного воздействия на её подсистемы. Вместо физического уничтожения систем управления осуществляется переход к активному информационному противоборству, в ходе которого дезорганизуется процесс управления уже на дальних подступах к боевым порядкам войсковых формирований;

– информационные атаки на системы управления осуществляются в случайные моменты времени во всем диапазоне их функционирования и из разных сред (суша, воздух, вода, космос).

Таблица 2

Основные тенденции внедрения информационных технологий в разработку систем управления

№ п.п.	Современные тенденции внедрения информационных технологий в разработку систем управления специального назначения
1	Декларация операции «революционной военной трансформации» в соответствии с новыми принципами: – обеспечение реальной интеграции действий разновидовых группировок, использующих сетецентрическую систему управления; – использование открытой архитектуры и модульности построения систем и комплексов реализации всех задач противоборства, позволяющих им оперативно адаптироваться к любым условиям действий; – реализация идеи вертикальной и горизонтальной взаимосвязи и взаимодействия участников конфликта во всем спектре выполняемых задач и во времени, близком к реальному
2	Безусловное достижение главных целей, имеющих принципиальное значение для развития перспективных исследований: – повышение уровня взаимодействия между отдельными подсистемами каждой из сторон, применяющих различные способы защиты систем управления, в условиях единого информационного пространства; – достижение качественно нового эффекта за счет реализации принципов сетецентрических концепций и интеграции отдельных подсистем управления со средствами и методами защиты информации в единую систему; – обеспечение системной интеграции усилий всех проектировщиков, разработчиков и специалистов в области защиты систем управления в условиях информационного противоборства

Заключение

Таким образом, в современных условиях в армиях экономически развитых стран активно реализуется сетецентрическая парадигма управления. Благодаря этому актуальным становится поиск новых методов решения проблем обеспечения исследований перспектив развития АСУ в условиях сетецентрической парадигмы управления и информационного противоборства. Особое внимание необходимо уделять развитию систем управления, которые реализуют сложнейшую функцию интеграции систем поражения, разведки и боевого обеспечения в ходе военных действий во всех средах. Поэтому в эпоху информационного противоборства конфликтующих сторон вопросы защиты систем управления специального назначения требуют пристального внимания.

Интеграция задач информационного противоборства в технологию защиты процессов, реализующих сетецентрическую парадигму управления, будет способствовать:

– достижению устойчивого информационно-управленческого превосходства над противником в течение времени, необходимого для победы;

– удержанию инициативы в ходе всего цикла управления, реализуемого соответствующей системой;

– сохранению информационного потенциала, информационных ресурсов для достижения поставленных целей;

– реализации фактора внезапности в ходе решения задач управления с минимальными потерями ресурсов.

Список источников

1. Герасимов В.В. Организация обороны Российской Федерации в условиях применения противником «традиционных» и «гибридных» методов ведения войны // Вестник Академии военных наук. 2016. № 2. С. 19–24.

2. Воронцова Л.В., Фролов Д.Б. История и современность информационного противоборства. М.: Горячая линия-Телеком, 2006. 192 с.

3. Буренок В.М., Мельников И.Д. Информационное обеспечение автоматизированных систем обоснования перспектив развития вооружения и военной техники // Военная мысль. 2002. № 5 (9–10). С. 42–46.

4. Кузнецов Н., Расчислов А. Некоторые аспекты совершенствования системы управления общевойскового формирования нового облика // Военная мысль. 2010. № 6. С. 11–15.

5. Выпасняк В.И. О реализации сетецентрических принципов управления силами и средствами вооруженной борьбы в операциях (боевых действиях) // Военная мысль. 2009. № 12. С. 23–30.

6. Кежаев В.А., Кулешов Ю.В., Суровикин С.В. Актуальные проблемы развития теории управления группировками войск (сил) в интересах повышения эффективности огневого поражения противника с целью локализации международного вооруженного конфликта // Известия Российской академии ракетных и артиллерийских наук. 2018. № 1 (100). С. 24–32.

7. Левкин И.М. Комплексная обработка информации: монография. СПб.: ВКА им. А.Ф. Можайского, 2011. 271 с.

8. Мануйлов Ю.С., Новиков Е.А. Концептуальные основы управления в условиях неопределенности. СПб.: ВКА им. А.Ф. Можайского, 2008. 121 с.

9. Калинин В.Н. Теоретические основы системных исследований: учебник. СПб.: ВКА им. А.Ф. Можайского, 2016. 293 с.

10. Военная доктрина Российской Федерации // Российская газета — Федеральный выпуск № 6570 (298). 30.12.2014.

11. Brown G.G., Washburn A.R. The Fast Theater Model (FATHM) // Military Operations Research. 2007. V. 12. № 4. Pp. 33–45.

12. Сурма И.В., Анненков В.И., Карпов В.В., Моисеев А.В. «Сетецентрическое управление»: современная парадигма развития системы управления в вооруженных силах ведущих держав мира // Национальная безопасность. 2014. № 2 (31). С. 317–327.

13. Синявский В.К. Парадигма сетецентрического управления и её влияние на процессы управления войсками (силами) // Информационно-измерительные и управляющие системы. 2021. Т. 19. № 6. С. 37–44.

14. Соколов А.В. От «Ясеня» до «Акации» и «Созвездия». Создание и совершенствование отечественных автоматизированных систем управления войсками и оружием // Военно-исторический журнал. 2021. № 2. С. 4–9.

References

1. Gerasimov V.V. The organization of defense of the Russian Federation in the conditions of the enemy's use of «traditional» and «hybrid» methods of warfare // Bulletin of the Academy of Military Sciences. 2016. No 2. Pp. 19–24.

2. Vorontsova L.V., Frolov D.B. History and modernity information warfare. M.: Hotline-Telecom, 2006. 192 p.

3. Burenok V.M., Melnikov I.D. Information support of automated systems for substantiating the prospects for the development of weapons and military equipment // Military Thought. 2002. No 5 (9–10). Pp. 42–46.

4. Kuznetsov N., Raschislov A. Some aspects of improving the management system of the combined arms formation of a new look // Military thought. 2010. No 6. Pp. 11–15.

5. Vypasnyak V.I. On the implementation of network-centric principles of control of forces and means of armed struggle in operations (combat operations) // Military Thought. 2009. No 12. Pp. 23–30.

6. Kezhaev V.A., Kuleshov Yu.V., Surovikin S.V. Actual problems of the development of the theory of control of groups of troops (forces) in the interests of increasing the effectiveness of enemy fire damage in order to localize an international armed conflict // Proceedings of the Russian Academy of Rocket and Artillery Sciences. 2018. No 1 (100). Pp. 24–32.

7. Levkin I.M. Complex information processing: monograph. St. Petersburg: A.F. Mozhaisky VKA, 2011. 271 p.

8. Manuilov Yu.S., Novikov E.A. Conceptual foundations of management in conditions of uncertainty. St. Petersburg: A.F. Mozhaisky VKA, 2008. 121 p.

9. Kalinin V.N. Theoretical foundations of system research: textbook. St.Petersburg: A.F. Mozhaisky VKA, 2016. 293 p.

10. Military doctrine of the Russian Federation // Rossiyskaya gazeta — Federal issue № 6570 (298), 30.12.2014.

11. Brown G.G., Washburn A.R. The model of a rapid theater of military operations (FATHM) // Military Operations Research. 2007. Vol. 12. No 4. Pp. 33–45.

12. Surma I.V., Annenkov V.I., Karpov V.V., Moiseev A.V. «Network-centric management»: a modern paradigm for the development of the management system in the armed forces of the world's leading powers // National Security. 2014. № 2 (31). Pp. 317–327.

13. Sinyavskiy V.K. Paradigm of network-centric management and its impact on the processes of troop (force) management // Information-measuring and control systems. 2021. T. 19. № 6. Pp. 37–44.

14. Sokolov A.V. From «Yasen» to «Acacia» and «Constellation». Creation and Improvement of Domestic Automated Systems of Troops and Weapons Control // Military History Journal. 2021. № 2. Pp. 4–9.