



МРНТИ 78.27.13

<https://doi.org/10.56132/2791-3368-2026-3-67-109-119>**Ж.А. Корабаев¹, Р.А. Якубов¹, К. Койчикулов²**¹National Defense University of the Republic of Kazakhstan,
Астана, Казахстан²Military Institute of Land Forces named after S. Nurmagambetov,
Алматы, Казахстан
E-mail: korabavzh@mail.ru

ОСОБЕННОСТИ ТАКТИКИ НЕЗАКОННЫХ ВООРУЖЕННЫХ ФОРМИРОВАНИЙ В СОВРЕМЕННЫХ КОНФЛИКТАХ: ОТ КЛАССИЧЕСКОЙ ПАРТИЗАНСКОЙ ВОЙНЫ К ГИБРИДНО- СЕТЕВОЙ МОДЕЛИ

Аннотация. В статье на основе обобщения опыта вооруженных конфликтов последних трех десятилетий предпринят критический анализ трансформации тактики незаконных вооруженных формирований (НВФ). Современные НВФ переходят к гибридно-сетевой модели, где огневой компонент подчинен информационно-психологическим и кибернетическим задачам. Автор предлагает трехпоколенную временную шкалу развития тактики незаконных вооруженных группировок. Отмечены системные конфликты в новой парадигме, включая зависимость от технологий, уязвимость перед кибератаками и внутреннюю борьбу между традиционной идеологией и технократическими инструментами. Выдвинуты гипотезы о возникновении «точки бифуркации», связанной с широким использованием автономного искусственного интеллекта. Сделаны выводы о необходимости переосмысления методов противодействия этим опасностям.

Ключевые слова: незаконные вооруженные формирования, тактика, гибридная война, сетевые структуры, беспилотные системы, информационно-психологическое воздействие, искусственный интеллект, контртеррористические операции.

Введение.

Изучение тактики незаконных вооруженных формирований (НВФ) традиционно строится на систематизации эмпирического материала, накопленного в ходе вооруженных конфликтов второй половины XX — начала XXI века. Учебные пособия и монографии последовательно описывают засады, минно-взрывные заграждения, оборону в населенных пунктах, использование местного населения в качестве укрытия и разведывательного ресурса [2, 8, 10]. В течение последних 25 лет этот канон воспроизводился с минимальными изменениями.



Однако аналитик, систематически отслеживающий конфликты в течение последних пяти-семи лет — от Сирии и Йемена до Нагорного Карабаха и зоны специальных операций, — не может не заметить растущее несоответствие между «книжной» тактикой и реальными действиями незаконных вооруженных группировок на поле боя. Боевики все чаще демонстрируют поведение, не вписывающееся в старые модели, но при этом добиваются оперативных побед, превосходящих возможности традиционных партизанских группировок [4, 16].

Это позволяет нам сформулировать исследовательский вопрос: имеем ли мы дело с количественным накоплением новых процедур или с качественным скачком, изменяющим фундаментальную сущность явления? Ответ на этот вопрос влияет как на научное, так и на сугубо практическое значение работы — от содержания программ военной подготовки до стратегии контртеррористических операций.

Цель исследования — провести критический анализ известных представлений о тактике незаконных вооруженных организаций с учетом технических, организационных и когнитивных достижений за последнее десятилетие.

Материалы и методы.

Теоретической базой послужили работы отечественных и зарубежных авторов по тактике иррегулярных формирований, гибридным войнам и информационно-психологическому противоборству [2, 3, 7, 10, 11, 12, 13, 18]. Эмпирическую основу составили аналитические отчеты экспертных центров (Jamestown Foundation, Tactics Institute, MIDAS), материалы военно-исторических исследований и открытые данные о ходе вооруженных конфликтов [4, 5, 16, 17].

Использованы методы историко-сравнительного анализа, системно-структурного моделирования и теоретического обобщения. Особое внимание уделено выявлению устойчивых паттернов, повторяющихся в разных конфликтах, и их интерпретации в контексте технологической эволюции.

Результаты и обсуждение.

1. Поколения тактики НВФ: попытка периодизации.

Анализ эмпирического материала позволяет предложить следующую периодизацию эволюции тактики НВФ.

Первое поколение (1990–2010 гг.) — классическая партизанская тактика с опорой на засады, минно-взрывные заграждения, укрытие среди населения и ограниченное использование средств связи. В ходе боевых действий на Северном Кавказе с 1994 по 1996 год террористы умело устраивали засады с фронтальным и фланговым огнем, уделяя большое внимание последовательности отступления [7, с. 56–59]. В этот период действия незаконных вооруженных группировок, как правило, были предсказуемы и



могли быть нейтрализованы при наличии достаточных знаний и огневой мощи.

Второе поколение (2010–2020): интеграция коммерческих БПЛА, зашифрованных мессенджеров и первые формы продвижения через социальные сети [20, с. 156–160]. Одним из таких примеров является деятельность ИГИЛ в Сирии и Ираке, когда беспилотники использовались для разведки, координации огня и психологической войны. В это время незаконные вооруженные группировки начали осваивать интернет, хотя и лишь в качестве вспомогательного инструмента.

Третье поколение (с 2020 года): гибридные сетевые структуры, объединяющие физическую агрессию, цифровые атаки и информационно-психологические операции в единый оперативный комплекс.

Характерные черты включают автономные БПЛА, управляемые нейронными сетями, децентрализованные ячеистые коммуникационные сети, устойчивые к цензуре, широкое использование дипфейков и генеративного ИИ для дезинформации, а также кибератаки на ключевую инфраструктуру [4, 5, 21]. Это качественно новый уровень, где традиционные тактические подходы отходят на второй план.

Главный вывод этого раздела заключается в том, что методы незаконных вооруженных организаций меняют свою онтологическую позицию, а не просто усложняются. Если первое поколение вело бои на земле, второе использовало местность, а третье – цифровую среду, то физическое пространство становится лишь платформой для подтверждения победы в виртуальной сфере.

2. Технологический фундамент новой тактики: дроны, сети, автономия.

Основной движущей силой перемен стало появление технологий, ранее доступных исключительно вооруженным силам государств. Однако сводить все к «дронам» — ошибка. Обсуждается систематическая интеграция трех элементов:

1) Датчики и вооружение. Коммерческие БПЛА включают тепловизоры, дроны-камикадзе с FPV-камерами и механизмы сброса. К 2025 году задокументирован переход к автономному тепловизионному наведению на последнем участке траектории без участия оператора [15, с. 110–112]. Это снижает эффективность радиоэлектронного подавления, поскольку цель фиксируется до входа в зону глушения.

2) Связь и управление. Переход от иерархических систем к децентрализованным ячеистым сетям связи с использованием LoRa или спутниковых терминалов. Такие сети способны выдерживать потерю отдельных узлов и их сложнее подавить [13, с. 204–208]. Система управления становится сетевцентрической, при этом каждый истребитель выступает в роли приемника и ретранслятора.

3) Автономные алгоритмы. Реализация детекторов на основе нейронных сетей для распознавания целей с использованием силуэтов и тепловых сигнатур. Это позволяет БПЛА функционировать без GPS и в постоянной



связи с оператором, что делает их неуязвимыми для традиционных средств радиоэлектронной борьбы [26, с. 208–212].

Однако здесь возникает системное противоречие. Технологизация создает новую уязвимость: зависимость от аккумуляторов, спутникового сигнала, программного обеспечения и калибровки сенсоров. Как только противник находит способ нарушить эти цепочки, высокотехнологичное подразделение НВФ может оказаться беспомощнее классического боевика с автоматом. Этот парадокс — технологическая мощь при колоссальной хрупкости — пока слабо учитывается в стратегиях противодействия.

Сформулируем гипотезу №1: в ближайшие 2–3 года НВФ перейдут к массовому использованию автономных дронов с полным циклом «обнаружение — захват — поражение» без участия человека. Это создаст «точку бифуркации», после которой классические средства РЭБ и ПВО тактического звена станут малоэффективными. Если это произойдет, характер противоборства изменится радикально.

3. Информационно-психологический контур: новый центр тяжести.

В военной науке долгое время информационно-психологические операции трактовались как вспомогательные. Анализ деятельности действующих незаконных вооруженных организаций показывает обратную картину: для них это основной канал причинения вреда. Доказательства:

ИГИЛ использовал до 30–40% своих операционных расходов на создание и распространение пропагандистского контента [20, с. 156–160].

Группировка «Аль-Шабаб» использует дроны не только для нападений, но и для создания видеороликов высокого разрешения, которые размещаются в TikTok с целью вербовки молодежи [5].

Поступали сообщения об использовании технологии дипфейк для создания поддельных видеороликов, на которых сотрудники полиции отдают предательские приказы [21, с. 34–37].

Это уже не "информационная поддержка", а прямое боевое действие, по своему эффекту сравнимое с артиллерийским обстрелом. Более того, в ряде случаев информационная атака оказывается дешевле и результативнее: один грамотно сфабрикованный ролик способен парализовать работу штаба на сутки, посеять недоверие среди личного состава и деморализовать население.

Но и здесь есть слабое место. Технологии генеративного ИИ работают на основе существующих данных. Чем больше «цифрового следа» оставляет объект, тем убедительнее его имитация. Однако лидеры незаконных вооруженных группировок часто минимизируют свою публичную видимость, создавая «цифровой шум» вокруг второстепенных персонажей. Это означает, что мы можем использовать ту же стратегию против них: создавать фиктивные каналы, фабриковать приказы и вводить в заблуждение их аналитические системы. Однако для этого необходимы не только технологии, но и оперативная культура, которых сейчас не хватает.

Гипотеза №2: в ближайшей перспективе центр противоборства окончательно сместится в когнитивную плоскость. Победа будет достигаться



не количеством уничтоженных боевиков, а способностью разрушить их нарратив, подорвать доверие внутри сети и перехватить управление символическими ресурсами. Физические потери станут лишь индикатором успеха, а не его сутью.

4. Киберфизическая среда городов: новая арена.

Городская застройка традиционно считалась наиболее благоприятной средой для НВФ — плотные укрытия, развитая инфраструктура, большое количество мирных жителей [9, 24]. Однако с цифровизацией городов появляется новое измерение. Современный мегаполис — это миллионы подключенных устройств: камеры, светофоры, системы управления транспортом, датчики коммунальных служб [25, с. 134–137].

Уже фиксируются случаи (пока единичные, но системно значимые), когда НВФ:

- изменяли режим работы светофоров для создания заторов и изоляции районов действий сил правопорядка;
- отключали камеры видеонаблюдения в ключевых точках;
- теоретически возможно вмешательство в системы оповещения для трансляции панических сообщений.

Это уже не «городская партизанская война» в традиционном смысле, а скорее киберфизический подход, при котором атака на цифровой слой города предшествует или заменяет физический удар.

Интересно, что тот же контекст предоставляет возможности для противодействия. Тщательное изучение сетевого трафика, нарушений в потреблении электроэнергии и странных запросов GPS может указывать на планирование незаконных действий вооруженных групп. Однако для этого необходимы не только технологические средства, но и правовая база, общественное доверие и квалифицированные специалисты. Пока эти условия выполнены далеко не везде.

Гипотеза №3: в будущем именно способность контролировать и защищать цифровой слой города, а не физический контроль улиц, станет ключевым фактором успеха в противостоянии с НВФ. Это потребует пересмотра организационной структуры подразделений, задействованных в контртеррористических операциях — включения в их состав киберспециалистов и аналитиков данных на постоянной основе.

5. Системные противоречия и уязвимости новой модели.

Переход к гибридно-сетевой модели порождает внутренние противоречия, которые можно использовать для противодействия.

Первое противоречие: между идеологией и технологией. Классическая партизанская идеология опирается на «близость к земле», «простоту», «народность». Технократическая тактика требует сложного оборудования, регулярного питания аккумуляторов, постоянных обновлений ПО и высокой квалификации. Это создает разрыв между традиционными боевиками, которые составляют костяк, и «цифровым авангардом». Этот разрыв можно



усиливать через точечную ликвидацию технических специалистов и дезинформацию о «предательстве» технологов.

Второе противоречие существует между децентрализацией и координацией. Сетевые архитектуры устойчивы к потере лидеров, хотя они в значительной степени зависят от каналов связи и алгоритмов распространения информации. Нарушение синхронизации (например, введение противоречащих директив) может остановить их деятельность. Этот недостаток обуславливает необходимость разработки методов «контролируемого хаоса» в информационных потоках противника.

Третье противоречие — между скоростью и глубиной. Незаконные вооруженные организации третьего поколения наносят удары быстро и бегут, но они редко способны к долгосрочному стратегическому планированию. Их подходы основаны на использовании существующих технологических решений, а не на их разработке. Это подразумевает, что они могут действовать на опережение, расставляя технические ловушки и создавая неблагоприятные условия для противника.

Заключение.

Исследование показывает, что тактика незаконных вооруженных организаций вступила в период качественной трансформации, которую нельзя объяснить лишь приобретением новых навыков. Современная незаконная вооруженная организация — это не «боевой отряд», а скорее гибридная сеть, сочетающая физическое насилие, интернет-атаки и психологическое давление в единую оперативную структуру.

1. Классические тактические стратегии по-прежнему существуют, но они теряют свою первостепенную важность. Они превращаются в «тактические ритуалы» и часть оперативного контекста, а не в доминирующую силу.

2. Технологический прогресс создает новые уязвимости. Зависимость от батарей, средств связи и программного обеспечения делает высокотехнологичные незаконные вооруженные организации уязвимыми для целенаправленных кибератак и радиоэлектронной борьбы нового поколения.

3. Информационно-психологический контур становится основным полем боя. Способность управлять нарративами, создавать фейки и разрушать доверие внутри сети противника становится важнее огневой мощи.

4. Городская среда трансформируется в киберфизический театр войны, где цифровой контроль становится таким же важным, как физический.

5. Существующие подходы к противодействию устаревают. Они строятся на симметричном принципе (против БПЛА — РЭБ, против пропаганды — контрпропаганда), тогда как НВФ действуют асимметрично. Ответ должен быть асимметричным: упреждающее кибервоздействие, взлом систем управления, подмена каналов связи, создание ложных целей и ложных приказов.



В заключение следует отметить, что в статье предлагаются не столько готовые решения, сколько свежий взгляд на проблему. Вместо вопроса «как бороться с тактикой незаконных вооруженных группировок?», в ней задается вопрос: «в какой обстановке мы воюем, и как эта обстановка меняет саму природу противника?» Без ответа на этот вопрос любые тактические рекомендации будут отложены.

СПИСОК ЛИТЕРАТУРЫ

1. Biddle S. Nonstate Warfare: The Military Methods of Guerillas, Warlords, and Militias. – Princeton University Press, 2021. – 328 p.
2. Федулов Б.А. и др. Тактика действий незаконных вооруженных формирований в Северо-Кавказском регионе и методы противодействия им: учебное пособие. – Барнаул: Барнаульский юридический институт МВД России, 2003. – 94 с.
3. Потапов А.А. Тактика антитеррора: сборник методических инструкций по борьбе с незаконными вооруженными формированиями. – М.: Фаир, 2008. – 480 с.
4. Arip L.A. From Guns to Gadgets: The Digital Shift in Armed Group Warfare // MIDAS Commentary. – 2026. – 3 February.
5. Quadcopter Drones Reshaping Pakistan's Militant Landscape // Jamestown Foundation. – 2026. – 16 March.
6. Орехов А.Л. Малая война. Организация и тактика боевых действий малых подразделений: хрестоматия. – М., 2006. – 320 с.
7. Божедомов Б.А., Левченко Т.Г. Особенности боевых действий незаконных вооружённых формирований на Северном Кавказе на примерах боестолкновений 1994–1996 гг. // Военно-исторический журнал. – 2022. – № 5. – С. 54-61.
8. Федулов Б.А. и др. Тактика действий незаконных вооруженных формирований в Северо-Кавказском регионе и методы противодействия им: учебное пособие. – Барнаул: Барнаульский юридический институт МВД России, 2003. – С. 5-7.
9. Кондрашов А., Таненя Д. Тактика незаконных вооруженных формирований при ведении боевых действий в населенном пункте // Армейский сборник. – 2022. – № 5. – С. 22-27.
10. Потапов П. Борьба с НВФ – негосударственными вооруженными формированиями. – Минск: Харвест, 2007. – 448 с.
11. Тиханычев О.В. История развития «гибридных» действий от войн «под чужим флагом» до «умной силы» // Национальная безопасность / Nota bene. – 2025. – № 1. – С. 77-102.
12. Карпович О.Г., Гришанов А.А., Козюлин В.Б. и др. Гибридные войны: учебник. – М., 2025. – 420 с.
13. Biddle S. Nonstate Warfare. – Princeton, 2021. – 328 p.



14. Schulzke M. Twenty-First Century Military Innovation: Technological, Organizational, and Strategic Change Beyond Conventional War. – University of Michigan Press, 2021. – 280 с.
15. Современные вооруженные конфликты: эволюция и применение беспилотных летательных аппаратов // Russia Global SPbSTU. – 2025. – № 2. – С. 110-118.
16. Digital Warfare By Terror Groups In Eurasian Conflicts // Tactics Institute. – 2025. – 15 November.
17. Modern Armed Conflict: The Evolution and Impact of Unmanned Aerial Vehicles // Russia Global SPbSTU. – 2025.
18. Звягин А.А., Артамонов Б.А., Мельников И.А. Россия в гибридной войне. Информационно-психологическая безопасность: монография. – М.: НИЦ ИНФРА-М, 2024. – 329 с.
19. Информационная составляющая гибридной войны // CyberLeninka. – 2024.
20. Ярошенко М.П. Использование идеологии экстремизма как инструмента в ведении гибридной войны // CyberLeninka. – 2023.
21. Гибридная война как форма межгосударственных конфликтов // CyberLeninka. – 2023.
22. Гибридная война как понятие и явление // CyberLeninka. – 2024.
23. Ярошенко М.П. Использование идеологии экстремизма как инструмента в ведении гибридной войны // CyberLeninka. – 2023. – С. 4.
24. Тактика действий НВФ в условиях городской застройки // Военная мысль. – 2023. – № 3. – С. 54-62.
25. Адаптивный подход к применению сил и средств для борьбы с террористами по опыту вооруженных конфликтов за пределами России // Военная мысль. – 2024. – № 2. – С. 132-140.
26. Основы международной безопасности: учебное пособие. – 3-е изд. – М., 2024. – 350 с.
27. Частные военные компании как инструмент осуществления силовой стратегии гибридных войн // CyberLeninka. – 2024.
28. Потапов А.А. Тактика антитеррора. – М., 2008. – С. 3-5.
29. Федулов Б.А. и др. Тактика действий НВФ. – Барнаул, 2003. – С. 67-70.
30. Асыллов Н.Ж., Садуев Р.С., Портнов В.В., Макаров Е.Л. Особенности и направление совершенствования современной тактики ведения боевых действий против незаконных вооруженных формирований // Наука. – 2020. – С. 5-7.

REFERENCES

1. Biddle S. Nonstate Warfare: The Military Methods of Guerillas, Warlords, and Militias. – Princeton University Press, 2021. – 328 p.



2. Fedulov B.A. i dr. Taktika dejstvij nezakonnyh vooruzhennyh formirovanij v Severo-Kavkazskom regione i metody protivodejstviya im: uchebnoe posobie. – Barnaul: Barnaul'skij juridicheskij institut MVD Rossii, 2003. – 94 s.
3. Potapov A.A. Taktika antiterrora: sbornik metodicheskikh instrukcij po bor'be s nezakonnyimi vooruzhennymi formirovanijami. – M.: Fair, 2008. – 480 s.
4. Arip L.A. From Guns to Gadgets: The Digital Shift in Armed Group Warfare // MIDAS Commentary. – 2026. – 3 February.
5. Quadcopter Drones Reshaping Pakistan's Militant Landscape // Jamestown Foundation. – 2026. – 16 March.
6. Orehov A.L. Malaja vojna. Organizacija i taktika boevykh dejstvij malyh podrazdelenij: hrestomatija. – M., 2006. – 320 s.
7. Bozhedomov B.A., Levchenko T.G. Osobennosti boevykh dejstvij nezakonnyh vooruzhjonnyh formirovanij na Severnom Kavkaze na primerah boestolknovenij 1994–1996 gg. // Voenno-istoricheskij zhurnal. – 2022. – № 5. – S. 54-61.
8. Fedulov B.A. i dr. Taktika dejstvij nezakonnyh vooruzhennyh formirovanij v Severo-Kavkazskom regione i metody protivodejstviya im: uchebnoe posobie. – Barnaul: Barnaul'skij juridicheskij institut MVD Rossii, 2003. – S. 5-7.
9. Kondrashov A., Tanenja D. Taktika nezakonnyh vooruzhennyh formirovanij pri vedenii boevykh dejstvij v naselennom punkte // Armejskij sbornik. – 2022. – № 5. – S. 22-27.
10. Potapov P. Bor'ba s NVF – negosudarstvennymi vooruzhennymi formirovanijami. – Minsk: Harvest, 2007. – 448 s.
11. Tihanychev O.V. Istorija razvitija «gibridnyh» dejstvij ot vojn «pod chuzhim flagom» do «umnoj sily» // Nacional'naja bezopasnost' / Nota bene. – 2025. – № 1. – S. 77-102.
12. Karpovich O.G., Grishanov A.A., Kozjulin V.B. i dr. Gibridnye vojny: uchebnyk. – M., 2025. – 420 s.
13. Biddle S. Nonstate Warfare. – Princeton, 2021. – 328 p.
14. Schulzke M. Twenty-First Century Military Innovation: Technological, Organizational, and Strategic Change Beyond Conventional War. – University of Michigan Press, 2021. – 280 s.
15. Sovremennye vooruzhennye konflikty: jevoljucija i primenenie bespilotnyh letatel'nyh apparatov // Russia Global SPbSTU. – 2025. – № 2. – S. 110-118.
16. Digital Warfare By Terror Groups In Eurasian Conflicts // Tactics Institute. – 2025. – 15 November.
17. Modern Armed Conflict: The Evolution and Impact of Unmanned Aerial Vehicles // Russia Global SPbSTU. – 2025.
18. Zvjagin A.A., Artamonov B.A., Mel'nikov I.A. Rossiya v gibridnoj vojne. Informacionno-psihologicheskaja bezopasnost': monografija. – M.: NIC INFRA-M, 2024. – 329 s.
19. Informacionnaja sostavljajushhaja gibridnoj vojny // CyberLeninka. – 2024.



20. Jaroshenko M.P. Ispol'zovanie ideologii jekstremizma kak instrumenta v vedenii gibridnoj vojny // CyberLeninka. – 2023.
21. Gibridnaja vojna kak forma mezhgosudarstvennyh konfliktov // CyberLeninka. – 2023.
22. Gibridnaja vojna kak ponjatie i javlenie // CyberLeninka. – 2024.
23. Jaroshenko M.P. Ispol'zovanie ideologii jekstremizma kak instrumenta v vedenii gibridnoj vojny // CyberLeninka. – 2023. – S. 4.
24. Taktika dejstvij NVF v uslovijah gorodskoj zastrojki // Voennaja mysl'. – 2023. – № 3. – S. 54-62.
25. Adaptivnyj podhod k primeneniju sil i sredstv dlja bor'by s terroristami po opytu vooruzhennyh konfliktov za predelami Rossii // Voennaja mysl'. – 2024. – № 2. – S. 132-140.
26. Osnovy mezhdunarodnoj bezopasnosti: uchebnoe posobie. – 3-e izd. – M., 2024. – 350 s.
27. Chastnye voennye kompanii kak instrument osushhestvlenija silovoj strategii gibridnyh vojn // CyberLeninka. – 2024.
28. Potapov A.A. Taktika antiterrora. – M., 2008. – S. 3-5.
29. Fedulov B.A. i dr. Taktika dejstvij NVF. – Barnaul, 2003. – S. 67-70.
30. Asylov N.Zh., Saduev R.S., Portnov V.V., Makarov E.L. Osobennosti i napravlenie sovershenstvovaniya sovremennoj taktiki vedeniya boevykh dejstvij protiv nezakonnyh vooruzhennyh formirovanij // Nauka. – 2020. – S. 5-7.

Жарылкасын Қорабаев, PhD, доцент, полковник, National Defence University of the Republic of Kazakhstan, Астана, Қазақстан

Радикжан Якубов, магистр, аға оқытушы, полковник, National Defence University of the Republic of Kazakhstan, Астана, Қазақстан

Комекбай Койчыкулов, полковник, доцент, Military Institute of Land Forces named after S. Nurmagambetov, Алматы, Казахстан

ҚАЗІРГІ ҚАҚТЫҒЫСТАРДАҒЫ ЗАҢСЫЗ ҚАРУЛЫ ҚҰРЫЛЫМДАРДЫҢ ТАКТИКАСЫНЫҢ ЕРЕКШЕЛІКТЕРІ: КЛАССИКАЛЫҚ ПАРТИЗАНДЫҚ СОҒЫСТАН ГИБРИДТІ-ЖЕЛІЛІК МОДЕЛЬГЕ ДЕЙІН

Аңдатпа. Мақалада соңғы отыз жылдағы қарулы қақтығыстар тәжірибесін жинақтау негізінде заңсыз қарулы құралымдар (ЗҚҚ) тактикасының трансформациясына сынды талдау жасалған. Қазіргі ЗҚҚ гибриді-желілік үлгіге көшуде, мұнда оттық компонент ақпараттық-психологиялық және кибернетикалық міндеттерге бағынады. ЗҚҚ тактикасы эволюциясының үш буынға бөлінген авторлық мерзімділігі ұсынылған. Жаңа үлгінің жүйелік қайшылықтары анықталған — технологиялық тәуелділік, киберәсерге осалдық және дәстүрлі идеология мен технократиялық құралдар арасындағы ішкі қақтығыс. Автономды жасанды интеллектті жаппай



енгізумен байланысты «бифуркация нүктесінің» туындауы туралы болжамдар тұжырымдалған. Қарсы іс-қимыл тәсілдерін қайта қарау қажеттілігі туралы қорытындылар жасалған.

Түйінді сөздер: заңсыз қарулы құралымдар, тактика, гибридті соғыс, желілік құрылымдар, ұшқышсыз жүйелер, ақпараттық-психологиялық әсер ету, жасанды интеллект, терроризмге қарсы операциялар.

Zharylkasyn Korabaev, PhD, associate professor, Colonel, National Defense University of the Republic of Kazakhstan, Astana, Kazakhstan

Radikzhan Yakubov, master, senior lecturer, Colonel, National Defense University of the Republic of Kazakhstan, Astana, Kazakhstan

Komekbai Koichikulov, colonel, docent, Military Institute of Land Forces named after S. Nurmagambetov, Almaty, Kazakhstan

FEATURES OF THE TACTICS OF ILLEGAL ARMED FORMATIONS IN MODERN CONFLICTS: FROM CLASSIC GUERRILLA WARFARE TO A HYBRID-NETWORK MODEL

Abstract: Based on a synthesis of experience from armed conflicts over the past three decades, this article presents a critical analysis of the transformation of tactics employed by illegal armed formations (IAFs). Modern illegal armed groups are evolving toward a hybrid network-centric model, where kinetic operations are subordinated to information-psychological and cyber objectives. An original periodization of IAF tactical evolution into three generations is proposed. Systemic contradictions of the new model are identified — technological dependency, vulnerability to cyber influence, and the internal conflict between traditional ideology and technocratic tools. Hypotheses regarding the onset of a «bifurcation point» associated with the mass adoption of autonomous artificial intelligence are formulated. Conclusions are drawn about the necessity of revising counteraction approaches.

Keywords: illegal armed formations, tactics, hybrid warfare, network structures, unmanned systems, information-psychological influence, artificial intelligence, counter-terrorist operations.

Поступила: 07 февраля 2026 года

Рецензирована: 21 августа 2026 года

Принята: 28 августа 2026 года