

Станкевич Антон Сергеевич,
курсант 3 курса
Научный руководитель Милашевский А. В.,
кандидат технических наук, доцент
Учреждение образования
«Гродненский государственный университет имени Янки Купалы»,
г. Гродно, Республика Беларусь

ЭВОЛЮЦИОННЫЕ ТРАНСФОРМАЦИИ СЕТЕЦЕНТРИЧЕСКОЙ ВОЙНЫ: ПРЕДПОСЫЛКИ И ПЕРСПЕКТИВЫ РАЗВИТИЯ В КОНТЕКСТЕ СОВРЕМЕННЫХ УГРОЗ И ВЫЗОВОВ

Аннотация. Статья посвящена анализу концепции сетецентрической войны, ее предпосылкам, теоретическим основам и технологическим аспектам реализации в зонах актуального и перспективного развития. Проведен анализ руководящих документов министерства обороны США, зарубежных и отечественных изданий, посвященных феномену сетецентрической войны. Рассматриваются ключевые идеи, заложенные в развитие концепции в конце XX века, особенности реализации, а также принципы интеграции данных и автоматизации управления в современных вооруженных конфликтах. Раскрыты ее сущность и особенности ведения, проанализированы основные направления развития сетецентричных систем, их влияние на тактику и стратегию ведения боевых действий, а также перспективы внедрения передовых технологий. Особое внимание уделено научным подходам к моделированию, системному анализу и нормативному регулированию предметной области, способствующим повышению эффективности и вооруженных противостояний современности.

Ключевые слова: сетецентризм, инфосфера, цикл управления, самосинхронизация, вооруженный конфликт.

В условиях современного динамичного развития научно-технического прогресса и глобализации в военной сфере наблюдается постепенный переход от традиционных форм и методов ведения боевых действий к инновационным концепциям, основанным на использовании информационных и коммуникационных технологий. Одной из наиболее актуальных и широко исследуемых концепций является сетецентрическая война, представляющая собой моделирование и реализацию боевой деятельности с опорой на интеграцию информационных систем, средств автоматизации и сетевой инфраструктуры.

Данная концепция обусловлена необходимостью повышения эффективности управления вооруженными силами, ускорения процессов принятия решений, а также расширения возможностей по сбору, обработке и распространению разведывательной информации в реальном времени. В результате формирования сетецентрических систем увеличивается оперативно-тактическое

и стратегическое превосходство, что обуславливает существенные сдвиги в теоретическом и практическом аспектах военной деятельности.

Истоки развития концепции сетецентрической войны насчитывают более двух десятилетий, однако свои корни она берет из концептуальных предпосылок, сформулированных в конце XX века. Значительный вклад в организацию научного подхода внес вице-адмирал Артур Цебровски и его коллеги, в статье 1998 года под названием «Сетецентрическая война: истоки и перспективы» [2], обозначившей рубежи современной теории информационного превосходства в военном деле.

Цебровски аргументировал, что современные вооруженные конфликты уже не могут рассматриваться с позиции классических платфоцентрических концепций, поскольку развитие технологий существенно изменяет баланс сил и управляемости. Он предложил рассматривать боевые системы как составляющие единых информационных сетей, в которых интеграция данных, автоматизация процессов и обмен информацией в реальном времени становятся ключевыми факторами успеха. Идея о полном переходе от платформенно-ориентированной тактики к сетевой военной стратегии представляет собой революцию в методах ведения боевых действий, аналогичную промышленной революции в XIX веке.

Дополнительно в рамках концепции были опровержены идеи о роли отдельных элементов вооружения и техники, а также подчеркнута значимость взаимосвязи всех систем и подсистем через концепцию информационно-управляемых сетей. Данное направление активно развивалось при поддержке концепций футуристов Элвина Тоффлера и Хайди Тоффлера, которые в своих работах отразили трансформационные изменения, связанные с переходом от индустриальной к информационной эпохе.

На научном уровне особое внимание уделяется исследованиям в области информационных технологий, систем управления, кибербезопасности и сетевых коммуникаций. В рамках современного научного дискурса подчеркивается принципиальное отличие сетецентрической системы от традиционных военных сетей: не только в использовании технологий, но и в моделях организации взаимодействия, принципах обмена данными и уровнях автоматизации.

Ключевыми компонентами современных систем являются [3–4]:

информационное превосходство, означающее способность своевременного сбора, обработки и распространения разведывательных данных;

интегрированные системы управления, связывающие различные роды войск и военные формирования в единую сетевую инфраструктуру;

автоматизация процессов принятия решений, которая сокращает временные циклы реакции и усиливает динамичность вооруженных систем;

киберзащита и информационная безопасность, обеспечивающие устойчивость систем к внешним и внутренним угрозам.

Реализация указанных принципов достигается посредством внедрения современных информационно-коммуникационных технологий, таких как широкополосные коммуникационные сети, системы спутниковой связи, системы

автоматизированного управления, системы раннего оповещения и обмена разведанными в реальном времени. Кроме того, в рамках научных исследований большое внимание уделяется моделированию, симуляции и прогнозированию поведения сложных военных систем на базе теорий системной динамики и вычислительной математики.

Одним из краеугольных камней теории сетецентрической войны является признание принципа высокой динамичности боевых ситуаций и необходимости быстрого принятия решений. В этом контексте ключевым является не только наличие информации, но ее эффективное использование, а также минимизация временных и ресурсных затрат.

Научная концепция подчеркивает, что достижение превосходства достигается за счет:

- информационного доминирования – концентрации и быстрого распространения разведывательной информации;

- комбинированного эффекта – интеграции разнотипных систем, средств и сил в единое боевое пространство, позволяющее реализовать синергетический эффект;

- лишения противника возможности управления – осуществляется за счет быстрого реагирования и введения дезорганизации в его системы командования и связи.

В рамках теоретических исследований особое значение уделяется системному анализу, теории сложности и вычислений. Использование этих подходов позволяет построить модели, учитывающие как состоящие из элементов системы, так и взаимодействия между ними, а также выявить факторы, критичные для обеспечения высокой боеспособности в условиях информационной войны.

В рамках совокупного научного анализа выделяются основные тенденции, усиливающие роль сетецентричности военных операций:

- переход к информационной эпохе, характеризующийся увеличением объемов, скорости и сложности обрабатываемых данных;

- расширение диапазона угроз и сложности условий ведения боевых действий, включая кибервойны, информационные операции и гибридные конфликты;

- интеграция новых технологий, в частности, искусственного интеллекта, автоматических систем распознавания образов, робототехники и спутниковых систем.

Научные исследования в данном направлении сосредоточены на моделировании системной архитектуры, разработке протоколов взаимодействия и обеспечении отказоустойчивости систем управления.

На практике концепция сетецентрической войны реализуется через стратегические программы развития вооруженных сил, корпоративные стандарты и нормативные документы. В США, например, компетентными органами были подготовлены специальные руководства, регламентирующие использо-

вание информационно-коммуникационных систем, организацию элементов системы командования и контрольных точек.

Однако в нормативных документах отсутствует универсальное и однозначное определение понятия «сетевая война», что создает сложности в стандартизации и управлении развитием данной концепции. Тем не менее, автоматизация процессов управления, интеграция систем и ускорение циклов командования продолжают оставаться приоритетными направлениями исследований и практической деятельности.

Анализ современных научных исследований свидетельствует о прогрессирующем движении в направлении формирования систем с высокой степенью автоматизации, быстродействия и информационной интеграции. Концепция сетевой войны позволяет рассчитывать на существенное увеличение эффективности боевых действий за счет снижения временных задержек, усиления сетевого взаимодействия и повышения степени синергии сил.

В перспективе ожидается дальнейшее развитие технологий, таких как искусственный интеллект, квантовые вычисления, расширение возможностей киберзащиты и автоматического управления боевыми системами. Важным аспектом остается нормативно-правовое регулирование данного направления, а также развитие теоретических и методологических оснований, обеспечивающих внедрение и эксплуатацию систем нового типа.

Список использованных источников

1. Макаренко, С. И. Проблемы и перспективы применения кибернетического оружия в современной сетевой войне / С. И. Макаренко // Спецтехника и связь : журнал. – 2011. – № 3. – С. 41–47.
2. Киселев, В. Новые формы разведки и их особенности: принципы тактической разведки в условиях сетевых действий / В. Киселев, И. Рябченко // Армейский сборник : журнал. – 2014. – № 1. – С. 36–40.
3. Хамзатов, М. Адаптация к современности: влияние концепции сетевой войны на характер боевых операций / М. Хамзатов // Армейский сборник : журнал. – 2014. – № 1. – С. 41–43.
4. Милашевский, А. В. Подход к моделированию распределенного во времени комплексного сценария дестабилизирующих воздействий на элементы сети связи специального назначения на основе схем функциональной целостности / А. В. Милашевский, Н. Н. Потапчик // Вестник Военной академии Республики Беларусь. – 2023. – № 4 (81). – С. 27–35.
5. Милашевский, А. В. Факторы, влияющие на функциональную целостность и устойчивость функционирования подвижного узла связи специального назначения / А. В. Милашевский [и др.] // Известия Тульского государственного университета. Технические науки. – 2020. – Вып. 12. – С. 339–344.
6. Воробьев, И. Н. Тактика сетевых действий / И. Н. Воробьев, В. А. Киселев // Армейский сборник : журнал. – 2014. – № 4. – С. 44–46.

7. Литвиненко, В. Комплексная интеграция систем разведки, управления и средств поражения в условиях военных концепций XXI века / В. Литвиненко // Армейский сборник : журнал. – 2015. – № 8. – С. 33–36.

8. Левчук, Н. Н. Сетецентрическая парадигма управления массовыми информационными процессами / Н. Н. Левчук // Вестник БДУ. Сер. 4. – № 1. – С. 62–65.

9. Агафонов, Д. А. Принципы построения системы обеспечения безопасности и защиты информации в системе управления сетью связи специального назначения / Д. А. Агафонов [и др.] // Известия Тульского гос. ун-та. Техн. науки. – 2020. – Вып. 11. – С. 317–321.