ISSN 3107-3328 (Print)
ISSN 3107-3336 (Online)

ҒЫЛЫМИ ИННОВАЦИЯЛАР

ғылыми журналы

№ 3 (2)
2026

научный журнал

НАУЧНЫЕ ИННОВАЦИИ

scientific journal

SCIENTIFIC INNOVATIONS

«ҒЫЛЫМИ ИННОВАЦИЯЛАР» ҒЫЛЫМИ ЖУРНАЛЫ

НАУЧНЫЙ ЖУРНАЛ «НАУЧНЫЕ ИННОВАЦИИ»

«SCIENTIFIC INNOVATIONS» SCIENTIFIC JOURNAL

Журнал 2025 жылдан бастап шығады

Журнал издается с 2025 года

The journal is published from 2025

Меншік иесі: «Неотехнология жене кауіпсіздік гылыми-зерттеу институты» ЖМ

Собственник: ЧУ «Научно-исследовательский институт Неотехнологий и Безопасности»

Owner:ChU «Research Institute of Neotechnology and Security»

Журнал Қазақстан Республикасы Ақпарат жене қоғамдық даму министрлігінін Ақпарат комитетінде тіркелген,

2025 жылы 4 карашадағы № KZ06VPY00133490 куәлік

Журнал зарегистрирован в Комитете информации Министерства информации и общественного развития Республики Казахстан,

свидетельство №KZ06VPY00133490 от 4 ноября 2025 года.

The journal is registered with the Information Committee of the Ministry of Information and Social Development of the Republic of Kazakhstan, certificate

№ KZ06VPY00133490 dated November 4, 2025

Журнал тоқсан сайын шығарылады (жылына 4 рет)

Журнал издаётся ежеквартально (4 раза в год)

The magazine is published quarterly (4 times a year)

Редакцияның мекен-жайы: 150000, Қазақстан Республикасы, Солтүстік-Қазақстан облысы, Петропавл қаласы, Бостандық көшесі, 51

Адрес редакции: 150000, Республика Казахстан, Северо-Казахстанская область, г. Петропавловск, ул. Бостандыкская, 51.

Editorial office: 150000, Republic of Kazakhstan, North Kazakhstan region, Petropavlovsk, st. Bostandyk, 51

Сайт журнала: www.nii-ntb.com

E-mail: jornal@nii-ntb.com

Телефоны редакции: +7 (7152) 33-44-35, +7 778 569 19 61, +7 707 279 85 75

РЕДАКЦИЯЛЫҚ АЛҚА
РЕДАКЦИОННАЯ КОЛЛЕГИЯ
EDITORIAL BOARD

Графикалық дизайнер / Графический дизайнер / Graphic designer

Дергалёва Наталья Владимировна,
Дергалёва Наталья Владимировна,
Dergaleva Natalia Vladimirovna,

МАЗМҰНЫ / СОДЕРЖАНИЕ / TABLE OF CONTENTS

ИННОВАЦИЯЛЫҚ ПЕДАГОГИКА ЖӘНЕ БІЛІМ БЕРУ ТЕХНОЛОГИЯЛАРЫ
ИННОВАЦИОННАЯ ПЕДАГОГИКА И ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ
INNOVATIVE PEDAGOGY AND EDUCATIONAL TECHNOLOGIES

ИНЖЕНЕРИЯ, ОЗЫҚ МАТЕРИАЛДАР ЖӘНЕ ТЕХНИКАЛЫҚ ҒЫЛЫМДАР
ИНЖЕНЕРИЯ, ПЕРЕДОВЫЕ МАТИЕРИАЛЫ И ТЕХНИЧЕСКИЕ НАУКИ
ENGINEERING, ADVANCED MATERIALS AND TECHNICAL SCIENCES

ӘОЖ: 004.056.57
ҒТАМР: 81.93.29

ШАПАШЕВ М.А.

философия докторы (PhD), доцент, полковник. Қазақстан, Петропавл қаласы. ORCID: 0009- 0006-8866-8946, E-mail:shapashev@bk.ru

КИБЕРСОҒЫС – ҚАЗІРГІ ӘЛЕМНІҢ ҚАУПІ

Андатпа. Киберсоғыс – ақпараттық технологиялар мемлекеттік, әскери және экономикалық қызметтің ажырамас бөлігіне айналған қазіргі әлемдегі ең маңызды қауіптердің бірі. Мақалада киберсоғыстың мәні, оның негізгі әдістері мен құралдары, сондай-ақ цифрлық кеңістікте әскери іс-қимылдарды жүргізудің ерекшеліктері қарастырылады. Кибершабуылдардың маңызды инфрақұрылым нысандарына, байланыс жүйелеріне, мемлекеттік мекемелер мен әскери құрылымдарға тигізетін әсері талданады. Киберқауіпсіздік мәселелеріне, халықаралық ынтымақтастыққа және киберқауіптерден қорғану құралдарын дамыту перспективаларына ерекше назар аударылады. Зерттеу нәтижесінде киберкеңістіктің мемлекеттер арасындағы жаңа қарсыластық алаңына айналғаны және ақпараттық қауіпсіздікті қамтамасыз ету XXI ғасырдағы ұлттық қауіпсіздіктің маңызды шарты екендігі анықталды.

Түйінді сөздер: Түйін сөздер: киберсоғыс, кибершабуыл, киберқауіпсіздік, ақпараттық қауіпсіздік, цифрлық технологиялар, маңызды инфрақұрылым, киберқауіптер, ұлттық қауіпсіздік.

ШАПАШЕВ М.А.

доктор философии (PhD), ассоциированный профессор (доцент), полковник, г. Петропавловск, Казахстан. ORCID: 0009- 0006-8866-8946, E-mail:shapashev@bk.ru

КИБЕРВОЙНА - УГРОЗА СОВРЕМЕННОГО МИРА

Аннотация. Кибервойна представляет собой одну из наиболее значимых угроз современного мира, где информационные технологии стали неотъемлемой частью государственной, военной и экономической деятельности. В статье рассматривается сущность кибервойны, ее основные методы и инструменты, а также особенности ведения боевых действий в цифровом пространстве. Анализируется влияние кибератак на объекты критической инфраструктуры, системы связи, государственные учреждения и военные структуры. Особое внимание уделяется вопросам кибербезопасности, международного сотрудничества и перспективам развития средств защиты от киберугроз. Сделан вывод о том, что киберпространство стало новым полем противоборства государств, а обеспечение информационной безопасности является важнейшим условием национальной безопасности в XXI веке.

Ключевые слова: Ключевые слова: кибервойна, кибератака, кибербезопасность, информационная безопасность, цифровые технологии, критическая инфраструктура, киберугрозы, национальная безопасность.

SHAPASHEV M.A.

Doctor of Philosophy (PhD), Associate Professor, Colonel, Petropavlovsk, Kazakhstan. ORCID: 0009-0006-8866-8946 E-mail: shapashev@bk.ru

CYBER WARFARE AS A THREAT TO THE MODERN WORLD

Annotation. Cyber warfare is one of the most significant threats facing the modern world, where information technologies have become an integral part of governmental, military, and economic activities. This article examines the essence of cyber warfare, its main methods and tools, as well as the specific features of conducting military operations in cyberspace. The impact of cyberattacks on critical infrastructure facilities, communication systems, government institutions, and military organizations is analyzed. Particular attention is paid to issues of cybersecurity, international cooperation, and the prospects for developing protection mechanisms against cyber threats. The study concludes that cyberspace has become a new arena of confrontation among states, while ensuring information security has become a crucial prerequisite for national security in the 21st century.

Keywords: Keywords: cyber warfare, cyberattack, cybersecurity, information security, digital technologies, critical infrastructure, cyber threats, national security.

Кіріспе.

XXI ғасырда ақпараттық технологиялардың қарқынды дамуы халықаралық қауіпсіздік пен әскери қарсыласу саласында елеулі өзгерістерге алып келді. Компьютерлік желілер, байланыс жүйелері, деректер базалары және маңызды инфрақұрылым нысандары қазіргі мемлекеттердің қызмет етуінің маңызды элементтеріне айналды. Сонымен қатар, цифрлық технологияларды әскери және саяси мақсаттарда пайдаланумен байланысты жаңа қауіптер пайда болды.

Осындай қауіптердің ең маңыздыларының бірі – киберсоғыс. Киберсоғыс ақпараттық және компьютерлік технологиялар арқылы киберкеңістікте жүзеге асырылатын қарсыласу түрі болып табылады. Дәстүрлі қарулы қақтығыстардан айырмашылығы, киберсоғыс ұрыс алаңында тікелей физикалық қатысуды талап етпейді, алайда мемлекеттік мекемелерге, әскери нысандарға, энергетикалық жүйелерге, қаржы секторына және байланыс құралдарына елеулі зиян келтіруі мүмкін.

Бұл тақырыптың өзектілігі ақпараттық жүйелердің жұмысын бұзуға, құпия деректерді алуға және мемлекеттердің қорғаныс қабілетін әлсіретуге бағытталған кибершабуылдар санының артуымен түсіндіріледі. Қазіргі таңда киберкеңістік құрлық, теңіз, әуе және ғарыш кеңістіктерімен қатар әскери іс-қимылдарды жүргізудің дербес саласы ретінде қарастырылады.

Осы мақаланың мақсаты – киберсоғыстың мәнін, оның негізгі әдістері мен құралдарын қарастыру, сондай-ақ киберқауіптердің ұлттық және халықаралық қауіпсіздікке әсерін анықтау. Қойылған мақсатқа жету үшін қазіргі заманғы киберқақтығыстардың ерекшеліктерін зерттеу, олардың салдарын талдау және киберқорғаныс құралдарының даму перспективаларын бағалау қажет.

Материалдар мен әдістер.

Зерттеудің ақпараттық базасын киберқауіпсіздік, ақпараттық соғыс және халықаралық қауіпсіздік саласындағы шетелдік ғалымдардың ғылыми еңбектері

құрады. Киберсоғыс мәселелерін зерттеуге «Cyber War Will Not Take Place» еңбегінің авторы Томас Рид [1], киберқақтығыстар мен ақпараттық қарсыласу мәселелерін зерттеген Мартин Либицки [2], сондай-ақ ақпараттық технологиялардың халықаралық қатынастар мен қауіпсіздікке ықпалын қарастырған Джозеф Най [3] елеулі үлес қосты. Ақпараттық қауіпсіздік пен киберқауіптер теориясын дамытуға А.В. Манойло [4], И.Н. Панарин [5], В.В. Цыганов [6] маңызды үлес қосты. Олардың зерттеулері ақпараттық қарсыласу, цифрлық ортадағы ұлттық мүдделерді қорғау және мемлекеттің киберқауіпсіздігін қамтамасыз ету мәселелеріне арналған.

Зерттеудің әдіснамалық негізін жалпығылыми және арнайы таным әдістері құрады. Зерттеу барысында киберқауіпсіздік пен киберсоғыс мәселелеріне арналған ғылыми әдебиеттерді, нормативтік-құқықтық құжаттарды, талдамалық есептер мен жарияланымдарды талдау және жинақтау әдістері пайдаланылды.

Киберсоғыстың мәні мен ерекшеліктерін зерттеу үшін салыстырмалы әдіс қолданылды, ол дәстүрлі қарулы қарсыласу нысандарын киберкеңістіктегі заманауи әскери іс-қимылдарды жүргізу тәсілдерімен салыстыруға мүмкіндік берді. Киберқауіптердің даму кезеңдерін және киберкеңістіктің әскери қарсыласудың жаңа саласы ретінде қалыптасуын қарастыру үшін тарихи әдіс пайдаланылды.

Зерттеу нәтижелері.

Жүргізілген зерттеу нәтижесінде киберсоғыстың қазіргі халықаралық қауіпсіздік жүйесінің маңызды элементтерінің бірі екендігі анықталды. Цифрлық технологиялардың дамуы және мемлекеттік, әскери әрі экономикалық үдерістердің жаппай компьютерленуі жаңа қарсыласу кеңістігінің – киберкеңістіктің қалыптасуына алып келді. Дәстүрлі қарулы қақтығыстардан айырмашылығы, киберсоғыс компьютерлік желілер мен ақпараттық жүйелерді пайдалану арқылы жүзеге асырылады, бұл мемлекеттер мен мемлекеттік емес субъектілерге әскери күшті тікелей қолданбай-ақ қарсыласқа ықпал етуге мүмкіндік береді.

Ғылыми жарияланымдар мен практикалық мысалдарды талдау көрсеткендей, кибершабуылдардың негізгі нысандары мемлекеттік ақпараттық ресурстар, әскери басқару жүйелері, энергетикалық инфрақұрылым, банк секторы, көлік желілері және байланыс құралдары болып табылады. Аталған нысандардың жұмысын бұзу елеулі экономикалық шығындарға, мемлекеттің қорғаныс қабілетінің төмендеуіне және әлеуметтік тұрақсыздықтың туындауына әкелуі мүмкін.

Зерттеу қазіргі кибероперациялардың ықпал ету әдістерінің кең ауқымын қамтитынын көрсетті. Олардың ішінде зиянды бағдарламалық қамтамасыз ету, DDoS типті үлестірілген шабуылдар, фишинг, кибертыңшылық, бопсалаушы бағдарламаларды енгізу және бағдарламалық қамтамасыз ету жеткізу тізбегіне жасалатын шабуылдар кең таралған. Әсіресе маңызды инфрақұрылым нысандарына

бағытталған шабуылдар аса қауіпті болып табылады, өйткені олардың салдары миллиондаған азаматтарға әсер етіп, мемлекеттің өмірлік маңызы бар жүйелерінің жұмысын бұзуы мүмкін.

Осындай мысалдардың бірі – 2021 жылы АҚШ-тағы Colonial Pipeline құбыр жүйесіне жасалған шабуыл. Қаскөйлердің әрекеті салдарынан АҚШ-тың шығыс бөлігіндегі ең ірі отын құбырының жұмысы уақытша тоқтатылып, жанармай жеткізуде іркілістер мен экономикалық шығындар орын алды. Бұл оқиға маңызды инфрақұрылым нысандарының қазіргі киберқауіптер алдындағы осалдығын көрсетті [7].

Зерттеу барысында киберсоғыстың басты ерекшеліктерінің бірі шабуыл көзін анықтаудың күрделілігі екендігі белгілі болды. Анонимді желілерді, аралық серверлерді және үлестірілген инфрақұрылымдарды пайдалану кибершабуылдарды ұйымдастырушыларды анықтауды айтарлықтай қиындатады. Бұл халықаралық құқық пен осындай оқиғаларға әрекет ету тетіктері үшін күрделі мәселелер туындатады. Дәстүрлі қарулы қақтығыстарда шабуыл жасаған тарапты анықтау мүмкін болса, киберкеңістікте атрибуция үдерісі көп жағдайда елеулі уақыт пен техникалық ресурстарды талап етеді.

Соңғы онжылдықтардағы ең белгілі киберинциденттерді талдауға ерекше назар аударылды. Зерттеу көптеген мемлекеттердің шабуылдаушы және қорғаныстық кибермүмкіндіктерін белсенді түрде дамытып жатқанын көрсетті. Бірқатар ауқымды шабуылдар зиянды бағдарламалардың өнеркәсіптік басқару жүйелерін істен шығаруға, мемлекеттік мекемелердің жұмысын бұзуға және айтарлықтай экономикалық шығын келтіруге қабілетті екенін дәлелдеді. Бұл киберқарудың қазіргі әскери стратегиялардың маңызды элементіне айналып келе жатқанын көрсетеді.

Киберқақтығыстар тарихында 2007 жылы Эстонияның мемлекеттік инфрақұрылымына жасалған шабуылдар ерекше орын алады. Бірқатар DDoS-шабуылдардың нәтижесінде мемлекеттік сайттардың, банк қызметтерінің, бұқаралық ақпарат құралдарының және коммуникациялық жүйелердің жұмысы бұзылды. Бұл оқиғалар киберкеңістік арқылы мемлекетке кең ауқымды ықпал етудің алғашқы мысалдарының бірі болды [8].

Алынған нәтижелер киберсоғыстың дәстүрлі әскери іс-қимыл әдістерімен салыстырғанда бірқатар артықшылықтарға ие екенін растады. Олардың қатарына операцияларды жүргізудің салыстырмалы түрде төмен құны, шабуылдарды іске асырудың жоғары жылдамдығы, қарсыласқа жасырын ықпал ету мүмкіндігі және басқа мемлекеттің аумағында тікелей физикалық қатысудың қажет болмауы жатады. Сонымен қатар, кибершабуылдардың тиімділігі мемлекеттің технологиялық

даму деңгейіне, барлау ақпаратының сапасына және қарсыластың ақпараттық жүйелерінің қорғалу дәрежесіне тікелей байланысты.

Жүргізілген талдау киберқауіптердің өсуі мемлекеттерді арнайы киберқорғаныс бөлімшелерін құруға және ұлттық ақпараттық қауіпсіздік стратегияларын жетілдіруге ынталандыратынын көрсетті. Әлемнің жетекші мемлекеттері киберкеңістікті әскери қарсыласудың толыққанды саласы ретінде қарастырып, жаңа қорғаныс және шабуыл құралдарын әзірлеуге белсенді түрде инвестиция салуда. Осыған байланысты цифрлық ортада мемлекеттердің мінез-құлқының ортақ нормаларын қалыптастыруға және ауқымды киберқақтығыстардың алдын алуға бағытталған халықаралық ынтымақтастықтың рөлі артып келеді.

Зерттеу нәтижелерін талқылау қоғамның одан әрі цифрлануы ұлттық және халықаралық қауіпсіздік мәселелеріндегі киберкеңістіктің маңызын арттыра түсетінін көрсетеді. Ақпараттық жүйелердің осалдығы, мемлекеттердің цифрлық инфрақұрылымға тәуелділігі және кибершабуыл әдістерінің үздіксіз жетілдірілуі киберқауіпсіздікті қамтамасыз етуде кешенді тәсілді талап етеді. Қазіргі қауіптерге тиімді қарсы тұру техникалық, ұйымдастырушылық, құқықтық және халықаралық қорғаныс шараларын үйлестіру арқылы ғана мүмкін болады.

Талқылау.

Жүргізілген зерттеу нәтижесінде киберсоғыстың қазіргі халықаралық қауіпсіздік жүйесінің маңызды элементтерінің бірі екендігі анықталды. Цифрлық технологиялардың дамуы және мемлекеттік, әскери әрі экономикалық үдерістердің жаппай компьютерленуі жаңа қарсыласу кеңістігінің – киберкеңістіктің қалыптасуына алып келді. Дәстүрлі қарулы қақтығыстардан айырмашылығы, киберсоғыс компьютерлік желілер мен ақпараттық жүйелерді пайдалану арқылы жүзеге асырылады, бұл мемлекеттер мен мемлекеттік емес субъектілерге әскери күшті тікелей қолданбай-ақ қарсыласқа ықпал етуге мүмкіндік береді.

Ғылыми жарияланымдар мен практикалық мысалдарды талдау көрсеткендей, кибершабуылдардың негізгі нысандары мемлекеттік ақпараттық ресурстар, әскери басқару жүйелері, энергетикалық инфрақұрылым, банк секторы, көлік желілері және байланыс құралдары болып табылады. Аталған нысандардың жұмысын бұзу елеулі экономикалық шығындарға, мемлекеттің қорғаныс қабілетінің төмендеуіне және әлеуметтік тұрақсыздықтың туындауына әкелуі мүмкін.

Зерттеу қазіргі кибероперациялардың ықпал ету әдістерінің кең ауқымын қамтитынын көрсетті. Олардың ішінде зиянды бағдарламалық қамтамасыз ету, DDoS типті үлестірілген шабуылдар, фишинг, кибертыңшылық, бопсалаушы бағдарламаларды енгізу және бағдарламалық қамтамасыз ету жеткізу тізбегіне жасалатын шабуылдар кең таралған. Әсіресе маңызды инфрақұрылым нысандарына

бағытталған шабуылдар аса қауіпті болып табылады, өйткені олардың салдары миллиондаған азаматтарға әсер етіп, мемлекеттің өмірлік маңызы бар жүйелерінің жұмысын бұзуы мүмкін.

Осындай мысалдардың бірі – 2021 жылы АҚШ-тағы Colonial Pipeline құбыр жүйесіне жасалған шабуыл. Қаскөйлердің әрекеті салдарынан АҚШ-тың шығыс бөлігіндегі ең ірі отын құбырының жұмысы уақытша тоқтатылып, жанармай жеткізуде іркілістер мен экономикалық шығындар орын алды. Бұл оқиға маңызды инфрақұрылым нысандарының қазіргі киберқауіптер алдындағы осалдығын көрсетті [7].

Зерттеу барысында киберсоғыстың басты ерекшеліктерінің бірі шабуыл көзін анықтаудың күрделілігі екендігі белгілі болды. Анонимді желілерді, аралық серверлерді және үлестірілген инфрақұрылымдарды пайдалану кибершабуылдарды ұйымдастырушыларды анықтауды айтарлықтай қиындатады. Бұл халықаралық құқық пен осындай оқиғаларға әрекет ету тетіктері үшін күрделі мәселелер туындатады. Дәстүрлі қарулы қақтығыстарда шабуыл жасаған тарапты анықтау мүмкін болса, киберкеңістікте атрибуция үдерісі көп жағдайда елеулі уақыт пен техникалық ресурстарды талап етеді.

Соңғы онжылдықтардағы ең белгілі киберинциденттерді талдауға ерекше назар аударылды. Зерттеу көптеген мемлекеттердің шабуылдаушы және қорғаныстық кибермүмкіндіктерін белсенді түрде дамытып жатқанын көрсетті. Бірқатар ауқымды шабуылдар зиянды бағдарламалардың өнеркәсіптік басқару жүйелерін істен шығаруға, мемлекеттік мекемелердің жұмысын бұзуға және айтарлықтай экономикалық шығын келтіруге қабілетті екенін дәлелдеді. Бұл киберқарудың қазіргі әскери стратегиялардың маңызды элементіне айналып келе жатқанын көрсетеді.

Киберқақтығыстар тарихында 2007 жылы Эстонияның мемлекеттік инфрақұрылымына жасалған шабуылдар ерекше орын алады. Бірқатар DDoS-шабуылдардың нәтижесінде мемлекеттік сайттардың, банк қызметтерінің, бұқаралық ақпарат құралдарының және коммуникациялық жүйелердің жұмысы бұзылды. Бұл оқиғалар киберкеңістік арқылы мемлекетке кең ауқымды ықпал етудің алғашқы мысалдарының бірі болды [8].

Алынған нәтижелер киберсоғыстың дәстүрлі әскери іс-қимыл әдістерімен салыстырғанда бірқатар артықшылықтарға ие екенін растады. Олардың қатарына операцияларды жүргізудің салыстырмалы түрде төмен құны, шабуылдарды іске асырудың жоғары жылдамдығы, қарсыласқа жасырын ықпал ету мүмкіндігі және басқа мемлекеттің аумағында тікелей физикалық қатысудың қажет болмауы жатады. Сонымен қатар, кибершабуылдардың тиімділігі мемлекеттің технологиялық

даму деңгейіне, барлау ақпаратының сапасына және қарсыластың ақпараттық жүйелерінің қорғалу дәрежесіне тікелей байланысты.

Жүргізілген талдау киберқауіптердің өсуі мемлекеттерді арнайы киберқорғаныс бөлімшелерін құруға және ұлттық ақпараттық қауіпсіздік стратегияларын жетілдіруге ынталандыратынын көрсетті. Әлемнің жетекші мемлекеттері киберкеңістікті әскери қарсыласудың толыққанды саласы ретінде қарастырып, жаңа қорғаныс және шабуыл құралдарын әзірлеуге белсенді түрде инвестиция салуда. Осыған байланысты цифрлық ортада мемлекеттердің мінез-құлқының ортақ нормаларын қалыптастыруға және ауқымды киберқақтығыстардың алдын алуға бағытталған халықаралық ынтымақтастықтың рөлі артып келеді.

Зерттеу нәтижелерін талқылау қоғамның одан әрі цифрлануы ұлттық және халықаралық қауіпсіздік мәселелеріндегі киберкеңістіктің маңызын арттыра түсетінін көрсетеді. Ақпараттық жүйелердің осалдығы, мемлекеттердің цифрлық инфрақұрылымға тәуелділігі және кибершабуыл әдістерінің үздіксіз жетілдірілуі киберқауіпсіздікті қамтамасыз етуде кешенді тәсілді талап етеді. Қазіргі қауіптерге тиімді қарсы тұру техникалық, ұйымдастырушылық, құқықтық және халықаралық қорғаныс шараларын үйлестіру арқылы ғана мүмкін болады.

Қорытынды.

Жүргізілген зерттеу киберсоғыстың қазіргі заманғы қарсыласудың ең қарқынды дамып келе жатқан түрлерінің бірі екенін және қоғамның цифрлануы мен мемлекеттердің ақпараттық технологияларға жаһандық тәуелділігі жағдайында оның маңызы артып келе жатқанын анықтауға мүмкіндік берді.

Зерттеу барысында киберкеңістіктің дәстүрлі әскери іс-қимыл театрларымен қатар қақтығыстар жүргізілетін толыққанды салаға айналғаны анықталды. Киберсоғыстың негізгі сипаттамаларына жасырындық, шабуылдарды іске асырудың жоғары жылдамдығы, қауіптердің трансшекаралық сипаты және шабуыл көздерін нақты анықтаудың күрделілігі жатады.

Теориялық тәсілдер мен практикалық мысалдарды талдау кибершабуылдардың мемлекеттік, әскери және азаматтық жүйелерге елеулі зиян келтіре алатынын көрсетті. Киберқауіптердің дамуы мемлекеттерден киберқорғаныс жүйелерін үздіксіз жетілдіруді, білікті мамандар даярлауды және ақпараттық қауіпсіздікті қамтамасыз етудің заманауи технологияларын енгізуді талап ететіні ерекше атап өтілді. Сонымен қатар мемлекеттердің киберкеңістіктегі іс-қимылдарының ортақ қағидаларын қалыптастыруға және ауқымды қақтығыстардың алдын алуға бағытталған халықаралық ынтымақтастық маңызды рөл атқарады.

Осылайша, киберсоғыс қазіргі қауіпсіздік жүйесінің ажырамас бөлігі болып табылады және халықаралық қатынастардың сипатына барған сайын елеулі ықпал

ететін болады. Ақпараттық технологиялардың одан әрі дамуы, бір жағынан, мемлекеттердің мүмкіндіктерін кеңейтсе, екінші жағынан, киберқауіптердің деңгейін арттырады. Бұл аталған мәселені XXI ғасырдың ең өзекті проблемаларының біріне айналдырады.

СПИСОК ЛИТЕРАТУРЫ:

1. Rid T. Cyber War Will Not Take Place. — London: Hurst & Company, 2013. — 218 б. (қаралған күні: 15.05.2026).
2. Libicki M. Cyberdeterrence and Cyberwar. — Santa Monica: RAND Corporation, 2009. — 238 б. (қаралған күні: 15.05.2026).
3. Nye J. S. Cyber Power. — Cambridge: Belfer Center for Science and International Affairs, Harvard Kennedy School, 2010. (қаралған күні: 15.05.2026).
4. Манойло А. В. Ерекше жағдайлардағы мемлекеттік ақпараттық саясат. — Мәскеу: МИФИ, 2003.
5. Панарин И. Н. Ақпараттық соғыс және дипломатия. — Мәскеу: Горячая линия – Телеком, 2015.
6. Цыганов В. В. Бизнес пен саясаттағы ақпараттық соғыстар: теориясы мен әдіснамасы. — Мәскеу: Академиялық жоба, 2007.
7. BBC News. АҚШ-тағы жанармай құбырына жасалған кибершабуыл тапшылыққа әкелді. (қаралған күні: 15.05.2026).
8. Kerttunen M., Tikk E. 2007 жылғы Эстонияға қарсы жасалған кибершабуылдар. NATO CCDCOE жарияланымдары. (қаралған күні: 15.05.2026).
9. Малюк А. А. Ақпараттық қауіпсіздік: ақпаратты қорғаудың тұжырымдамалық және әдіснамалық негіздері. — Мәскеу: Горячая линия – Телеком, 2022.
10. Шнайер Б. Құпиялар мен жалғандықтар. Цифрлық әлемдегі деректер қауіпсіздігі. — Санкт-Петербург: Питер, 2021.
11. Кастельс М. Ақпараттық дәуір: экономика, қоғам және мәдениет. — Мәскеу: Жоғары экономика мектебі баспасы, 2020.

REFERENCES:

1. Rid T. Cyber War Will Not Take Place. — London: Hurst & Company, 2013. — 218 b. (qaralghan kuni: 15.05.2026).
2. Libicki M. Cyberdeterrence and Cyberwar. — Santa Monica: RAND Corporation, 2009. — 238 b. (qaralghan kuni: 15.05.2026).
3. Nye J. S. Cyber Power. — Cambridge: Belfer Center for Science and International Affairs, Harvard Kennedy School, 2010. (qaralghan kuni: 15.05.2026).
4. Manoylo A. V. Erekshe zhaghdaylardaghy memlekettik aqparattyq sayasat. — Maskeu: MIFI, 2003.

5. Panarin I. N. Aqparattyq soghys zhane diplomatiya. — Maskeu: Goryachaya liniya – Telekom, 2015.
6. Tsyganov V. V. Biznes pen sayasattaghy aqparattyq soghystar: teoriyasy men adisnamasy. — Maskeu: Akademiyalyq zhoba, 2007.
7. BBC News. AQSh-taghy zhanarmay qubyryna zhasalghan kibershabuyl tapshylyqqa akeldi. (qaralghan kuni: 15.05.2026).
8. Kerttunen M., Tikk E. 2007 zhylghy Estoniyagha qarsy zhasalghan kibershabuyldar. NATO CCDCOE zhariyalanymdary. (qaralghan kuni: 15.05.2026).
9. Malyuk A. A. Aqparattyq qauipsizdik: aqparatty qorghaudyng tuzhyrymdamalyq zhane adisnamalyq negizderi. — Maskeu: Goryachaya liniya – Telekom, 2022.
10. Shnayer B. Qupiyalar men zhalghandyqtar. Tsifrlyq alemdegi derekter qauipsizdigi. — Sankt-Peterburg: Piter, 2021.
11. Kastels M. Aqparattyq dauir: ekonomika, qogham zhane madeniet. — Maskeu: Zhoghary ekonomika mektebi baspasy, 2020.

Баспаға 30.06.2026 ж. 60х84/8 форматында қол қойылды
Офсеттік басып шығару. Офсеттік қағаз. Шығыс. Л. 12,8 б.п.
Таралымы 500 дана
Баспахананың мекен-жайы: 150000, Қазақстан Республикасы, Солтүстік Қазақстан облысы, Петропавл қаласы, Бостандық көшесі, 51
«Неотехнология және қауіпсіздік ғылыми-зерттеу институты» ЖМ

Подписано в печать 30.06.2026 г. Формат 60х84/8
Печать офсетная. Бумага офсетная. Уч.-изд. Л. 12,8 п.л.
Тираж 500 экз.
Адрес типографии: 150000, Республика Казахстан, Северо-Казахстанская область, г. Петропавловск, ул. Бостандыкская, 51
ЧУ «Научно-исследовательский институт Неотехнологий и безопасности»

Signed for printing in 30.06.2026. Format 60x84/8
Offset printing. Offset paper. Academic edition L. 12,8 p.p.
Circulation 500 copies
Printing house address: 150000, Republic of Kazakhstan, North Kazakhstan region, Petropavlovsk, st. Bostandyk, 51
PI «Research Institute of Neotechnology and Safety»