Секция «Политические и социально-экономические процессы на евразийском пространстве»

Гибридные войны и их влияние на региональную безопасность: как ОДКБ и СНГ адаптируют свои стратегии под новые виды угроз

Научный руководитель – Кротов Михаил Иосивофич

Халяпин Илья Дмитриевич

Студент (магистр)

Московский государственный университет имени М.В.Ломоносова, Факультет мировой политики, Кафедра международной безопасности, Москва, Россия

E-mail: street291@mail.ru

Современные вызовы безопасности всё чаще приобретают гибридный характер, сочетая военные, экономические, информационные и технологические методы воздействия. Гибридная война представляет собой совокупность мер, включающих как классические вооружённые действия, так и применение невоенных инструментов – информационных, кибернетических, экономических и правовых. В условиях динамично меняющейся международной обстановки ОДКБ и СНГ вынуждены модернизировать свои стратегические доктрины для противодействия новым вызовам. Гибридная война, как и всякое социально-политическое явление, нуждается в системе средств для его реализации [1]. Для постсоветского пространства, где ОДКБ и СНГ играют ключевую роль в обеспечении стабильности, адаптация к таким угрозам становится критически важной.

Гибридные войны характеризуются асимметричностью и размытостью границ между войной и миром. Гибридность отражает существенные изменения характера современных войн, которые отличаются разноплановостью и многомерностью [2]. В отличие от традиционных конфликтов, они включают:

1. Информационно-психологические операции (манипуляция общественным мнением, дезинформация);
2. Кибератаки на критическую инфраструктуру;
3. Экономическое давление через санкции и контроль ресурсов [3].

Для ОДКБ и СНГ подобные угрозы особенно актуальны в контексте конфликтов на постсоветском пространстве, таких как события в Нагорном Карабахе (2020) и кризисы в Центральной Азии [4]. Данные события демонстрируют, как локальная нестабильность может перерасти в более широкий конфликт, затрагивая систему коллективной безопасности.

Для противодействия гибридным угрозам страны-участницы ОДКБ и СНГ реализуют комплекс практических мер: проведение совместных учений по реагированию на кибератаки и информационные операции, создание оперативных центров мониторинга угроз, разработку унифицированных доктрин по защите критической инфраструктуры и систематизированный обмен разведданными. Эти шаги способствуют модернизации оборонных стратегий и повышению кибербезопасности, снижая уязвимость региона к дестабилизирующим воздействиям.

Стратегия коллективной безопасности ОДКБ до 2025 года предусматривает формирование системы информационной безопасности для государств-членов, развитие межгосударственного сотрудничества и межведомственной координации, а также проведение совместных мероприятий по противодействию и нейтрализации противоправной деятельности в информационно-телекоммуникационном пространстве. [5].

СНГ акцентирует внимание на укреплении информационной безопасности участников. С 2013 года подписанное Соглашение предусматривает создание единой нормативно-

правовой базы, разработку совместных актов, унификацию стандартов и создание защищённых информационных систем, а также совершенствование технологий защиты, организацию трансграничного обмена информацией, постоянный анализ угроз и повышение квалификации кадров [6].

Несмотря на успехи в цифровых технологиях и безопасности, остаются нерешённые вызовы. Разрыв в технологических возможностях приводит к неравномерному распределению ресурсов: одни страны оснащены современными средствами киберзащиты и оперативного реагирования, а другие отстают, что создаёт уязвимости в системе коллективной безопасности. Кроме того, политическая разнонаправленность интересов (например, различия между Беларусью и Арменией по санкционным мерам) затрудняет формирование единой позиции по противодействию гибридным угрозам.

Для повышения эффективности противодействия современным вызовам в области кибербезопасности и информационных угроз необходим комплекс мер. Унификация законодательства создаст единые правовые рамки, гармонизируя нормативные акты между странами и ускоряя взаимодействие регуляторов для выявления и пресечения кибератак. Расширение сотрудничества с международными организациями, такими как ШОС и БРИКС, способствует формированию «пояса цифровой стабильности», объединяя усилия в противодействии информационным угрозам, обмене лучшими практиками и технологиями, что позволяет создать устойчивую цифровую инфраструктуру. Интеграция искусственного интеллекта в системы раннего предупреждения обеспечивает автоматический анализ больших объёмов данных, прогнозирование киберинцидентов и оперативное выявление аномалий. Комплексное применение этих мер повышает кибербезопасность и укрепляет стабильность цифрового пространства в условиях динамично развивающихся угроз.

Таким образом, гибридные угрозы требуют постоянного совершенствования стратегий стран ОДКБ и СНГ. Сочетая, военные, экономические, информационные и технологические методы воздействия, они стимулируют необходимость унификации законодательства в сфере кибербезопасности, расширения сотрудничества с ШОС и БРИКС для создания «пояса цифровой стабильности», а также интеграции искусственного интеллекта в системы раннего предупреждения. Реализация этих мер способствует оперативному реагированию и укреплению региональной безопасности.

Источники и литература

1 Алиев Д.Ф. Конвенциональные технологии как элемент гибридной войны // Политконсультант. 2022. Т. 2. № 3.

2 Бартош А.А. Стратегия и контрстратегия гибридной войны // Военная мысль. М.: № 10-2018, С. 5-21.

3 Федоров А. В. Гибридные угрозы – новый вызов или жупел постдемократии? (западный дискурс) // Полилог 2022. – Т. 6.

4 Юрьева Т.В. Проблемы региональной безопасности: современный опыт Европы // Вестник МГИМО-Университета. 2010;(6(15)):126-133.

5 Стратегия коллективной безопасности Организации Договора о коллективной безопасности на период до 2025 года: https://odkb-csto.org/documents/statements/strategiya_kollektivnoy_bezopasnosti_organizatsii_dogovora_o_kollektivnoy_bezopasnosti_na_period_do_/#loaded

6 Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в области обеспечения информационной безопасности: https://cis.minsk.by/reestrv2/doc/4074#tex