УДК 327.8

ГИБРИДНАЯ ВОЙНА: ВЫЗОВЫ ЦИФРОВОЙ ЭПОХИ И СТРАТЕГИИ ПРОТИВОДЕЙСТВИЯ

Р. В. Яхимович, М. В. Цупрунюк, студенты факультета инженерных систем и экологии
Научный руководитель: Е. Г.Кудрицкая, ст. преподаватель
БрГТУ, Брест, Беларусь

Аннотация. Статья посвящена анализу гибридной войны как феномена, который объединяет военные и нетрадиционные методы воздействия в условиях цифровизации. Рассматриваются ключевые механизмы – информационные операции, кибератаки, экономическое давление и субверсивные действия, а также предлагаются стратегии противодействия данному вызову для обеспечения политической и экономической стабильности.

Ключевые слова: гибридная война, кибератаки, информационные технологии, международное сотрудничество, стратегии противодействия.

В современном мире традиционные вооруженные конфликты уступают место новым формам противостояния, где помимо обычной военной силы активно используются информационные технологии и экономические инструменты. В последние годы в политической и политологической среде, в контексте гибридизации мировых процессов, ведется активная дискуссия феномена «гибридной войны». Повышенный интерес к данному явлению связан с резким увеличением значимости информационного компонента в современных международных отношениях, а также закономерным продолжением реализации концепций, так называемых «цветных революций», предусматривающих в достижении политических и стратегических целей использование невоенных методов, реализуемых с задействованием протестного потенциала местного населения и дополняемых военными мерами и действиями сил специальных операций. Гибридная война объединяет в себе разнообразие методы кибератак, дезинформационных кампаний, санкционных мер и использование негосударственных акторов, что делает ее крайне актуальной в современных реалиях.

Гибридная война представляет собой интегрированный комплекс мер, где традиционные военные действия комбинируются с современными методами воздействия. Основные принципы данного явления:

– многоуровневость: использование как прямых военных методов, так и косвенных (информационных, кибернетических, экономических);

– асимметрия: субъекты с ограниченными ресурсами могут успешно противостоять более мощным противникам, применяя нестандартные подходы;

– скрытность: методы направлены на сокрытие истинных источников агрессии, что усложняет своевременную реакцию;

– информационное воздействие: манипулирование общественным мнением и дезинформация играют ключевую роль.

Эти черты обусловливают актуальность гибридной войны в эпоху цифровизации, когда информационные и кибернетические технологии становятся важными инструментами геополитического влияния, обуславливающими

внутреннюю и международную политику, а также определяющие стратегию снижения угрозы.

Гибридные операции включают несколько направлений, каждое из которых обеспечивает устойчивость государства. К ним можно отнести следующие способы действия:

– информационные операции. Современные медийные стратегии используют социальные сети и онлайн-платформы для формирования негативного образа власти, провоцирования раскола в обществе и создания искусственных кризисов. Такие меры ослабляют доверие к официальным источникам и способствуют дезориентации населения;

– кибератаки. Нарушение работы критически важных инфраструктур (энергетики, транспорта, банковского сектора) через кибернетические вторжения, кражу данных и саботаж цифровых систем может привести к экономическому коллапсу и дестабилизации деятельности как государственных, так и частных структур;

– экономическое давление. Санкции, валютные манипуляции и энергетическая зависимость используются для ухудшения инвестиционного климата, повышения рисков и оттока капитала. Эти меры приводят к ухудшению баланса платежей и снижению покупательной способности граждан;

– субверсивные методы. Привлечение негосударственных структур (частных военных компаний, террористических групп, криминальных элементов) позволяет проводить операции вне рамок официального контроля, усложняя идентификацию виновников и оперативное реагирование.

Для достижения целей в политико-экономической сфере, которая является наиболее уязвимой, используются гибридные войны. Они оказывают существенное воздействие, активно используя следующие методы:

– экономическую нестабильность. Кибератаки и санкционные меры приводят к снижению активности ключевых отраслей, ухудшению инвестиционного климата и росту инфляционных процессов, что негативно сказывается на уровне жизни;

– политическую дезинтеграция. Информационные кампании усиливают социальное расслоение, вызывают протестные настроения и подрывают доверие к государственным институтам, что может способствовать политической нестабильности и ухудшению международных отношений;

– нарушение глобальных цепочек поставок. Ограничения в торговле и финансовые манипуляции приводят к перебоям в международных поставках, требуя значительных ресурсов для перестройки логистических систем и поиска новых партнеров.

На сегодняшний день, важную роль в противодействии гибридным угрозам играют следующие концептуальные стратегии:

– интегрированная система национальной безопасности. Необходимо объединение усилий военных, киберспециалистов и экономистов, создание оперативных центров и использование аналитических систем для раннего обнаружения угроз;

– укрепление кибербезопасности. Разработка современных технологий защиты, подготовка специалистов и расширение международного сотрудничества помогут снизить уязвимость критически важной инфраструктуры;

– повышение информационной грамотности. Проведение образовательных программ, развитие систем проверки достоверности информации и поддержка независимых медиа способствуют укреплению критического мышления среди населения.

– экономическая диверсификация. Развитие отечественных технологий, создание финансовых резервов и поддержка малого и среднего бизнеса помогут снизить влияние санкций и внешних экономических воздействий;

– международное сотрудничество. Заключение многосторонних соглашений, обмен опытом и проведение совместных учений способствуют выработке общих стандартов противодействия гибридным угрозам.

Таким образом, гибридная война представляет собой сложное явление, способное значительно повлиять на политическую и экономическую устойчивость государства. В условиях цифровой эпохи, когда информационные и кибернетические технологии играют центральную роль, для противодействия гибридным угрозам необходим комплексный подход. Интеграция мер национальной безопасности, усиление киберзащиты, повышение информационной грамотности и диверсификация экономики помогут обеспечить устойчивость и стабильность в быстро меняющемся глобальном пространстве.

Список использованных источников

1. Гринин, Л. Е. Формирования нового мирового порядка / Л. Е. Гринин // Век глобализации. – 2016. – № 1–2. – С. 3–18.

2. Комлева, Н. А. Гибридная война: сущность и специфика / Н. А. Комлева // Известия Уральского федерального университета. Серия 3. Общественные науки. – 2017. – Т. 12. – № 3 (167). – С. 128–137.

3. Коданева, С. И. Гибридные угрозы безопасности России: выявление и противодействие / С. И. Коданева // Контуры глобальных трансформаций: политика, экономика, право. – 2020. – № 2. – С. 44–62.

4. Арчаков, В. Ю. Информационные технологии гибридных войн / В. Ю. Арчаков, О. С. Макаров // Аналитический и научно-практический журнал. – 2017. – № 4 (40). – С. 22–25.