

## АҚПАРАТТЫҚ СОҒЫС: ТЕОРИЯЛЫҚ ТҰЖЫРЫМ ЖӘНЕ ПРАКТИКАДАҒЫ ҚОЛДАНЫС

**Н. И. Байғараев**

### АНДАТПА

Бұл мақалада «ақпараттық соғыс» феноменінің теориялық негіздері мен қазіргі халықаралық қатынастардағы практикалық қолданылуы кешенді түрде талданады. Зерттеу барысында ақпараттық соғыс ұғымына қатысты әртүрлі ғылыми анықтамалар мен тұжырымдамалар салыстырылып, оның бірыңғай теориялық моделінің қалыптаспағаны және көпқырлы, пәнаралық сипатқа ие екені анықталды. Автор ақпараттық соғыстың технологиялық, психологиялық және стратегиялық өлшемдерін бөліп көрсетіп, оның гибридік қақтығыстар жүйесіндегі дербес әрі маңызды рөлін негіздейді. Мақалада ақпараттық соғыстың негізгі белгілері, түрлері мен жіктемелері жүйеленіп, әртүрлі ғылыми мектептердің көзқарастарының ұқсастықтары мен айырмашылықтары сараланады. Сонымен қатар саяси мәлімдемелер, медиа ықпал және кибероперациялар мысалында ақпараттық соғыстың практикадағы көріністері талданып, оның қоғамдық санаға, шешім қабылдау процесіне және ақпараттық инфрақұрылымға әсер ету механизмдері айқындалады. Зерттеу нәтижелері ақпараттық соғыстың қазіргі кезеңде тек әскери құрал емес, әлеуметтік, технологиялық және когнитивтік ықпал етудің қуатты тетігіне айналғанын көрсетеді. Ақпараттық соғыс жүргізілген жағдайда оның салдары ұзақ мерзімді сипатқа ие болып, қоғамның құндылық жүйесіне терең өзгерістер енгізуі мүмкін екені дәлелденеді. Осыған байланысты оны кешенді әрі пәнаралық тұрғыдан зерттеу қажеттігі негізделеді.

**Түйін сөздер:** ақпараттық соғыс, ақпараттық күрес, кибер шабуыл, қоғамдық сана, психологиялық ықпал, ақпараттық қысым.

Л.Н.Гумилев атындағы  
Еуразия ұлттық университеті,  
Астана, Қазақстан

**Автор-корреспондент:**

Н.И.Байғараев,  
baunur01@gmail.com

**Сілтеме:**

Байғараев Н. Ақпараттық соғыс: теориялық тұжырым және практикадағы қолданыс // Адам әлемі. – 2026. – Т. 28. – №2 (108). – Б. 230-240. – DOI: 10.48010/dpv2qw77

**Ашық қолжетімділік**

© Автор(лар), 2026  
Бұл ашық қолжетімді мақала Creative Commons Attribution 4.0 International License (CC BY 4.0) лицензиясының талаптарына сәйкес таратылады.  
<https://creativecommons.org/licenses/by-nc-nd/4.0/>

Редакцияға түсті: 25/03/2026  
Қабылданды: 27/05/2026  
Онлайн жарияланды: 30/06/2026

### Информационная война: теоретическая концепция и практическое применение

**Аннотация.** В данной статье комплексно анализируются теоретические основы феномена «информационной войны» и его практическое применение в современных международных отношениях. В ходе исследования сопоставляются различные научные определения и концепции информационной войны, в результате чего выявляется отсутствие единой универсальной теоретической модели, а также подчеркивается ее многогранный и междисциплинарный характер. Автор выделяет технологическое, психологическое и стратегическое измерения информационной войны, обосновывая ее самостоятельную и значимую роль в системе гибридных конфликтов. В статье систематизируются основные признаки, виды и классификации информационной войны, а также проводится сравнительный анализ сходств и различий между подходами различных научных школ. Кроме того, на примере политических заявлений, медийного воздействия и киберопераций рассматриваются практические проявления информационной войны, раскрываются механизмы ее влияния на общественное сознание, процессы принятия решений и информационную инфраструктуру. Результаты исследования показывают, что на современном этапе информационная война превратилась не только в военный инструмент, но и в мощный механизм социального, технологического и когнитивного воздействия. Доказывается, что последствия ее применения могут носить долгосрочный характер и приводить к глубоким трансформациям ценностной системы общества. В этой связи обосновывается необходимость ее всестороннего и междисциплинарного изучения.

**Ключевые слова:** информационная война, информационное противоборство, кибератака, общественное сознание, психологическое воздействие, информационное давление.

### Information warfare: theoretical concept and practical application

**Abstract.** This article offers a comprehensive examination of the theoretical foundations underlying the phenomenon of «information warfare» and its practical applications in contemporary international relations. The study compares various academic definitions and conceptual approaches to information warfare, revealing the absence of a unified theoretical model and highlighting its multidimensional and interdisciplinary nature. The author distin-

guishes technological, psychological, and strategic dimensions of information warfare, substantiating its independent and significant role within the system of hybrid conflicts.

The article systematizes the main characteristics, types, and classifications of information warfare, while also offering a comparative analysis of similarities and differences among various academic schools of thought. In addition, practical manifestations of information warfare are examined through examples such as political statements, media influence, and cyber operations. The study further identifies the mechanisms through which information warfare affects public consciousness, decision-making processes, and information infrastructure.

The findings demonstrate that, at the present stage, information warfare has evolved beyond a purely military instrument into a powerful tool of social, technological, and cognitive influence. It is argued that its consequences can be long-term in nature, potentially leading to profound transformations in the value systems of society. In this regard, the necessity of its comprehensive and interdisciplinary study is strongly justified.

**Keywords:** Information Warfare, Information Confrontation, Cyberattack, Public Consciousness, Psychological Influence, Information Pressure.

### Кіріспе

Қазіргі халықаралық қатынастар жүйесінде ақпараттық технологиялар маңызының артуы «ақпараттық соғыс» ұғымын ғылыми және практикалық тұрғыдан өзекті зерттеу нысанына айналдырды. Бұл феноменнің мазмұны мен мәнін түсіндіруге бағытталған еңбектер саны артқанымен, ғылыми әдебиеттерде оның бірыңғай, әмбебап анықтамасы қалыптаспаған. Керісінше, әртүрлі зерттеушілер ақпараттық соғысты өз ғылыми парадигмаларына сәйкес түрлі қырынан қарастырады. Біреулері оны әскери-стратегиялық құрал ретінде түсіндірсе, енді біреулері психологиялық ықпал ету тетігі немесе ақпараттық-коммуникациялық технологияларға негізделген күрделі жүйе ретінде сипаттайды.

Осыған байланысты ақпараттық соғысқа қатысты теориялық көзқарастар мен жіктелердің әралуандығы байқалады. Әртүрлі ғылыми мектептер ұсынған тұжырымдамалар бұл құбылыстың көпқырлы табиғатын ашуға мүмкіндік бергенімен, олардың арасында ортақ концептуалдық негіздің жеткіліксіздігі сезіледі. Бұл жағдай ақпараттық соғысты түсіндіруде белгілі бір фрагментарлықтың бар екенін және оны жүйелеу қажеттігін көрсетеді. Сондықтан қолданыстағы теориялар мен модельдер салыстырмалы тұрғыда талданады, олардың ұқсастықтары мен айырмашылықтары анықталады. Бұл – осы зерттеудің негізгі мақсатының бірі. Сондай жұмыстың негізінде «ақпараттық соғыс» ұғымына жаңа анықтама ұсынылады. Бұл автор мақаласының өзге еңбектерден айырмашылығы болады.

Сонымен қатар ақпараттық соғыс тек теориялық категория ретінде ғана емес, қазіргі геосаяси процесте белсенді қолданылатын практикалық құрал ретінде де маңызды. Соңғы жылдары болған қарулы қақтығыстар мен саяси текетірестер ақпараттық ықпал ету механизмдерінің тиімділігін және олардың стратегиялық маңызын айқын көрсетті. Бұл

өз кезегінде ақпараттық соғысты тек әскери әрекеттердің қосымша элементі емес, дербес ықпал ету құралы ретінде қарастыру қажеттігін алға тартады.

Осы тұрғыдан алғанда аталған зерттеудің мақсаты – ақпараттық соғыс ұғымының теориялық негіздерін талдау, әртүрлі ғылыми көзқарастарды салыстыру және оның қазіргі заманғы халықаралық қатынастардағы практикалық қолданылуын айқындау. Зерттеу барысында ақпараттық соғыстың мәні, негізгі белгілері, түрлері мен жүзеге асу механизмдері кешенді түрде қарастырылады.

### Әдіснама

Аталған зерттеу жұмысы кешенді сипатқа ие болып, ақпараттық соғыс феноменін теориялық және эмпирикалық деңгейде талдауға бағытталды. Зерттеу барысында бірнеше ғылыми әдістер жүйелі түрде қолданылды. Ең алдымен, теориялық талдау әдісі кеңінен пайдаланылды. Бұл әдіс арқылы ақпараттық соғыс ұғымына қатысты шетелдік зерттеушілердің еңбектері қарастырылып, олардың анықтамалары, тұжырымдамалары мен көзқарастары салыстырмалы түрде зерделенді.

Сонымен қатар салыстырмалы талдау әдісі қолданылды. Бұл әдіс ақпараттық соғыстың түрлі жіктелерін (функционалдық, технологиялық, психологиялық және стратегиялық) өзара салыстыруға мүмкіндік берді. Нәтижесінде, әртүрлі авторлар ұсынған модельдердің артықшылықтары мен шектеулері анықталып, олардың бір-бірін толықтыратын тұстары айқындалды.

Зерттеуде жүйелік талдау әдісі де маңызды рөл атқарды. Ақпараттық соғыс біртұтас жүйе ретінде қарастырылып, оның құрылымдық элементтері (ақпараттық ықпал ету құралдары, субъектілері, нысандары, мақсаттары) өзара байланыста зерттелді. Бұл әдіс ақпараттық соғыстың тек жеке әрекеттер жиынтығы емес,

белгілі бір логикаға бағынатын, ұйымдасқан және мақсатты ықпал ету жүйесі екенін көрсетуге мүмкіндік берді.

Практикалық бөлімде кейс-стади әдісі қолданылды. Заманауи халықаралық қатынастардағы нақты мысалдар (саяси мәлімдемелер, әлеуметтік желілердегі ақпараттық ықпал, кибершабуылдар) талданып, ақпараттық соғыстың практикадағы көріністері қарастырылды. Бұл тәсіл теориялық тұжырымдардың нақты жағдайларда қалай жүзеге асатынын көрсетуге мүмкіндік берді.

Сондай-ақ контент-талдау элементтері пайдаланылды. Саяси лидерлердің мәлімдемелері, медиа кеңістіктегі ақпараттық хабарламалар мен дискурстар мазмұндық тұрғыдан талданып, олардың ықпал ету сипаты, мақсаттары мен аудиторияға әсер ету механизмдері анықталды. Бұл әдіс ақпараттық соғыстың психологиялық және коммуникативтік аспектілерін ашуға ықпал етті.

### Негізгі бөлім

«Ақпараттық соғыс» ұғымы ХХ ғасырда пайда болғанымен, оның әдіс-амалдары ертерек қолданыла бастады. Наполеон Бонапарттың кең тараған «төрт жүз мың әскерге қарағанда төрт газет жауға көбірек шығын келтіреді» деген сөзі ақпараттық соғыстың мәнін ашады. Ал Бірінші дүниежүзілік соғыс кезінде-ақ «пропаганда» термині қолданысқа еніп, үгіт-насихат технологиялары кеңінен пайдаланылған. Антанта елдері сол кезде неміс қалалары мен елді-мекендеріне 30 млн үгіт парақша, газет, брошюра таратқан екен [1]. Ал Екінші дүниежүзілік соғыста Германия пропаганданы мықтап қолға алып, 1933 жылы арнайы министрлік құрып, оның басшысы Йозеф Геббельс бұл іспен кәсіби түрде айналысты. Аталған министрліктің бюджеті жыл сайын өсіп, 1941 жылы 187 млн рейхсмаркаға жеткен [2]. Яғни, ақпараттық соғыс тәсілдері өткен ғасырдың бастапқы кезеңінде-ақ қарулы қақтығыстар барысында іс жүзінде кеңінен қолданылған.

XX ғасырдың екінші жартысында халықаралық қауіпсіздік пен әскери стратегия саласында «information warfare» ұғымы қалыптасты. Аталған терминді Томас Рон ғылыми айналымға алғаш рет 1976 жылы енгізді және әскери құрылымдардың ақпараттық әлеуетін талдау аясында қолданды. Яғни, «ақпараттық соғыс» ұғымын әскери категорияда қолданды. Кейін бұл термин Пентагонның (АҚШ) 1992 жылғы 21 желтоқсандағы директивасында ресми түрде бекітілді. Ғылыми-теориялық тұрғыдан

«warfare» ұғымы тек қана қарсы әрекетті емес, сонымен қатар қарсы тарапқа бағытталған жүйелі, мақсатты және агрессивті ықпал ету кешенін білдіреді. Бұл әскери көзқарас RAND Corporation жүргізген 1996-1998 жылдардағы зерттеулерде де көрініс тапқан [3].

### «Ақпараттық соғыс» ұғымының анықтамасы

Жалпы, «ақпараттық соғыс» ұғымы ХХІ ғасырға тән жаңа құбылыс емес. Бұл түсініктің алғашқы көріністері «қырғи-қабақ соғыс» идеологы А.Даллестің «Құпия капитуляция» еңбегінде кездеседі. Ол ақпараттық соғысты қарсылас мемлекетке қарсы бағытталған барлау және диверсиялық сипаттағы әрекеттер жиынтығы ретінде қарастырып, оның негізгі мақсаты қарсыластың «тылын» әлсірету деп түсіндірген. Бұл көзқарас ақпараттық соғыс әскери-стратегиялық әрекеттің құрамдас бөлігі екенін көрсетеді [6]. Яғни, Даллес ақпараттық ықпал ету құралдарының ашық қарсыласудан гөрі жасырын және жанама тәсілдер арқылы жүзеге асырылатынына назар аударған.

Белгілі ресейлік зерттеуші А.В. Манойло да ақпараттық соғыс ұғымын осы әскери қырынан сипаттайды. Оның анықтамасына сәйкес, «ақпараттық соғыс – бір саяси субъектінің екінші бір саяси құрылымды әлсірету немесе жою мақсатында жүргізетін ақпараттық қызметі». Сонымен қатар бәсекелес тараптар арасындағы ақпараттық күрес немесе екі жаппай қарсылас (мысалы, армия) арасындағы ақпараттық әскери қақтығыс ретінде де түсіндіріледі [6].

«Ақпараттық соғыс» терминінің анықтамасы әртүрлі. Бұл тақырыпта еңбек жазған зерттеушілердің түсініктемесі, сипаттамасы сан алуан. Себебі бұл ұғым түрлі қырынан зерттелген. Мысалы, А.П. Багаеваның ғылыми жетекшілігімен жазылған еңбекте бұл ұғым кибер-технологиялық категорияда қолданылып, «басқару, командалық үйлестіру және саясат салаларында ақпарат маңызының артуымен байланысты қалыптасқан кешенді стратегия» деп сипатталады.

Осы тұрғыдан алғанда ақпараттық соғыстың әрекет ету аясы кең болады, мемлекеттің негізгі инфрақұрылымын (телекоммуникациялар, көлік желілері, энергетика, банк жүйесі) қамтиды. Сонымен қатар оған өнеркәсіптегі тыңшылық, маңызды деректерді бұрмалау немесе жою, қарсылас туралы барлау мәліметтерін жинау жатады. Киберкеңістікте жеке парольдерді,

сәйкестендіру нөмірлерін және банк шоттарының бұзу да ақпараттық соғыстың құрамдас бөлігі. Осылайша, ақпараттық соғыс қазіргі заманғы қақтығыстарда тек әскери емес, экономикалық және технологиялық салаларды да қамтитын көпқырлы құбылыс ретінде түсіндіріледі [4].

Ақпараттық соғыстың мақсаты дәстүрлі соғыс түсінігінен едәуір ерекшеленеді. Егер классикалық соғыста негізгі мақсат қарсыластың қарулы күштерін жою және стратегиялық маңызды объектілерін талқандау болса, ақпараттық соғыста басты назар қарсылас жүйесінің функционалдық тұрақтылығын әлсіретуге бағытталады. Атап айтқанда, қаржылық, көлік және коммуникациялық желілердің жұмысын кең ауқымда бұзу, экономикалық инфрақұрылымға ішінара зиян келтіру, сондай-ақ ақпараттық-психологиялық ықпал арқылы қоғамды басқару тетіктеріне әсер ету негізгі міндеттердің қатарына жатады. Мұндай ықпалдың түпкі мақсаты – қарсылас мемлекеттің ішкі тұрақтылығын әлсіретіп, оның халқын сыртқы субъектінің еркіне бағындыру [4].

Ал енді ресейлік зерттеуші Д.Л. Шукуровтың еңбегінде «ақпараттық соғыс» ұғымы психологиялық-когнитивті категория тұрғысынан сипатталады. «Жаңа типтегі соғыс ретінде, ең алдымен, адамның санасын нысанаға алады. Ол қоғамдық сананы басқару және манипуляциялау мүмкіндігіне негізделген. Бұл процесс әдетте ақпараттық-психологиялық ықпалға ұшыраған субъектілер үшін бейсаналық деңгейде жүзеге асады, яғни, адамдар өздеріне жасалып жатқан ықпалды толықтай аңғармауы мүмкін». Бұл сипаттама ақпараттық қарудың адам санасы үшін қаншалық қауіпті екенін көрсетеді.

Ол ары қарай бұл соғыстың мақсатына тоқталады. Оның пікірінше, қоғамдық топтар немесе мемлекеттер арасында жүретін ақпараттық күрес қоғамдағы күштердің тепеңдігін өзгертуді көздейді. Ал ақпараттық соғыстың мақсаты – қарсылас тараптың ақпараттық ресурстарына ықпал ету арқылы ақпараттық үстемдікке қол жеткізу және оны мемлекеттік әскери стратегияны қолдау құралы ретінде пайдалану. Сонымен қатар өз ақпараттық жүйелерінің қауіпсіздігін қамтамасыз ету де маңызды міндеттердің бірі. Автор ақпараттық соғыстар әдетте адам психикасын бұзуға бағытталатынын айтады. Себебі сау психикаға ие адамды манипуляциялау қиын, өйткені ол естіген, көргенін сыни тұрғыда бағалап, тексеріп көруі мүмкін.

Осыған байланысты ақпараттық ықпал көбіне адамның эмоционалдық күйіне, әсіресе, кінә сезіміне әсер ету арқылы жүзеге асырылады. Бұл қазіргі психоанализ теориясында қоғамдық тұрақтылықты реттеудің негізгі тетіктерінің бірі ретінде қарастырылады [5]. Д.Л. Шукуровтың мақаласы жеке адамның не қоғамның санасы қашанда ақпараттық соғыстың нысанасы болып қала беретінін көрсетеді. Өйткені оған ықпал ете алған субъект келешекте өзінің дегеніне оңай жетуі мүмкін.

Зерттеуші В.Г. Рошупкин де еңбектерінде «ақпараттық күрес» ұғымын психологиялық-когнитивті категория тұрғысынан қарастырады және өзара байланысты ұғымдар арқылы түсіндіреді. Ол «ақпараттық күрес» терминін ақпараттық-психологиялық кеңістікте ұлттық мүдделерді қамтамасыз етуге бағытталған шабуыл және қорғаныс сипатындағы іс-әрекеттер жиынтығы ретінде анықтайды. Оның негізгі мақсаты мемлекеттің геосаяси және ақпараттық-психологиялық қауіпсіздігін қамтамасыз ету екенін көрсетеді. Оған қоса, зерттеуші «ақпараттық соғыс» ұғымын мемлекеттер арасындағы ақпараттық күрес құралдары, әдістері мен іс-шаралары ретінде түсіндіреді. Автор «ақпараттық-психологиялық соғыс» ұғымына мынадай анықтама береді: белгілі бір әлеуметтік топтарға ықпал етуді көздейтін әскери, дипломатиялық, экономикалық және ақпараттық құралдар арқылы жүргізілетін жасырын сипаттағы ақпараттық-психологиялық операциялар жүйесі. Нәтижесінде, сырттан енгізілген идеологиялық бағдарлар арқылы жекелеген әлеуметтік топтардың мінез-құлқытық модельдері өзгеріп, жалған стереотиптер қалыптасады [6]. Бұл жерде Рошупкиннің басты назарды ақпараттық-психологиялық ықпалға аударған. Ол ақпараттық күресті тек ақпарат тарату емес, адамдардың қабылдауын, сенімін және мінез-құлқын өзгертуге бағытталған құралдар жүйесі ретінде көрсетеді. Яғни әсер тікелей емес, жасырын сипатта жүреді.

Енді зерттеуші Г.Г. Почепцов көзқарасына келсек. Ол ұсынған анықтаманы коммуникациялық-пропагандалық категорияға жатқызуға болады. Оның сипаттамасы мынадай: «ақпараттық соғыс – бұқаралық санаға қысқа және ұзақ мерзімді мақсатта ықпал етуді көздейтін коммуникативті технология. Негізгі мақсат – когнитивті құрылымға өзгерістер енгізу арқылы мінез-құлқыты өзгерту». Яғни, басқаша айтса, белгілі бір қоғамға ақпараттық тұрғыда ықпал етіп, олардың көзқарасын, ұстанымын, қабылдайтын

шешімдерін өзгерту деп те түсінуге болады. Бұл анықтама ақпараттық соғыстың психологиялық аспектісін айқын көрсетеді. Осыған байланысты, ақпараттық соғыстың құрамдас бөлігі ретінде «психологиялық соғыс» ұғымын бөліп қарастырған жөн. Бұл ұғым мазмұндық тұрғыдан «насихат» (пропаганда) түсінігімен тығыз байланысты және көп жағдайда «пропагандалық соғыс» ретінде түсіндіріледі [6]. Аталған құбылысты, әсіресе, мемлекетаралық қарулы қақтығыс барысында жиі байқауға болады. Мұндай кезде БАҚ-тағы мақала, сюжеттер, саясаткерлердің мәлімдемелері, әлеуметтік желідегі жазбалар арқылы нақты месседждер насихатталады.

Ақпараттық соғыстарды зерттеуші И.Н. Панарин өз еңбегінде бұл терминге келесідей анықтама береді: «ақпараттық соғыс – ноосфераны және әлемдік ақпараттық-психологиялық кеңістікті өз мүдделеріне сай ұйымдастыру мақсатында ақпараттық ағындарды басқару жүйесін құру тәсілі». Бұл анықтама ақпараттық соғыстың тек тактикалық немесе жекелеген ықпал ету құралдарымен шектелмейтінін, керісінше, кең ауқымды басқару және ықпал ету жүйесі ретінде қарастырылатынын көрсетеді. Оған қоса, мұнда ақпараттық кеңістікті бақылау арқылы стратегиялық артықшылыққа қол жеткізу идеясы айқын байқалады [7]. Яғни, И.Н. Панариннің анықтамасын да коммуникациялық-пропагандалық категорияға жатқызуға болады.

Бұл «ақпараттық соғыс» ұғымын сипаттайтын анықтамалар еді. Жалпы алғанда, түрлі авторлар ұсынған «ақпараттық соғыс» анықтамаларының әркелкілігі бұл ұғымның көпқырлы сипатын айқын көрсетеді. Бірқатар зерттеушілер оны мемлекеттік деңгейдегі инфрақұрылымға, басқару жүйесіне және стратегиялық ресурстарға бағытталған кешенді әрекет ретінде қарастырса, басқа ғалымдар ақпараттық-психологиялық ықпалға, яғни адамның санасы мен мінез-құлқын өзгерту тетіктеріне басымдық береді. Сонымен қатар бұл терминді кең ауқымды басқару және геосаяси үстемдік құралы ретінде де сипаттайды. Осылайша, анықтамалардың айырмашылығына қарамастан, олардың барлығы ақпараттық соғыстың негізгі мәні – ақпараттық кеңістікке ықпал ету арқылы қарсыластың тұрақтылығын әлсірету, қоғамдық сананы трансформациялау және стратегиялық артықшылыққа қол жеткізу екендігіне тоғысатынын байқаймыз.

Бірақ осы тұста мына жайтты айта кеткен жөн. Бұл анықтамалар әлемдегі соңғы қарулы қақтығыстарда қолданылып жатқан ақпараттық

күрестің кейбір тұстарын қамтымайды. Мысалы, әлеуметтік желі арқылы жүргізіліп отырған күрес. Бұл қарулы қақтығыстар барысында жиі байқалады. Немесе қандай да бір мемлекеттің негізсіз қателігін, шабуылын әлемдік медиа алдында ақтауы. Мысалы, бұл категорияға Ресей 2022 жылы Украинадағы Буча қаласында жасаған қырғынын, Израильдің 2025 жылы жазда Иранға ресми себепсіз зымыран атқылап шабуыл жасауын, АҚШ 2026 жылы Иранға шабуылы барысында түрлі қателіктерге бой алдыруын халықаралық БАҚ-та түсіндіріп, ақтауға, негіздеуге тырысып, айыпты өзінен алып тастауға ұмтылуын жатқызуға болады. Бұл да ақпараттық күрестің заманауи бір санаты.

Қорыта келе, бұл терминге мынадай анықтама беруге болады. «Ақпараттық соғыс» – қарсы тараптың санасына, ақпараттық ресурстарына және басқару жүйесіне ықпал ету арқылы стратегиялық артықшылыққа қол жеткізуге бағытталған күрес түрі. Ол насихат, манипуляция, психологиялық ықпал, пропаганда, кибершабуыл және ақпаратты бұрмалау сияқты құралдар арқылы жүзеге асады. Негізгі мақсаты – қарсыластың имиджіне нұқсан келтіріп, ақпараттық тұрғыда әлсіретіп, ақпараттық кеңістікте үстемдік орнату.

### **Ақпараттық соғыстың түрлері**

Енді ақпараттық соғыс қақтығыстың бір түрлеріне келсек, Олар жеке категория ретінде нақты белгілерге ие. Соларды кеңірек жазсақ. Ақпараттық соғыстың белгілері:

- мемлекеттік мүдделерге зиян келтіру мақсатындағы қызмет;
- жасырын ақпараттық-психологиялық операциялардың жүзеге асырылуы;
- ақпараттық қаруды қолдану [3].

Яғни, осы белгілерді негізге ала отырып, ақпараттық соғысты қарсы тараптағы мемлекеттік мүдделерге нұқсан келтіруге бағытталған кешенді әрекет деуге болады. Бұл соғыс барысында ақпараттық қару кеңінен қолданылады. Ендеше ақпараттық қару дегеніміз не?

Зерттеулерде оған мынадай сипаттама беріледі. Бұл – ақпаратты ұрлауға, бұрмалауға немесе жоюға мүмкіндік беретін құралдар мен әдістердің жиынтығы; заңды пайдаланушылардың оған қол жеткізуін шектеу немесе толық тоқтату; қоғам мен мемлекеттің тіршілігін қамтамасыз етуде қолданылатын телекоммуникациялық желілер мен компьютерлік жүйелердің жұмысын бұзу немесе істен шығару әдістері. Сондай-

ақ ақпараттық қару адамдардың санасын өзгертіп, олардың ақиқатты қате қабылдап, иллюзиялар әлемінде өмір сүруіне итермелейді және өздері үшін қауіпті әрекеттер жасауға мәжбүр етуі мүмкін [4].

Ақпараттық қарудың негізгі функциялық мақсаты – қарсыластың ақпараттық ресурстарын бақылауға алу және оның басқару мен байланыс жүйелеріне ықпал ету арқылы стратегиялық артықшылыққа қол жеткізу. Бұл ретте араласу формалары жасырын немесе ашық сипатта жүзеге асырылып, жүйелердің жұмысын бұзу, олардың тиімділігін төмендету немесе толық істен шығару мақсаттарын көздейді. Аталған әрекеттер бейбіт кезеңде де, әскери қақтығыс жағдайында да, дербес немесе өзге ықпал ету құралдарымен үйлесімде отырып іске асырылуы мүмкін [4]. Мына сипаттамалар ақпараттық қарудың қоғам үшін қаншалық қауіпті екенін көрсетеді. Оны кейбір көрші елдерде жылдар бойы жүргізіліп келе жатқан пропагандалық-

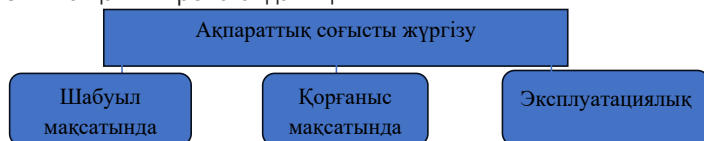
идеологиялық ақпараттық саясаттан көреміз. Сондай саясаттың нәтижесінде қоғамның басым бөлігінде соғыс пен агрессияны қолдау, шетелдіктерге жаугершілікпен қарау сынды көзқарастар бекем орнаған.

Енді ақпараттық соғыстың түрлеріне келсек. Оның санаттары, түрлері көп. Бұл жөнінде де зерттеушілерде ортақ көзқарас жоқ. Мысалы, Г. Ковачич және А. Джонс ақпараттық соғысты жүргізуді үш негізгі санатқа бөледі:

– Шабуыл мақсатында – қарсыластың ақпаратын жоққа шығару, бұрмалау, жою немесе оны пайдалану, сондай-ақ қарсыластың ақпаратты қабылдауына ықпал ету.

– Қорғаныс мақсатында – өзіңді және одақтастарды осындай әрекеттерден (түрлі шабуылдан) қорғау.

– Эксплуатациялық – қолжетімді ақпаратты уақтылы пайдалану арқылы өзіңнің шешім қабылдау және әрекет ету процесіңді жетілдіру, сондай-ақ қарсыластың осы процесін бұзу.



**1 сурет** – Ақпараттық соғысты жүргізудің санаттары (Г. Ковачич және А. Джонс бойынша)

Осылайша, аталған жіктеу ақпараттық соғыстың көпқырлы табиғатын көрсетіп, оны бір мезгілде ықпал ету, қорғану және стратегиялық артықшылыққа қол жеткізу құралы ретінде түсіндіруге мүмкіндік береді [8].

Ал зерттеушілер В.С. Овчинский мен Е.С. Ларина да ақпараттық соғыстарды бірнеше түрге бөледі. Алайда олардың нұсқасы Г. Ковачич және А. Джонстың категорияларына ұқсамайды. Себебі бұл ұғымды санаттарға басқа қырынан бөледі:

– Менталды соғыс. Ақпараттық контент арқылы адам санасына ықпал етуді көздейді. Оның негізгі мақсаты – жекелеген тұлғалардың, әлеуметтік топтардың немесе тұтас қоғамның құндылық бағдарын, сенімін және психикасын өзгерту.

– Киберсоғыс. Ол – ақпараттық инфрақұрылымдарға бағытталған техникалық әрекеттер жиынтығы. Қарсыластың компьютерлік жүйелеріне, желілеріне және деректер базаларына заңсыз ену, оларды бұзу немесе істен шығару арқылы жүзеге асырылады. Бұл тұрғыда кибершабуылдар энергетика, өнеркәсіп, қорғаныс және басқару жүйелері сияқты стратегиялық маңызды салалардың жұмысын бұзуға қабілетті.

– Мінез-құлықтық соғысы. Бұл бағыт әлеуметтік ортада қалыптасқан әдеттер мен әрекет үлгілерін басқаруға бағытталған. Ол адамның күнделікті мінез-құлық алгоритмдеріне, стереотиптеріне және дағдыларына әсер ету арқылы олардың белгілі бір мақсаттарға бейімделуін қамтамасыз етеді. Мұндай тәсілдерді іс жүзінде қолдану үшін заманауи суперкомпьютерлер мен үлкен деректерді талдау мүмкіндіктері қажет [4].

Жалпы алғанда, Овчинский мен Ларинаның жіктемесі өзге зерттеушілердің қорытындысына сәл ұқсас. Ақпараттық соғыстың кешенді табиғатын ашып көрсетеді. Ол ақпараттық ықпалдың когнитивтік (менталды), технологиялық (кибер) және бихевиористік (мінез-құлықтық) деңгейлерде жүзеге асатынын көрсетеді. Бірақ мұны ерекше пікір деуге болмас.

Ақпараттық соғыстың түрлері:		
Менталды соғыс	Киберсоғыс	Мінез-құлықтық соғысы

**2 сурет** – Ақпараттық соғыстың түрлері (В. С. Овчинский мен Е. С. Ларина бойынша)

Ақпараттық соғысты категорияға бөлу кезегін АҚШ өкілі, белгілі Мартин Либикиға берсек. Ол – түрлі мемлекеттік органдарда, ғылыми институттарда тәжірибе жиып, мойындалған маман. Мартин Либики ақпараттық соғысты ақпаратқа ықпал ету процесі ретінде қарастырған. Оның негізгі элементтерінде ақпаратты қорғау, манипуляциялау, бұрмалау және жоққа шығару жатады. М. Либики ақпараттық соғысты келесідей формаларға бөледі. Оны төмендегі кестеден көруге болады.

**1-кесте - Ақпараттық соғыстың түрлері (М.Либики бойынша)**

№	Ақпараттық соғыс түрлері	Ерекшеліктері
1	Командалық-басқарушылық	басқару органдары мен оларға бағынышты әскер арасындағы байланыс арналары нысанаға алынады, басқару мен әрекеттерді үйлестіру мүмкіндігі шектеледі
2	Барлау	әскери маңызы бар ақпаратты жиналады және қорғалады
3	Электронды	электрондық байланыс құралдары мен компьютерлік техника істен шығарылады
4	Психологиялық	қарсылас аумағындағы халыққа ақпарат арқылы психологиялық тұрғыда ықпал етеді
5	Хакерлік	компьютерлік вирустар арқылы ықпал ету, соның нәтижесінде байланыс жүйелерін істен шығарады
6	Экономикалық-ақпараттық	сауда операцияларын жүзеге асыру арналары бұғатталады
7	Киберсоғыс	басты мақсат – ақпаратты иелену

Ресейлік зерттеушілер де ақпараттық соғысты бірнеше санатқа бөледі. Мысалы, Ю. П. Сурмин мен Н. В. Туленков ұстанымдарына сәйкес, ақпараттық соғыс бірнеше түрге бөлінеді. Біріншіден, ақпараттық агрессия – қарсыластың ақпараттық жүйесін бұзуды және оған бөгде құндылықтар жүйесін күштеп таңуды көздейтін ықпал ету формасы. Екіншіден, ақпараттық экспансия – қарсыласқа эволюциялық сипатта өз ақпараттық ресурстары арқылы ұзақ уақыт ықпал етіп, оны біртіндеп бағындыру. Үшіншіден, ақпараттық-психологиялық азаматтық соғыс – қоғамның өз ішіндегі әртүрлі әлеуметтік топтар арасындағы күрес [6]. Қос автордың жіктелімін ақпараттық соғыстың логикасын түсіндіретін концептуалды модель ретінде бағалауға болады. Ол қарапайым әрі жүйелі болғанымен, қазіргі гибриді, цифрлық және көпдеңгейлі ақпараттық күресті толық қамти алмайды. Сондықтан бұл үлгі бастапқы талдау үшін пайдалы, бірақ терең зерттеулерде оны заманауи теориялармен толықтыру қажеттігі туындайды.

Біз осы тұста мына мәселеге ерекше назар аударуымыз қажет. Ақпараттық соғыс қазіргі заманғы гибридік соғыстың ажырамас құрамдас бөлігі ретінде қарастырылады, себебі ол дәстүрлі әскери әрекеттермен қатар жүріп, қарсыластың санасына, қоғамдық пікіріне және шешім қабылдау үдерістеріне ықпал етуді

Либикидің жіктелімі өзгелерге қарағанда ауқымдырақ, алайда кейбір санаттарды өзара біріктіруге болады, мысалы, электронды, хакерлік, кибер соғысты. Өйткені бұл санаттар өзара мәндес. Бірақ автор ақпараттық соғысты көп өлшемді, жүйелі және интеграцияланған құбылыс ретінде және заманауи қақтығыстардың ажырамас бөлігі секілді қарастырады.

көздейді. Бұл тұрғыда ақпараттық ықпал ету құралдары – медиа, әлеуметтік желілер, кибероперациялар және пропагандалық стратегиялар – әскери күш қолданбай-ақ стратегиялық басымдыққа ие болудың тиімді тәсіліне айналып отыр.

Енді осы ойды дәлелдеу үшін кейбір зерттеушілерге жүгінеміз. Жас зерттеушілер Горячева мен Мачнев өз еңбегінде жоғарыда көтерілген мәселеге бірнеше дәлел келтіреді. Яғни, ақпараттық соғысты гибридік соғыстың бір бөлігі ретінде сипаттайтын ерекшеліктерін тізіп кетеді:

- Стандартқа сай келмеу: мұндай ақпараттық қақтығыс классикалық майдан алаңдарынан тыс кеңістікте жүреді.

- Кешенділік: мақсатқа жету үшін әртүрлі әдістер қолданылады.

- Ауқымдылық: мемлекетаралық қатынастардан бастап қарапайым азаматтардың өміріне дейін ықпал етеді.

- Болжаудың мүмкін еместігі: ақпараттық соғыстың нәтижесін алдын ала дәл болжау қиын.

Бұл жіктеу ақпараттық соғысты гибридік қақтығыстардың негізгі және дербес элементі ретінде қарастыру қажеттігін айқындайды. Ол – тек көмекші құрал емес, керісінше, қазіргі геосаяси бәсекелестікте шешуші рөл атқаратын, стратегиялық нәтижелерге тікелей әсер ететін

эмбебап механизм [7]. Біз оны Иран және Израиль, АҚШ арасындағы қарулы қақтығыста (2026ж. көктем) анық байқап отырмыз. Кейде әскери шабуылдардан көрі саясаткерлердің мәлімдемесі, мәліметтері анағұрлым маңыздырақ әрі ықпалдырақ болуда.

Енді бұл мәселені тереңірек қарайтын болсақ, ақпараттық соғыстың дәстүрлі соғыстан бірнеше айырмашылығы бар. Себебі ақпараттық соғыс классикалық қақтығыс талаптарынан тыс сипатқа ие. Олар мынадай: ақпараттық соғыс дәстүрлі соғысқа қарағанда икемдірек құралдар жиынтығына ие; сол бір аудиторияны бірнеше рет «қайта бағындыру» (ықпал ету) мүмкіндігі болады; ақпараттық соғыстың нәтижесін болжау мүмкін емес; ақпараттық соғыста қарсыласқа ықпал астыртын жүреді; соңғысы – ақпараттық соғыстың салдарын бірден байқау қиын, себебі бұл соғыста көзге түсетін қиранды заттар жоқ [7].

### **Ақпараттық соғыс әдістерінің геосаяси қақтығыстардағы қолданысы**

Жоғарыда аталған категорияларда қарсыластың мінез-құлқына, әрекетіне ықпал ету – ақпараттық соғыстың бірден бір мақсаты әрі белгісі екені айтылды. Енді оның әлемдегі соңғы қарулы қақтығыстарда іс жүзінде қалай қолданылып жатқанын талдайық.

АҚШ кейсі. Оның нақты мысалын АҚШ президенті Дональд Трамп бірнеше рет көрсетті. Ол саяси мәлімдеме жасап, ақпараттық шабуыл жасайтын платформа – TruthSocial. Көбіне осы әлеуметтік желіде жарияланатын жазбалары қысым көрсету сипатында болады. Мысалы, 2025 жылы ЕуроОдақ елдерінде АҚШ-тың ірі ІТ компанияларына салық сала бастағанда (Google tax) Трамп мұны цензура деп бағалап, санкциямен, түрлі шектеулермен жауап қайырамыз деп үркітті. Сөйтіп, TruthSocial желісінде мынадай жазба қалдырды: «I put all Countries with Digital Taxes, Legislation, Rules, or Regulations, on notice that unless these discriminatory actions are removed, I, as President of the United States, will impose substantial additional Tariffs on that Country's Exports to the U.S.A., and institute Export restrictions on our Highly Protected Technology and Chips». Аудармасы: «Мен цифрлық салықтар, заңдар, ережелер немесе нормативтік актілер қолданылатын барлық елдерді ескертемін. Егер бұл кемсітуші әрекеттер жойылмаса, мен Америка Құрама Штаттарының президенті ретінде осы елдердің АҚШ-қа экспортына айтарлықтай қосымша

баж салығын енгіземін және біздің жоғары деңгейде қорғалатын технологияларымыз бен чиптеріміздің экспортын шектеймін» [9]. Бұл жазба ақпараттық әрі саяси қысым сипатында жазылған әрі ЕуроОдақ елдерінің АҚШ компанияларына арнайы салық енгізуіне бағытталған.

Бұдан бөлек, Дональд Трамп ақпараттық соғыс құралдарын Иранмен болған текетірес барысында да жиі қолданды. Алдымен 2026 жылы қаңтар айында Иранда болған жаппай ереуілшілерді қолдады. Нақтырақ айтсақ, TruthSocial платформасында мынадай жазба қалдырды: «Iranian Patriots, KEEP PROTESTING - TAKE OVER YOUR INSTITUTIONS!!! Save the names of the killers and abusers. They will pay a big price. I have cancelled all meetings with Iranian Officials until the senseless killing of protesters STOPS. HELP IS ON ITS WAY». Аудармасы: «Иран патриоттары, наразылық акцияларын жалғастырыңдар – мекемелерді басып алыңдар!!! Кісі өлтіріп, зорлық-зомбылық жасағандардың есімдерін ұмытпаңдар. Олар үлкен жазаға тартылады. Ереуілшілерді себепсіз өлтіру тоқтатылмайынша, мен Иран шенеуніктерімен барлық кездесуімді тоқтаттым. Көмек жолда» [10]. Трамп осы жазбасы арқылы басқа мемлекеттің ішкі ісіне араласып, «көмек жолда» деу арқылы жаппай наразылыққа қатысушыларды ереуілді үдетуге шақырды. Яғни, мемлекет басшыларының әлеуметтік желідегі қысқа жазбаларының өзі ақпараттық күрес, қысым не манипуляция болып саналады. Бұдан бөлек, ирандықтардың әрекетін, мінез-құлқын өзгертуге тырысты.

Ресей кейсі. Түрлі жария мәлімдемелер арқылы қарсы тараптағы елге саяси, ақпараттық қысым жасау басқа елдерде де байқалады. Әсіресе, Украина және Ресей арасындағы соғыс барысында бұған сан рет куә болдық. Мәселен, 2025 жылдың желтоқсан айының соңында Ресей президенті Владимир Путин Біріккен әскер тобының басқару пунктіне барып, Бас штаб басшылығымен кеңес өткізді. Сол жиын барысында ол Украинадағы қойылған барлық мақсатқа тек әскери жолмен жететінін айтып, көрші елге қоқан-лоқы көрсетті [11].

Украина кейсі. Мұндай саяси мәлімдемелер басқа да мақсатта жасалады. Мысалы, Украина президенті Владимир Зеленский 2026 жылдың наурыз айында «Украинаның қарулы күштеріне ЕуроОдақтағы бір кісінің мекенжайын беремін, өз тілінде сөйлеседі» деп жария ескерту жасады. Бұл Венгрия ЕуроОдақтың Украинаға 90 млрд долларлық көмегіне

кезекті рет кедергі болғаннан кейін жайт [12]. Яғни, Владимир Зеленский Венгрияның экс-президенті Виктор Орбанға қысым көрсетіп, қорқытты деген түсінік қалыптасты. Бұл жолғы ақпараттық қысымның мақсаты – үлкен көлемдегі көмекке қарсы дауыс бермеуді, кедергі болмауды талап ету.

Қарулы қақтығыс кезінде ақпараттық күрес тек саяси қысым, манипуляция немесе мәлімдемелер арқылы жүрмейді. Кибер шабуылдар да жиі қолданылады. Ол жөнінде зерттеушілердің жіктемесі көрсетілді. Мұндай әдістерге компьютерлік вирустарды жіберу, көшедегі камералардың бағдарламасына қол жеткізу, рация сынды коммуникация құралдарын жару, мобильдік байланыстарды өшіру және басқалары жатады.

Израиль кейсі. Мұндай типтегі шабуылды Израильдің қарулы күштері, барлау күштері жиі қолданады. Мысалы, 2024 жылы 17-18 қыркүйек күндері Ливандағы «Хезболла» ұйымының мүшелері қолданатын пейджер, рация сынды байланыс құралдары жаппай жарылған. Кейін онда жарылғыш зат болғаны анықталды. Екі күндегі жарылыстан 40 аса кісі қаза тауып, бірнеше мың адам орта және ауыр дәрежедегі жарақат алған. Бұл ауқымды әрі салдары ауыр болған кибер шабуыл саналады [13].

Израильдің барлау күштері мұндай операцияны 2026 жылы Иранмен болған соғыс кезінде де жүзеге асырған сыңайлы. Нақтырақ айтсақ, олар Тегеран көшелеріндегі камераларға онлайн қол жеткізіп, аятолла Али Хаменеи оққағарларының көлігін бақылап отырған. Оған қоса, Иранның діни лидерінің резиденциясының нақты мекенжайы анықталған. Мұндай деректерді өңдеуде жасанды интеллект те қолданылған. Осындай дәл ақпарат алынғаннан кейін 2026 жылдың 28 ақпан күні Израиль мен АҚШ қарулы күштерінің бірлескен шабуылы нәтижесінде аятолла Али Хаменеи және Иранның біршама әскери шенділері жиналған ғимаратқа зымыран тасталып, олар қаза тапты [14].

Соңғы қарулы қақтығыстар зымыран атылғанға дейін алдымен кибер және ғарыш күштері қарсыластың байланыс құралдарын істен шығаратынын көрсетті. Мысалы, 2026 жылы көктемдегі соғыс кезінде АҚШ-тың Орталық басшылығының қолбасшысы адмирал Брэд Купер «Біз Иранға теңіз түбінен бастап ғарыш пен киберкеңістікке дейінгі барлық бағытта соққыларды жасауды жалғастырып жатырмыз» деп мәлімдеді. Яғни, кибер шабуыл да бұл соғыста белсенді қолданылған.

Бұдан бөлек, генерал Дэн Кейн баспасөз мәслихатында осы қарулы жанжалдың алдыңғы шебінде ғарыш күштері мен кибер күштер болғанын және олар Иран әскерін көру, байланысу қабілетінен айырғанын жеткізді [15]. Яғни, заманауи қарулы қақтығыстарда алдымен ақпараттық, технологиялық, кибер шабуыл жасалып, байланыс, радар, басқа да аппараттарды істен шығарады. Бұл әдіс шабуылдың кейінгі кезеңдерін жеңілдетеді.

## Қорытынды

Жүргізілген зерттеу нәтижелері көрсеткендей, «ақпараттық соғыс» ұғымы – біржақты немесе әмбебап анықтамамен шектелмейтін, көпдеңгейлі және көпқырлы феномен. Түрлі зерттеушілердің тұжырымдарын салыстырмалы талдау бұл құбылыстың кемінде үш негізгі өлшемде қарастырылатынын айқындайды: технологиялық, психологиялық және стратегиялық. Ал ұсынылған жіктемелерді талдау олардың әрқайсысы ақпараттық соғыстың белгілі бір қырын ғана толық ашатынын көрсетті.

Зерттеу барысында ерекше назар аударатын жайт – ақпараттық соғыстың гибридік қақтығыстар жүйесіндегі рөлі. Қарастырылған теориялық және эмпирикалық материалдар ақпараттық ықпал етудің қазіргі заманғы соғыстарда дербес стратегиялық құралға айналғанын дәлелдейді. Ол тек әскери әрекеттерді сүйемелдейтін элемент емес, кей жағдайларда негізгі шешуші фактор ретінде көрінеді. Әсіресе, саяси мәлімдемелер, медиа кеңістіктегі манипуляциялар және кибершабуылдар арқылы қарсыласқа ықпал ету тәжірибесі бұл тұжырымды нақтылай түседі.

Ақпараттық соғыстың басты ерекшелігі оның нәтижесінің бірден байқалмауы және ықпал ету процесінің жасырын сипатта жүру екені анықталды. Бұл фактор оны дәстүрлі соғыс түрлерінен түбегейлі ажыратады және оның салдарын бағалауды қиындатады. Ақпараттық ықпалдың салдары көбіне ұзақ мерзімде көрініс тауып, қоғамның құндылық бағдары мен мінез-құлық модельдерінің өзгеруі арқылы байқалады.

Жүргізілген зерттеу «ақпараттық соғыс» ұғымының қазіргі халықаралық қатынастар жүйесінде күрделі, көпдеңгейлі және үнемі эволюцияланып отыратын құбылысқа айналғанын көрсетті. Теориялық талдау нәтижелері бұл феноменнің бір ғана анықтамамен шектелмейтінін, керісінше, технологиялық, психологиялық және стратегиялық өлшем-

дердің тоғысында қалыптасатынын айқындайды. Әртүрлі ғылыми көзқарастар мен жіктемелерді салыстыру ақпараттық соғыстың мазмұнын терең түсінуге мүмкіндік бергенімен, оның әмбебап теориялық моделінің әлі толық қалыптаспағанын көрсетеді. Сондай-ақ ақпараттық соғыстың қазіргі заманғы гибридік қақтығыстардағы рөлі ерекше екені дәлелденді.

Практикалық мысалдар ақпараттық соғыстың жүзеге асу формаларының алуан түрін және олардың тиімділігін көрсетті. Саяси мәлімдемелер, медиа және әлеуметтік желілер арқылы жүргізілетін ықпал ету, сондай-ақ кибероперациялар қарсыластың ақпараттық және басқару жүйелерін әлсіретуге бағытталған кешенді әрекеттердің құрамдас бөлігі екенін дәлелдеді. Бұл процесс ақпараттық кеңістіктің геосаяси бәсекелестіктің негізгі алаңдарының біріне айналғанын дәлелдейді.

Осылайша, ақпараттық соғыс қазіргі кезеңде тек әскери немесе саяси құрал ғана емес, кең ауқымды әлеуметтік, технологиялық және когнитивтік процестермен тығыз байланысты әмбебап құбылыс ретінде қарастырылуы тиіс. Сондықтан болашақ зерттеулерде бұл феноменді пәнаралық тұрғыдан талдау, оның ықпал ету механизмдерін тереңірек зерделеу және ақпараттық қауіпсіздікті қамтамасыз етудің тиімді стратегияларын әзірлеу өзекті ғылыми міндеттердің бірі болып қала береді.

### Әдебиеттер тізімі

- 1 Барабаш В.В., Котеленец Е.А., Лаврентьева М.Ю. Информационная война: к генезису термина // Знак: проблемное поле медиаобразования. – 2019. – №3 (33). – 76 с.
- 2 Давлетбаков С.К. Йозеф Геббельс и искусство пропаганды // Скиф. – 2022. – №7 (71). – 29 с.
- 3 Борхсениус А.В. Информационная война: проблема теоретической интерпретации // Вестник Российского университета дружбы народов. Серия: Государственное и муниципальное управление. – 2016. – №1. – 80 с.
- 4 Андрусова Т.Б., Гомонова Ю.Г., Багаева А.П. Информационное оружие и информационные войны // Актуальные проблемы авиации и космонавтики. – 2010. – Т. 1, №6. – 403 с.
- 5 Шукуров Д.Л. Информационные войны и психоанализ // На пути к гражданскому обществу. – 2012. – №1-2 (5-6). – 17 с.
- 6 Пичугин В.И., Годунова Л.А. Концепция информационной войны будущего // Известия Тульского государственного университета. Гуманитарные науки. – 2021. – №3. – 45 с.
- 7 Горячева А.И., Мачнев И.П. Информационная война как элемент гибридной войны // Скиф. Вопросы студенческой науки. – 2023. – №5 (81). – 171 с.

8 Загайнов М.Р. Особенности ведения информационных войн в XXI веке // Социально-политические науки. – 2024. – №4. – 131 с.

9 Gkritsi E., Wendler J. Trump threatens 'substantial' new tariffs against countries with 'discriminatory' digital rules // Politico. – [Электронды ресурсы] URL: <https://www.politico.eu/article/us-question-report-sanction-eu-officials-dsa-donald-trump/> (Қаралған күні: 26.07.2025)

10 Dahir A.L., Nikounazar L. Trump Urges Antigovernment Protesters in Iran to 'Take Over' // New York Times. – [Электронды ресурсы] URL: <https://www.nytimes.com/2026/01/13/world/middleeast/trump-iran-antigovernment-protests.html> (Қаралған күні: 13.01.2026)

11 Иванов Д. Путин грозит достичь целей войны в Украине военным путем // Deutsche Welle. – [Электронды ресурсы] URL: <https://www.dw.com/ru/putin-vnov-grozit-dostic-celej-vojny-v-ukraine-voennym-putem/a-75317700> (Қаралған күні: 27.12.2025)

12 Fortuna G. EU blasts Zelenskyy over veiled threat against Orbán // Politico. – [Электронды ресурсы] URL: <https://www.politico.eu/article/eu-to-volodymyr-zelenskyy-dial-down-not-acceptable-rhetoric-against-hungary-viktor-orban/> (Қаралған күні: 06.03.2026)

13 Конохов М.В. Актуальные вопросы правового обеспечения информационной безопасности военнослужащих и вооруженных сил Российской Федерации на современном этапе развития информационных технологий // Право и государство: теория и практика. – 2025. – №4. – 242 с.

14 Shalev T., Diamond J. Hacked traffic cameras and US intelligence: How a plot to kill Iran's supreme leader came together // CNN. – [Электронды ресурсы] URL: <https://edition.cnn.com/2026/03/03/middleeast/us-israel-plot-kill-iran-khamenei-latam-intl> (Қаралған күні: 04.03.2026)

15 Tidy J. What role has cyber warfare played in Iran? // BBC. – [Электронды ресурсы] URL: <https://www.bbc.com/news/articles/c5yr0576ygvo> (Қаралған күні: 12.03.2026)

### Transliteration

- 1 Barabash V.V., Kotelenec E.A., Lavrent'eva M.Ju. Informacionnaja vojna: k genезису termina [Information war: on the genesis of the term] // Знак: проблемное поле медиаобразования. – 2019. – №3 (33). – 76 с. (in Russ)
- 2 Davletbakov S.K. Jozef Gebbel's i iskusstvo propagandy [Josef Goebbels and the art of propaganda] // Skif. – 2022. – №7 (71). – 29 с. (in Russ)
- 3 Borhseniüs A.V. Informacionnaja vojna: problema teoreticheskoj interpretacii [Information war: the problem of theoretical interpretation] // Vestnik Rossijskogo universiteta družby narodov. Serija: Gosudarstvennoe i municipal'noe upravlenie. – 2016. – №1. – 80 с. (in Russ)
- 4 Andrusova T.B., Gomonova Ju.G., Bagaeva A.P. Informacionnoe oruzhie i informacionnye vojny [Information weapons and information wars] // Aktual'nye problemy aviacii i kosmonavтики. – 2010. – Т. 1, №6. – 403 с. (in Russ)
- 5 Shukurov D.L. Informacionnye vojny i psihoanaliz [Information wars and psychoanalysis] // Na puti k grazhdanskomu obshhestvu. – 2012. – №1-2 (5-6). – 17 с. (in Russ)

6 Pichugin V.I., Godunova L.A. Konceptija informacionnoj vojny budushhego [The concept of the information war of the future] // Izvestija Tul'skogo gosudarstvennogo universiteta. Gumanitarnye nauki. – 2021. – №3. – 45 s. (in Russ)

7 Gorjacheva A.I., Machnev I.P. Informacionnaja vojna kak jelement gibridnoj vojny [Informatory war as an element of hybrid war] // Skif. Voprosy studencheskoj nauki. – 2023. – №5 (81). – 171 s. (in Russ)

8 Zagajnov M.R. Osobennosti vedenija informacionnyh vojn v XXI veke [Features of conducting information wars in the 21st century] // Social'no-politicheskie nauki. – 2024. – №4. – 131 s. (in Russ)

9 Gkritsi E., Wendler J. Trump threatens 'substantial' new tariffs against countries with 'discriminatory' digital rules // Politico. – [Electronic resource] URL: <https://www.politico.eu/article/us-question-report-sanction-eu-officials-dsa-donald-trump/> (Accessed: 26.07.2025)

10 Dahir A.L., Nikounazar L. Trump Urges Antigovernment Protesters in Iran to 'Take Over' // New York Times. – [Electronic resource] URL: <https://www.nytimes.com/2026/01/13/world/middleeast/trump-iran-antigovernment-protests.html> (Accessed: 13.01.2026)

11 Ivanov D. Putin grozit dostich' celej vojny v Ukraine voennym putem [Putin threatens to achieve the goals of the war in Ukraine by military means] // Deutsche Welle. – [Electronic resource] URL: <https://www.dw.com/ru/putin-vnov-grozit-dostic-celej-vojny-v-ukraine-voennym-putem/a-75317700> (Accessed: 27.12.2025) (in Russ)

12 Fortuna G. EU blasts Zelenskyy over veiled threat against Orbán // Politico. – [Electronic resource] URL: <https://www.politico.eu/article/eu-to-volodymyr-zelenskyy-dial-down-not-acceptable-rhetoric-against-hungary-viktor-orban/> (Accessed: 06.03.2026)

13 Konohov M.V. Aktual'nye voprosy pravovogo obespechenija informacionnoj bezopasnosti voennosluzhashhih i vooruzhennyh sil Rossijskoj Federacii na sovremennom jetape razvitija informacionnyh tehnologij [Current issues of legal support for information security of military personnel and armed forces of the Russian Federation at the current stage of information technology development] // Pravo i gosudarstvo: teorija i praktika. – 2025. – №4. – 242 s. (in Russ)

14 Shalev T., Diamond J. Hacked traffic cameras and US intelligence: How a plot to kill Iran's supreme leader came together // CNN. – [Electronic resource] URL: <https://edition.cnn.com/2026/03/03/middleeast/us-israel-plot-kill-iran-khamenei-latam-intl> (Accessed: 04.03.2026)

15 Tidy J. What role has cyber warfare played in Iran? // BBC. – [Electronic resource] URL: <https://www.bbc.com/news/articles/c5yr0576ygyvo> (Accessed: 12.03.2026)

#### АВТОР ЖАЙЛЫ АҚПАРАТ

<i>Нұрмұхамед Исманұлы Байғараев</i>	PhD докторант, Л.Н.Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан, email: baynur01@gmail.com
<i>Нурмухамед Исманович Байғараев</i>	PhD докторант, Евразийский национальный университет имени Л.Н.Гумилёва, Астана, Казахстан, email: baynur01@gmail.com
<i>Nurmukhamed Baigarayev</i>	PhD student, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan, email: baynur01@gmail.com

