UOT 355.02; 327
DOI: https://doi.org/10.30546/19063.2026.06.5152

КОНЦЕПТУАЛЬНЫЕ ОСНОВЫ ОБЕСПЕЧЕНИЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ АЗЕРБАЙДЖАНА В УСЛОВИЯХ АСИММЕТРИЧНЫХ УГРОЗ И ИНФОРМАЦИОННОЙ ВОЙНЫ

ЛЕЙЛА ЭЛЬЧИН НАДЖАФОВА АЛИЗАДЕ
Докторант Бакинского Государственного Университета
г. Баку, ул., Академика З.Халилова 33, AZ1148
https://orcid.org/0009-0003-6635-6122
E-mail: leyla.nacafova-2@bsu.edu.az

РЕЗЮМЕ

В современной обстановке безопасности широкое использование цифровых технологий и усиление влияния информационного пространства на межгосударственные отношения создали условия для возникновения новых форм угроз национальной безопасности. В статье рассматривается природа асимметричных угроз, которые могут повлиять на национальную безопасность Азербайджана в контексте информационной войны. Анализируется влияние таких инструментов, как кибератаки, дезинформация, манипулирование информацией и психологическое воздействие на информационное пространство государства и общую обстановку в сфере безопасности. Кроме того, освещаются вопросы обеспечения информационной и кибербезопасности, защиты критической информационной инфраструктуры, своевременного выявления потенциальных угроз и формирования устойчивости в информационной среде. Укрепление институциональной координации, развитие стратегической коммуникации, повышение информационной грамотности общества и расширение международного сотрудничества рассматриваются как важные направления защиты национальной безопасности Азербайджана в соответствии с современными вызовами.

Ключевые слова: *асимметричные угрозы, информационная война, национальная безопасность, информационная безопасность, кибербезопасность, дезинформация, манипулирование информацией, стратегическая коммуникация.*

ВВЕДЕНИЕ

В условиях стремительной трансформации международной системы безопасности и ускоренного развития цифровых технологий вопросы обеспечения национальной безопасности государств приобретают качественно новое содержание. Современные угрозы характеризуются не только увеличением их масштабов и географии распространения, но и изменением способов, средств и субъектов их реализации. Если традиционно вопросы национальной безопасности преимущественно связывались с военными угрозами, вооружёнными конфликтами и прямым внешним воздействием, то в настоящее время спектр рисков существенно расширился и включает политические, экономические, социальные, информационные, технологические, экологические и иные взаимосвязанные угрозы.

В современной международной обстановке государства сталкиваются с терроризмом, экстремизмом и этническим сепаратизмом, вооружёнными конфликтами, транснациональной организованной преступностью, распространением оружия массового уничтожения, массовой миграцией, демографическими изменениями, экологическими рисками и истощением природных ресурсов. Одновременно процессы глобализации, цифровизации и взаимозависимости государств создают новые каналы распространения угроз, позволяя отдельным государственным и негосударственным субъектам воздействовать на политическую, экономическую и социальную стабильность других государств без непосредственного применения традиционной военной силы.

Особое место в данной системе занимают асимметричные угрозы, характерной особенностью которых является использование субъектом, обладающим относительно ограниченными ресурсами, нестандартных средств и методов для воздействия на более сильного противника и нейтрализации его преимуществ. Такие угрозы могут реализовываться в различных формах — от информационно-психологического воздействия и распространения дезинформации до кибератак, вмешательства в работу критической инфраструктуры, манипулирования общественным мнением и использования цифровых платформ в целях дестабилизации общественно-политической ситуации.

Актуальность исследования асимметричных угроз особенно возрастает в условиях формирования информационного общества, в котором информационное пространство становится одним из важнейших элементов национальной безопасности. Расширение использования информационно-коммуникационных технологий, социальных сетей, цифровых платформ и искусственного интеллекта существенно увеличивает возможности воздействия на общественное сознание и государственные институты. При этом информационные операции могут осуществляться скрытно, дистанционно и с использованием анонимных или трансграничных каналов, что затрудняет установление источника угрозы, определение истинных целей воздействия и своевременное принятие соответствующих мер реагирования.

В этих условиях информационная война становится одним из важных инструментов достижения политических, экономических и военно-стратегических целей. Воздействие на информационную среду может быть направлено не только на получение или уничтожение информации, но и на формирование определённых общественных настроений, подрыв доверия к государственным институтам, искажение восприятия происходящих событий, распространение ложной информации и ослабление общественной устойчивости. Поэтому обеспечение национальной безопасности требует формирования комплексной системы, способной одновременно защищать информационные ресурсы, цифровую инфраструктуру и общественное информационное пространство.

Для Азербайджанской Республики данная проблематика имеет особое стратегическое значение. Геополитическое положение страны, динамика региональной безопасности, наличие сложной системы политических, экономических и информационных взаимосвязей, а также возрастающая роль цифровых технологий обусловливают необходимость постоянного совершенствования механизмов защиты национальных интересов. Современная система обеспечения национальной безопасности Азербайджана должна учитывать не только традиционные формы внешних и внутренних угроз, но и новые способы воздействия, реализуемые посредством информационного и киберпространства.

Концептуальный подход к обеспечению национальной безопасности Азербайджанской Республики основывается на защите независимости государства, территориальной целостности, конституционного строя, национальных интересов народа и государства, а также на предотвращении и нейтрализации внутренних и внешних угроз. Принятие Концепции национальной безопасности Азербайджанской Республики стало важным институциональным этапом систематизации основных целей, принципов и приоритетов государственной политики в данной сфере. Концепция исходит из комплексного характера национальной безопасности и предусматривает взаимосвязанное развитие таких направлений, как оборона, внешняя политика, экономика, социальная сфера, культура, наука и образование, здравоохранение, транспорт и другие стратегически важные области [2, 3].

Такой подход свидетельствует о постепенном переходе от узкого понимания национальной безопасности как преимущественно военно-политической категории к её комплексному восприятию. В современных условиях устойчивость государства определяется совокупностью факторов, включающих способность государственных институтов противостоять внешнему и внутреннему воздействию, устойчивость экономики и социальной системы, защищённость критической инфраструктуры, уровень технологической независимости, информационную устойчивость общества и способность государства своевременно реагировать на новые формы угроз.

Особую значимость в данном контексте приобретает информационная и кибербезопасность. Цифровизация государственного управления, экономики, социальной сферы и предоставления государственных услуг приводит к тому, что функционирование государства всё в большей степени зависит от устойчивости информационных систем и цифровой инфраструктуры. Нарушение их работы, несанкционированный доступ к информационным ресурсам, утечка данных, кибератаки на объекты критической инфраструктуры и целенаправленное информационно-психологическое воздействие способны вызвать последствия, выходящие далеко за пределы информационной сферы и непосредственно затрагивающие национальную безопасность.

В этой связи особое значение приобретает формирование современной государственной политики в области информационной безопасности и кибербезопасности. Анализ и объективная оценка существующего состояния информаци-

онной среды, выявление актуальных и потенциальных рисков, прогнозирование возможных последствий и формирование эффективных механизмов реагирования являются необходимыми условиями устойчивого функционирования национальной системы безопасности. Использование методов стратегического анализа, включая SWOT-анализ, позволяет систематизировать сильные и слабые стороны существующей системы, определить имеющиеся возможности и потенциальные угрозы, а также сформировать приоритетные направления дальнейшего развития.

Важным этапом институционального развития данной сферы стала разработка и реализация Стратегии на 2023-2027 годы в области информационной безопасности и кибербезопасности. Стратегический подход предполагает не только совершенствование механизмов защиты информации, но и развитие национального потенциала в сфере кибербезопасности, повышение устойчивости критической информационной инфраструктуры, совершенствование механизмов мониторинга и реагирования на киберинциденты, защиту персональных данных и повышение безопасности цифровых услуг.

Особое внимание в рамках современных стратегических подходов уделяется развитию технологических возможностей, в том числе применению технологий искусственного интеллекта для выявления и оценки рисков, прогнозирования угроз, мониторинга информационной среды и противодействия информационной агрессии. Одновременно актуальными становятся поддержка отечественных производителей и стартапов в сфере информационной безопасности, развитие научно-технического потенциала, подготовка квалифицированных кадров и повышение уровня цифровой и информационной грамотности населения.

Таким образом, трансформация характера современных угроз требует переосмысления традиционных подходов к обеспечению национальной безопасности. В условиях асимметричных угроз и информационной войны устойчивость государства определяется не только его военным и экономическим потенциалом, но и способностью защищать собственное информационное пространство, критическую цифровую инфраструктуру и общество от различных форм информационного и кибернетического воздействия.

Глава 1. Концептуальные основы обеспечения национальной безопасности Азербайджана в условиях асимметричных угроз и информационной войны

1.1. Асимметричные угрозы и информационная война как современные факторы национальной безопасности

Актуальность настоящего исследования обусловлена необходимостью комплексного рассмотрения концептуальных и институциональных основ обеспечения национальной безопасности Азербайджанской Республики в условиях возрастающей роли асимметричных угроз и информационной войны. Исследование направлено на выявление основных тенденций трансформации современных угроз, анализ существующих механизмов информационной и кибербезопасности Азербайджана, а также определение направлений дальнейшего совершенствования государственной политики в данной сфере. Особое внимание уделяется взаимосвязи между защитой национального информационного пространства, обеспечением киберустойчивости, противодействием дезинформации и формированием комплексной системы национальной безопасности, способной эффективно реагировать на динамично изменяющийся характер современных угроз. Расширение борьбы с киберпреступностью, включая развитие киберкриминалистических возможностей, стимулирование научно-исследовательских и экспериментально-проектных работ в области информационной безопасности, а также разработка конкурентоспособных продуктов и технологий также входят в число стратегических целей. Кроме того, планируется определить требования к компетенциям в соответствующей области, разработать образовательные и учебные программы, усилить подготовку квалифицированных кадров и расширить возможности трудоустройства специалистов по информационной безопасности. Важным направлением также является формирование культуры информационной безопасности и просвещение общества. В этом контексте к основным целям относятся защита детей от глобальных и опасных информационных угроз, исходящих из интернет-среды, создание экосистемы информационной и кибербезопасности, расширение применения международных стандартов в стране и улучшение позиций Азербайджана в международных рейтингах. Одновременно планируется активизировать деятельность образовательных учреждений в области информационной безопасности, создать новые учебные центры и совместные

лаборатории с международными компаниями. Одной из важных целей обеспечения информационной безопасности является своевременное выявление существующих рисков безопасности в информационном пространстве, особенно в критически важных информационных инфраструктурах, и усиление готовности к ним. Для этого особое значение имеет развитие структурных подразделений информационной безопасности и сетей CERT, а также улучшение их взаимодействия. Параллельно в качестве важных стратегических направлений определены формирование индустрии информационной безопасности и кибербезопасности, снижение прямой зависимости от зарубежных технологий, поддержка развития программной инженерии и цифровой экономики, а также продвижение инновационных решений и стартапов. Глобальный характер информационной безопасности и кибербезопасности требует усиления как внутреннего, так и международного сотрудничества в этой области. Установление сотрудничества между государственными учреждениями, уполномоченными органами, CERT, частным сектором, организациями гражданского общества и другими заинтересованными сторонами в областях правового, организационного, технико-технологического, образовательного и скоординированного реагирования на инциденты является одним из главных условий национальной информационной безопасности. Тот факт, что частный сектор владеет определенной частью критической инфраструктуры и является одним из основных поставщиков ИКТ-услуг, повышает его роль в обеспечении информационной безопасности. Поэтому для частного сектора важно соблюдать требования информационной безопасности в своей деятельности и адаптировать предоставляемые услуги и ИКТ-продукты к соответствующим стандартам безопасности. Расширение внутреннего и международного сотрудничества создает условия для укрепления координации между государством, частным сектором и гражданским обществом, совершенствования управления информационной безопасностью и непрерывного развития национальных возможностей в области кибербезопасности [1, с.148].

Возрастающая важность киберпространства в сфере безопасности обусловила необходимость рассмотрения вопросов киберзащиты как отдельного стратегического направления в национальной политике безопасности государств. В этом контексте Центр передового опыта НАТО по совместной киберзащите (CCDCOE) привлекает внимание как одна из международных платформ, объединяющих научные исследования, экспертную и учебную деятельность в области киберзащиты и кибербезопасности. Деятельность центра охватывает различные области, связанные с изучением сущности киберугроз, развитием возможностей киберзащиты и укреплением потенциала безопасности государств в цифровой среде.

Одной из главных особенностей, отличающих киберугрозы от других угроз безопасности, является то, что они не ограничиваются географическими границами. Воздействие, осуществляемое с использованием цифровой инфраструктуры, может быть направлено на государственные учреждения, критически важные информационные системы, экономическую инфраструктуру и информационную среду общества. Эта особенность усиливает асимметричный характер киберугроз. В таких условиях атакующей стороне не обязательно обладать превосходящими техническими или материальными возможностями по сравнению с защищаемой стороной; воздействие на важные информационные и инфраструктурные объекты возможно даже при относительно ограниченных ресурсах. Подходы CCDCOE позволяют сформировать комплексную перспективу безопасности, показывая, что кибербезопасность не сводится только к применению технических средств защиты. Помимо технологических возможностей, защита киберсреды требует взаимодействия таких компонентов, как правовое регулирование, институциональная координация, развитие человеческих ресурсов, оценка рисков и международное сотрудничество. В этом контексте, помимо предотвращения кибер-инцидентов, важным элементом политики национальной безопасности можно считать также повышение устойчивости к последствиям возможных атак. Взаимодействие государственной деятельности в киберпространстве и международного права также является одним из основных направлений современных исследований в области безопасности. В этом контексте Таллиннское руководство 2.0 по международному праву, применимому к кибер-операциям, подготовленное в рамках CCDCOE, является важным научным источником, систематизирующим применение норм международного права к операциям, проводимым в киберпространстве, на основе экспертных подходов. В работе рассматриваются различные

вопросы, связанные с оценкой государственной деятельности в киберпространстве с точки зрения международного права, включая рассмотрение таких правовых категорий, как государственная ответственность, суверенитет и применение силы в цифровой среде. С точки зрения национальной безопасности Азербайджана, важность этих подходов особенно очевидна в таких областях, как защита критически важных информационных инфраструктур, повышение устойчивости государственных информационных систем, развитие оперативных возможностей реагирования на кибер-инциденты и защита информационного пространства. Поскольку киберугрозы в современных условиях могут взаимодействовать с другими средствами информационной войны, подход, основанный исключительно на технической защите, недостаточен для их предотвращения. Координация киберзащиты, информационной безопасности, стратегической коммуникации, правовых механизмов и международного сотрудничества в рамках единой системы безопасности создает условия для достижения более устойчивых результатов. В этом контексте научные исследования и экспертные подходы Центра координации кибербезопасности НАТО могут служить одной из теоретических основ для оценки воздействия асимметричных угроз на национальную безопасность. В частности, трансграничный и многогранный характер киберугроз требует усиления превентивных мер, преемственности и институционального сотрудничества в политике безопасности государств [4].

Быстрое развитие цифровых технологий не только повысило значимость информационной среды с точки зрения безопасности, но и облегчило распространение различных информационных эффектов среди более широкой аудитории. В этом контексте распространение заведомо ложного и манипулятивного контента становится фактором угрозы, способным повлиять на восприятие информации обществом, связи с общественностью и процессы принятия решений. В частности, целенаправленное использование информационного пространства иностранными субъектами создает новые вызовы для информационной безопасности государств. Европейская служба внешних действий (ЕВС) оценивает иностранное манипулирование информацией и вмешательство в нее как одну из важных проблем современной среды безопасности. В этом подходе основное внимание уделяется не только содержанию ложной информации, но и цели, средствам и аудитории, для которой эта информация предназначена. Такие эффекты могут быть направлены на влияние на направление общественных дебатов, создание путаницы вокруг определенных тем и усиление недоверия в обществе с использованием различных каналов коммуникации. Деятельность платформы EUvsDisinfo основана на выявлении и анализе конкретных примеров манипулирования информацией. Платформа изучает особенности распространения различных информационных нарративов и готовит материалы, позволяющие более точно оценивать информацию, представляемую общественности. Такой подход показывает, что одних лишь технических мер защиты недостаточно для обеспечения современной информационной безопасности; большое значение также имеют анализ источников информации, повышение медиаграмотности населения и своевременное выявление манипулятивного контента.

Эффективность борьбы с дезинформацией также зависит от информационной устойчивости общества. Развитие способности оценивать источник, цель и уровень достоверности информации может снизить вероятность того, что люди будут подвержены влиянию манипулятивного контента. В этом отношении важными компонентами информационной безопасности являются развитие медиаграмотности, повышение доступности надежных информационных каналов и установление прозрачной и оперативной коммуникации между государственными органами и общественностью.

В контексте национальной безопасности Азербайджана, манипулирование иностранной информацией и дезинформация являются областями, требующими внимания, особенно в контексте информационной войны. Важно разработать механизмы непрерывного мониторинга и аналитической оценки для своевременного выявления информационных кампаний, направленных на подрыв политической и социальной стабильности государства, его международного имиджа, национальных интересов и общественного мнения. В то же время, ответные меры на подобные угрозы не должны ограничиваться лишь опровергающей коммуникацией, а должны дополняться превентивной информацией, стратегической коммуникацией и повышением информационной устойчивости общества. Одним из главных направлений подхода ОБСЕ (ОБСЕ)

к безопасности, связанной с использованием информационно-коммуникационных технологий, является укрепление доверия и взаимного сотрудничества между государствами. В рамках резолюции Постоянного Совета Организации № 1106, принятой в 2013 году, были определены меры по укреплению доверия с целью снижения рисков конфликтов, которые могут возникнуть в результате использования ИКТ. Эти меры включают развитие коммуникационных возможностей между соответствующими государственными органами, расширение обмена информацией и усиление взаимной деятельности, связанной с безопасностью в киберпространстве.

Резолюция № 1202, принятая в 2016 году, дополнительно развила механизмы сотрудничества в этом направлении. В подходе ОБСЕ наличие связей между государствами, оперативный обмен информацией о кибер-инцидентах и предотвращение возможных недоразумений имеют большое значение для поддержания стабильности в киберпространстве. Такие механизмы служат для снижения вероятности того, что инциденты, происходящие в киберпространстве, перерастут в более широкий политический кризис и кризис безопасности.

Этот концептуальный подход ОБСЕ тесно связан с характеристиками асимметричных угроз. Для осуществления кибератак не обязательно обладать традиционной военной мощью. Различные государственные и негосударственные субъекты, используя технологические возможности, могут воспользоваться слабостями информационных систем и оказать значительное воздействие на субъектов, обладающих большими ресурсами. В то же время сложность выявления источника киберугроз затрудняет их предотвращение и точное определение ответственности. Эта особенность делает киберпространство благоприятной средой для применения инструментов асимметричного влияния. Особое значение имеет также взаимодействие между кибербезопасностью и информационной безопасностью. В условиях современной информационной войны технические кибератаки могут осуществляться параллельно с дезинформацией, манипулированием информацией и инструментами психологического воздействия. В результате целью атаки может быть не только нарушение функционирования информационных систем, но и влияние на общественное мнение, социальную стабильность и доверие к государственным институтам. Поэтому, помимо киберзащиты, важными направлениями в системе национальной безопасности следует также считать мониторинг информационной среды, стратегическую коммуникацию и укрепление информационной устойчивости общества.

Важность такого подхода для Азербайджана обусловлена тем, что цифровая инфраструктура и информационные ресурсы страны стали одним из важнейших элементов национальной безопасности. В условиях, когда киберугрозы, манипулирование информацией и другие асимметричные средства воздействия могут применяться взаимно, необходимо укреплять координацию между государственными органами, частным сектором и другими соответствующими субъектами. Одновременно с этим, раннее выявление кибер-инцидентов, защита критической информационной инфраструктуры, оперативный обмен информацией и расширение международного сотрудничества позволяют повысить устойчивость национальной информационной безопасности. Важный стратегический шаг в этом направлении был сделан в Азербайджанской Республике 28 августа 2023 года. В этот день указом Президента Азербайджанской Республики № 4060 была утверждена «Стратегия Азербайджанской Республики по информационной безопасности и кибербезопасности на 2023-2027 годы».

Принятие стратегии имеет большое значение с точки зрения объединения государственной политики в области информационной безопасности и кибербезопасности в единую стратегическую структуру. Тот факт, что документ охватывает 2023-2027 годы, создает условия для управления рисками, возникающими в информационном пространстве и цифровой инфраструктуре, не посредством краткосрочных мер, а на основе последовательного и долгосрочного подхода. Одна из главных целей такого подхода - укрепление безопасности государственных информационных ресурсов и информационных систем, повышение уровня готовности к киберугрозам и обеспечение устойчивости цифровой среды.

Важной особенностью стратегии является то, что она предусматривает обеспечение информационной безопасности на основе скоординированной деятельности различных государственных органов. В этом направлении предполагается координировать деятельность Государственной службы по специальной связи и информационной безопасности, Министерства цифрового развития и транспорта, Службы государственной

безопасности, Министерства юстиции, Министерства внутренних дел, Министерства науки и образования, Министерства экономики и других соответствующих государственных органов. Такая институциональная модель обеспечивает подход к информационной безопасности не как к ограниченной сфере деятельности отдельных ведомств, а как к комплексному направлению безопасности на государственном уровне.

3 октября 2023 года имеет особое значение с точки зрения практической реализации Стратегии. В этот день Кабинетом Министров Азербайджанской Республики было принято решение, направленное на обеспечение выполнения Плана действий по реализации Стратегии. В этом документе были определены конкретные задачи, поставленные перед различными государственными ведомствами в отношении реализации отдельных направлений Стратегии, а также механизмы координации и взаимодействия между соответствующими ведомствами. Таким образом, институциональные механизмы практической реализации стратегической рамочной программы, утвержденной 28 августа 2023 года, были более конкретно определены 3 октября 2023 года.

Этот стратегический подход к информационной и кибербезопасности напрямую связан с характеристиками асимметричных угроз. Современные киберугрозы способны оказывать более широкое воздействие при меньших ресурсах, чем традиционная военная конфронтация. Атаки, осуществляемые в киберпространстве, могут повлиять на функционирование государственных информационных систем, критической инфраструктуры, экономических процессов и общественной безопасности. При этом, когда манипулятивное воздействие, дезинформация и другие средства воздействия, направленные на информационную среду, используются параллельно с техническими кибератаками, представляемый ими риск для безопасности становится еще более сложным. В этом контексте значение Стратегии не ограничивается технической защитой информационных систем. Укрепление координации между государственными органами, повышение готовности к кибер-инцидентам, защита информационных ресурсов, подготовка соответствующих специалистов и развитие институционального потенциала в области кибербезопасности являются важными условиями для всестороннего обеспечения национальной безопасности. В частности, в контексте информационной войны, наряду с технологической безопасностью, важно также укрепление информационной устойчивости общества и стратегических коммуникационных возможностей государства.

ЗАКЛЮЧЕНИЕ

Таким образом, Стратегия на 2023-2027 годы, утверждённая приказом № 4060 от 28 августа 2023 года, представляет собой один из ключевых стратегических документов, определяющих приоритетные направления государственной политики Азербайджана в сфере информационной безопасности и кибербезопасности на современном этапе. Её значение обусловлено не только необходимостью защиты информационных ресурсов и цифровой инфраструктуры государства, но и формированием устойчивой системы противодействия современным угрозам, приобретающим всё более сложный, трансграничный и асимметричный характер.

Определение 3 октября 2023 года институциональных мер, направленных на реализацию Плана действий по осуществлению Стратегии, стало важным этапом перехода от концептуального определения приоритетов к формированию практических механизмов их реализации. В данном контексте особое значение приобретает обеспечение эффективного взаимодействия государственных органов, организаций, субъектов критической информационной инфраструктуры и иных участников цифровой среды. Такой подход позволяет рассматривать информационную и кибербезопасность не только как отдельное направление государственной политики, но и как составную часть системы обеспечения национальной безопасности.

Совместный анализ указанных документов показывает, что современная государственная политика Азербайджана в данной сфере ориентирована на комплексное укрепление национального информационного пространства, повышение его устойчивости к внешним и внутренним угрозам, совершенствование механизмов предупреждения и нейтрализации кибератак, а также развитие институционального и правового потенциала государства. При этом особую актуальность приобретает противодействие асимметричным угрозам, которые могут реализовываться посредством информационно-психологических операций, распространения дезинформации, манипу-

лирования общественным мнением, кибератак на критическую инфраструктуру и использования цифровых технологий в целях дестабилизации общественно-политической и экономической ситуации [5].

В условиях информационной войны защита национальной безопасности требует перехода от преимущественно реактивной модели противодействия угрозам к превентивной и риск-ориентированной модели, основанной на постоянном мониторинге информационной среды, раннем выявлении потенциальных угроз, оперативном обмене информацией и координации деятельности соответствующих государственных институтов. Важное значение при этом имеют развитие национальных возможностей в области киберразведки и киберзащиты, повышение уровня цифровой грамотности населения, подготовка квалифицированных специалистов, совершенствование механизмов защиты персональных данных и критической информационной инфраструктуры.

Следовательно, обеспечение национальной безопасности Азербайджана в условиях асимметричных угроз и информационной войны должно основываться на системном сочетании правовых, институциональных, технологических, организационных и информационно-коммуникационных мер. Эффективность такой системы во многом определяется способностью государства своевременно адаптироваться к динамично изменяющемуся характеру угроз, обеспечивать устойчивость ключевых информационных и цифровых систем и формировать механизмы стратегического реагирования на новые формы информационного воздействия.

В конечном итоге реализация положений Стратегии на 2023-2027 годы и соответствующего Плана действий создаёт основу для дальнейшего совершенствования национальной системы информационной и кибербезопасности Азербайджана. При этом стратегической задачей остаётся формирование целостной и устойчивой системы защиты национального информационного пространства, способной не только минимизировать последствия существующих угроз, но и своевременно выявлять, предупреждать и нейтрализовать новые формы асимметричного воздействия. Это, в свою очередь, является важным условием обеспечения информационного суверенитета, устойчивого социально-экономического развития и национальной безопасности Азербайджанской Республики в условиях цифровой трансформации и возрастающей роли информационного пространства в современных международных отношениях [6].

СПИСОК ЛИТЕРАТУРЫ:

1. Хасаналиев З.М. Основы национальной безопасности Азербайджанской Республики (Учебник). г.Баку, 2016г., 176 с.
2. Закон Азербайджанской Республики (от 22 декабря 2023 г.). О внесении изменений в Закон Азербайджанской Республики «О национальной безопасности» (№ 1060-VIQD). Газета «Азербайджан», № 4.

Интернет-ресурсы:

3. https://e-qanun.az/framework/13373
4. https://doi.org/10.1017/9781316822524
5. https://cert.gov.az/az/page/documents

ASİMMETRİK TƏHDİDLƏR VƏ İNFORMASİYA MÜHARİBƏSİ ŞƏRAİTİNDƏ AZƏRBAYCANIN MİLLİ TƏHLÜKƏSİZLİYİNİN TƏMİN EDİLMƏSİNİN KONSEPTUAL ƏSASLARI

Leyla Elçin qızı Nəcəfova Əlizadə
Bakı Dövlət Universitetinin doktorantı

XÜLASƏ

Müasir təhlükəsizlik mühitində rəqəmsal texnologiyaların geniş yayılması və informasiya məkanının dövlətlərarası münasibətlərdə təsir imkanlarının artması milli təhlükəsizliyə yönələn təhdidlərin yeni formalarının meydana çıxmasına şərait yaratmışdır. Məqalədə Azərbaycanın milli təhlükəsizliyinə təsir göstərə bilən asimmetrik təhdidlərin xarakteri informasiya müharibəsi kontekstində nəzərdən keçirilir. Kiberhücumlar, dezinformasiya, informasiya manipulyasiyası və psixoloji təsir kimi vasitələrin dövlətin informasiya məkanına və ümumi təhlükəsizlik mühitinə təsir imkanları təhlil edilir. Bununla yanaşı, informasiya və kibertəhlükəsizliyin təmin olunması, kritik informasiya infrastrukturunun qorunması, potensial təhdidlərin vaxtında müəyyənləşdirilməsi və informasiya mühitində dayanıqlılığın formalaşdırılması məsələləri önə çəkilir. Azərbaycanın milli təhlükəsizliyinin müasir çağırışlara uyğun qorunması

üçün institusional koordinasiyanın gücləndirilməsi, strateji kommunikasiyanın inkişaf etdirilməsi, cəmiyyətin informasiya savadlılığının artırılması və beynəlxalq əməkdaşlığın genişləndirilməsi mühüm istiqamətlər kimi qiymətləndirilir.

Açar sözlər: *asimmetrik təhdidlər, informasiya müharibəsi, milli təhlükəsizlik, informasiya təhlükəsizliyi, kibertəhlükəsizlik, dezinformasiya, informasiya manipulyasiyası, strateji kommunikasiya.*

CONCEPTUAL FRAMEWORK FOR ENSURING THE NATIONAL SECURITY OF AZERBAIJAN UNDER CONDITIONS OF ASYMMETRIC THREATS AND INFORMATION WARFARE

Leyla Elchin Najafova Alizada
Doctoral Student, Baku State University

SUMMARY

In the modern security environment, the widespread use of digital technologies and the increased influence of the information space in interstate relations have created conditions for the emergence of new forms of threats to national security. The article examines the nature of asymmetric threats that can affect the national security of Azerbaijan in the context of information warfare. The impact of tools such as cyberattacks, disinformation, information manipulation and psychological influence on the state's information space and the general security environment is analyzed. In addition, the issues of ensuring information and cyber security, protecting critical information infrastructure, timely identification of potential threats and forming resilience in the information environment are highlighted. Strengthening institutional coordination, developing strategic communication, increasing information literacy of society and expanding international cooperation are considered important directions for protecting Azerbaijan's national security in line with modern challenges.

Keywords: *asymmetric threats, information warfare, national security, information security, cybersecurity, disinformation, information manipulation, strategic communication.*

Rəyçi: Siyasi elmlər üzrə fəlsəfə doktoru, dosent Səbinə Qaraşova

Məqalə redaksiyaya daxil olub: 11.07.2026
Çapa qəbul olunub: 04.08.2026
The date of the admission of the article to the editorial office: 11.07.2026
Accepted for publication: 04.08.2026