

КИБЕРҚАУІПСІЗДІК: НЕГІЗГІ ТҮСІНІКТЕРІ МЕН БЕЛГІЛЕРІ

УДК 304.2

Аңдатпа. Соңғы технологиялық жетістіктер киберкеңістіктің едәуір өсіміне әкелді. Киберқауіпсіздік қарқынды ғылыми-зерттеушілік қызметтің саласына айналды. Сонымен қатар, Интернетке тәуелділіктің күшеюі оның ұлттық стратегиялық белсенділігін арттырды. Ғаламтордың кеңінен таралуы шарттарында киберқатерлердің дамуы жаһандық құбылыс болып табылады. Киберқауіптер күн сайын жетіліп келеді. Сондықтан киберкеңістік ұлттық қауіпсіздік пен өркендеуді қамтамасыз ету үшін үнемі қорғанышта болуы керек.

Ғылыми мақалада киберқауіпсіздіктің негізгі түсініктері мен белгілері қарастырылады. Зерттеу нысаны ретінде заманауи қоғамдағы киберқауіпсіздік саналады. Зерттеу пәніне киберқауіпсіздіктің негізгі түсініктері мен белгілері жатады.

Тірек сөздер: киберкеңістік, киберқауіпсіздік, кибералаяқтық, ғаламтор, әлеуметтік желілер, сананың виртуалдануы.

Jel: F52, H5, K24, L14, L86.

Аннотация. Последние технологические достижения позволило значительному росту киберпространства. Кибербезопасность стало областью интенсивной научно-исследовательской деятельности. В то же время, наша сильная зависимость Интернету сделали их стратегическими национальными активами. С распространением всемирной паутины развитие киберугроз стало глобальным явлением. Киберугрозы продолжают расти каждый день. Поэтому киберпространство должны быть защищены для обеспечения национальной безопасности и процветания.

В научной статье рассматриваются основные понятия и признаки кибербезопасности. Объектом исследования является кибербезопасность современного общества. Предметом исследования выступают основные понятия и признаки кибербезопасности.

Ключевые слова: киберпространство, кибербезопасность, кибермошенничество, интернет, социальные сети, виртуализация сознания.

Jel-коды: F52, H5, K24, L14, L86.

Abstract. Recent technological advances have allowed a significant increase in cyber space. Cyber security has become an area of intense research and development. At the same time, our strong dependence on the Internet has made them strategic national assets. With distribution of a world wide web progress cyber threats became the global phenomenon. Cyber threats continue to grow every day. Therefore, cyber space must be protected to ensure national security and prosperity.

The scientific article deals with the basic concepts and signs of cyber security. The object of research is the cyber security of modern society. The subject of the study are the basic concepts and signs of cyber security.

Keywords: cyber space, cyber security, cyber fraud, Internet, social networks, virtualization of consciousness.

Jel codes: F52, H5, K24, L14, L86.

М.Ө. НАСИМОВ¹

¹Саяси ғылымдарының кандидаты, қауымдастырылған профессор, ректор міндетін атқарушы, «Болашақ» университеті (Қызылорда)

Қазіргі заманғы әлемде жаһанданудың бет алысы күннен күнге артып келеді. Көз алдымызда Төртінші өнеркәсіптік революция кеңінен өрісін жаюда. Бұл революцияның негізгі ерекшелігі ретінде адамды ақпараттық технологиялар ықпалы тетіктерін пайдалану арқылы киберкеңістікке ендіру екендігін атап өте аламыз. Ғаламторда жаңа виртуалды ортаның пайда болуы қоғамдық өмірде көптеген өзгерістер әкелгендігі белгілі. Осы ғаламтор адам санасын өзгертудің басты себебі бола отырып, адамзатты шынайылықтан айырды.

Заманауи жаһандық ақпараттандыру әлемдік қауымдастықтағы мемлекеттердің қызметін белсенді басқарудың құралы болып табылады. Өз кезегінде ақпараттық

технологиялар ұлттық, әскери, экономикалық қауіпсіздікті қамтамасыз ету міндеттерін шешуде қолданылады. Мемлекеттік құрылымдардың жаһандық ақпараттандыру жағдайындағы іргелі алғышарттарында бәсекелес мемлекеттер күресінде жаңа орта киберкеңістік пайда болды.

Зерттеу жұмысының өзектілігі төмендегідей тұжырымдармен айқындалады: біріншіден, ақпараттық қауіпсіздік саласындағы терминдерге сәйкес киберкеңістік және киберқауіпсіздік ұғымдарының біртұтас термині қалыптаспаған. Екіншіден, киберкеңістік қызметінің барлық салаларын қамтитын және ықпалынан туындайтын қатерлерден қорғанысты қамтамасыз ететін көрсеткіштердің кешенді жүйесін әзірлеу қажеттілігі байқалады.

Үшіншіден, киберкеңістік қызметіне ықпал ететін негізгі факторлар мен қауіп-қатерлер үлгілерін білуіміз қажет. Төртіншіден, киберкеңістікке қауіпсіздік төнгенде оның мызғымастығын қамтамасыз ететін арнайы әдістер мен тәсілдерді меңгергеніміз дұрыс. Бесіншіден, киберқауіпсіздікті қамтамасыз етуде зияткерлік әдістерді қолдануды ерекше назарда ұстауымыз қажет.

Сонымен қатар, Қазақстан Республикасының Президенті Н.Ә. Назарбаевтың 2017 жылғы «Қазақстанның Үшінші жаңғыруы: жаһандық бәсекеге қабілеттілік» [1] атты Қазақстан халқына Жолдауында Үкімет пен Ұлттық қауіпсіздік комитетіне «Қазақстан киберқалқаны» жүйесін қалыптастыру шараларын қабылдауды тапсыруы ғылыми-зерттеу жұмысының өзектілігін арттырады.

Internet Live Stats агенттігінің сараптамалық зерттеулеріне сәйкес еліміз Интернет қолданушылар саны бойынша 43 орынды иеленіп отыр. Ұйымның ресми интернет-ресурсындағы бұл мәлімет өткен жылдың 1 шілдесінде берілген. Қолжетімділік бойынша Қазақстанда 10 миллионға жуық тұрғындар ғаламтор желісін пайдаланады. Соңғы жылдардағы көрсеткіш бойынша еліміздегі пайдаланушылар саны екі пайызға артқан. Бүгінгі күнде Қазақстан тұрғындарының 68 пайызының Интернет желісін қолдану мүмкіндігі бар. Ел ішіндегі ғаламторды пайдаланушылардың бір мезгілде 60 пайызға артқандығы байқалады. Соңғы жылдары Қазақстан түрлі рейтингтерде жоғары орындарға жетіп отырғандығын айта кеткеніміз жөн [2].

Әдебиеттерге шолу: Жалпы киберқауіпсіздік мәселелеріне байланысты еңбектер әлеуметтік-гуманитарлық ғылымдар саласында өте аз кездесетіндігін мойындауымыз қажет. Бұл өз кезегінде зерттеу жұмысын жүргізу барысында өз қиындықтарын туғызды. Дегенмен, зерттеу жұмысының ғылыми нысанына айналып отырған түсінікті Батыс ғалымдары қарқынды түрде зерттеп келеді [3], [4], [5]. Тақырып бойынша соңғы жылдары жарық көрген А. Сингхал (A. Singhal) [6], Р. Кларк (R.A. Clarke), Р. Нейк (R.K. Nake) [7], Д. Фрэнк Хсю (D. Frank Hsu), Д. Маринуччи (Dorothy Marinucci) [8] еңбектерінің теориялық маңыздылығы жоғары.

Ресейде 2013 жылдан бастап киберқауіпсіздік мәселелеріне арналған «Вопросы кибербезопасности» (<http://cyberus.com/>) атты ғылыми, ақпараттық-әдістемелік журнал тұрақты түрде жарық көріп келеді. Бүгінде 18 саны жарық көрген басылым ақпараттық қауіпсіздік саласына байланысты көптеген ғылыми мақалаларды жариялады.

Сонымен қатар, Ресейдің «Юрист» баспа тобы «Право и кибербезопасность» ғылыми-тәжірибелік және ақпараттық журналын 2014 жылға дейін шығарып келді [9].

Ресейлік авторлар қатарынан С.Л. Зефиров, А.Ю. Щербакова [10], Э. Кудинов, М. Дьяков, В. Ялтонский [11] еңбектерін ерекше атап өтуімізге болады. Ресей ғылым Академиясының жүйелік талдау институтының 2006 жылы Д. Черешкиннің [12] редакторлығымен жарыққа шығарған еңбектері ақпараттық қоғамдағы киберқауіпсіздік мәселелерін қарастырады.

Елімізде берілген сала бойынша зерттеулер аз жүргізілетіндігі байқалады. Отандық зерттеушілер арасынан Н.А. Биекенов [13], Л. Қаратаева [14], Г.С. Мәуленов [15] еңбектері маңызды деп ойлаймыз.

Материалдар мен әдістер

Зерттеу жұмысының әдістемелік және теориялық негізін шетелдік, ресейлік және отандық ғалымдардың еңбектері құрайды. Ретроспективті және салыстырмалы тұрғыдан талдайтын әр түрлі тұжырымдамалар және жүйелі-құрылымдық, тарихи-философиялық, институционалды талдау әдістері нәтижені алуға арқау болды. Зерттеудің міндеттері танымның жалпы ғылыми әдістері мен пәнаралық тәсілдерді қолдану негізінде ашылды.

Талқылау және нәтижелер

Бүгінде қатерлі сипатқа ие ақпараттық қауіпсіздік саласындағы оқиғалардың күрт өсімі байқалады. Көптеген кибершабуылдар мемлекеттік, жеке мүдделерге нұқсан келтіріп отыр. Қатерлер дамуының негізгі себептері мыналар деп ойлаймыз:

біріншіден, қомақты шығындарға әкелетін шабуылдар санының артуы; екіншіден, бірнеше кезеңдерден тұратын күрделі шабуылдардың көбеюі; үшіншіден, барлық электронды құрылғылар ықпалының арта түсуі; төртіншіден, мемлекеттік маңызы бар ақпараттық құрылымдарға жиі шабуылдардың жасалуы.

Киберкеңістік — бұл технологиялық құрылғы мен желілік байланыстар нәтижесіндегі адамдардың өзара қатынастарына ықпал ететін күрделі орта. Ұғымды алғаш рет 1982 жылы канадалық жазушы-фантаст Уильям Гибсон (W. Gibson) «Омни» журналында жарияланған «Хром өртелуі» (орысша: «Сожжение Хром», ағылшынша: «Burning Chrome») новелласында қолданған.

Жалпы киберкеңістікті қолданыстағы ғаламтормен шатастыруға болмайды. Аталмыш кеңістік компьютер желісінде кеңінен таралған барлық нысандарды сипаттауда

қолданылады. Мәселен, мемлекет немесе қалаларда орын алған ғаламтор оқиғалары іс жүзінде серверлерде орналасқанмен, жағдаят киберкеңістікте жүзеге асады. Киберкеңістіктегі қауіпсіздік ұғымы көп қырлы болғандықтан, оны түсіндіруде күрделіліктер туындайды. Сонымен бірге, түрлі деңгейдегі түсініктер мен көзқарастар да қалыптасты.

Ақпараттық кеңістікте барлық қолданушыларға ықпал ететін түрлі мән-мағыналар мен идеяларға толы мәліметтер киберқатысуды туындатып отыр. Киберкеңістікке ақпараттық вирустар енгізетін, адам санасын улайтын және құлдырау үдерістерін дамытатын қатерлер өте көп екендігі жасырын емес. Дегенмен, бүгінде вирустар заманауи қоғамды ақпараттандырудағы адам санасына ену деңгейінің көлемін айқындау күрделілік туындатады. Мәселен, біз қоғамдық пікірді қалыптастыру тетіктері мен әлеуметтік инженерия жұмыстарының әдістерін дәл әрі нақты анықтай алмайтындығынымыз анық.

Осы жылдың басында үш жүзге жуық түрлі сайттарға, оның ішінде биліктің жергілікті атқарушы және өкілдік органдарына хакерлік шабуылдар жасалғандығы белгілі болды. Кибершабуылдарды талдау және тексеру орталығының (ЦАРКА) хабарламасы бойынша бұзу барысында 323 сайтқа жаппай дефейс (веб-сайттың басты беті өзгеріске ұшырайтын хакерлік шабуылдар) жасалған. Кибершабуылдарға мемлекеттік органдармен қатар, ауруханалар, колледждер, театрлар мен кітапханалар ұшырады [16]. Ағымдағы жылдың наурызында Kaspi, Halyk Bank, «Казкоммерцбанк», «Сбербанк» және «Астана Банкі» өз клиенттеріне мәлімдеме жасады. Қаржыгерлер мәлімдеме арқылы банктік интернет қызметін пайдаланушылар шоттарына жасалуы мүмкін кибершабуылдар туралы ескертті [17].

Касперский Лабораториясының өткен жылғы қарашасындағы зерттеулері нәтижесінде еліміздегі мекемелердің 97 пайызы ішкі кибершабуылдарға ұшырап, компаниялардың 72 пайызы ақпараттық қауіпсіздіктің ішкі күрделі ахуалдарға тап болды. Мұндай оқиғаларға байланысты отандық компаниялардың 39 пайызы бизнес үшін маңызды қаржылық ақпараттар, клиенттердің жеке мәліметтері секілді құжаттарынан айырылды [18].

Байланыс технологияларының дамуы және ғаламтор қолданушылар белсенділігінің өсуіне байланысты бүгінде қылмыстың Интернет алаяқтық түрі ерекше артып отыр. Ғаламтор желісіндегі алаяқтық түрлері өте көп және технологиялардың дамуына байланысты жаңа алаяқтық қызмет түрлері пайда болуда. Азаматтардан алаяқтық жолмен табыс табуды көздеген бірнеше кең тараған түрлерін атап өтсек:

- беделді қызмет көрсетіп келе жатқан немесе түрлі банктік, несиелік ұйымдардың ресми сайттарын көшірген жасанды немесе тіркелмеген Интернет-дүкендер, фишингтік сайттармен байланысты алаяқтық;
- тіркеу жазбаларын ақшаға бұғаттан босатуды көздейтін танымал әлеуметтік желілердің жалған істелген сайттары;
- танымал брендтердің атын жамыла отырып файлдар алмасудың жасанды жүйесін құру;
- қайырымдылық қорлары, ауыр науқасты балалар ата-аналары атынан ғаламтордан көмек сұрау;
- қолданушылар файлдарын ғаламторда, телефонда шектейтін және мәліметтерді қайта қалпына келтіру үшін қаржы сұрайтын бұғаттау бағдарламалары;
- қолданушылардың түрлі ережелерді бұзғандығын негізге ала отырып айыппұл төлеуді сұрайтын бұғаттау бағдарламалары;
- әлеуметтік желі аккаунттарында, онлайн ойындарда, ақпарат алмасу жүйелеріндегі мәліметтерді «ұрлау» арқылы өзгенің атынан қимылдар жүргізу;
- ауқатты тұрғындарға бағытталған және олардан ақшаны алдап алуды көздейтін жасанды неке агенттіктері;
- қомақты сома төлеу арқылы ұтыссыз онлайн-лотереяларға қатыстыру;
- компьютерге алдамшы вирус тарату арқылы жалған антивирустарды сатып алу туралы ұсыныстар;
- рейтингісі жоғары ғылыми журналдардың «ұрланған» сайт нұсқалары;
- түрлі қоғамға танымал азаматтардың атын жамыла отырып тауарды олардың келісімінсіз насихаттау;
- түрлі онлайн төлемақылармен байланысты алаяқтық.

Сондықтан жоғарыда аталған кибералақтыққа жол бермеу және ұрынбау үшін қоғам мүшелерінде киберқылмыстарды алдын алу және қарсылық мәдениетін қалыптастыру қажеттілігі көрініп тұрғандығы анық.

Ғаламтордың жастарға ықпалы туралы ғылыми қауымдастықта аз талқыланып жатқан жоқ. Басым бөлігі Интернеттің құндылығы мен оның қоғамдық игілігіне мән береді. Дегенмен, желіде отырудың бірнеше әлеуметтік-психологиялық өзгерістерін бөліп көрсетуімізге болады.

1. Жастардың ғаламтор кеңістігіне гипер қосылуы арқылы олардың шынайы өмірмен байланысы үзіледі. Кибертәуелділік шамадан тыс ақпарат иелену, техноқүйзелістер, ойындар мен ғаламторға тәуелділік, өзін киберкейіпкермен ұқсату және сәйкестендіру, қиял мен фантазияға берілген эскапизмге ұмтылыс сынды нәтижелерге апарды. Жасанды интеллекттің тұлғаға ықпалы жастарды компьютерлік «тапшылыққа» ұрындырады.

2. Ғаламтор байланысы тұлғааралық қатынастарды өзгерту арқылы тілдесудің жаңа белгілерін қалыптастырады. Араласудың дәстүрлі түрлері жастардың басым көпшілігінің адамдармен шынайы байланысқа түскеніне қарағанда, компьютермен «достығы» артып отыр. Жастардың технологияларды тәжірибелі түрде пайдалануы виртуалды тілдесуде оларды кәсіпқой мамандандырса, шынайы өмірдегі тұлғааралық қатынастар барысында құрбы-құрдастарымен араласуымен қатар, отбасылық қарым-қатынастарда кейбір күрделіліктер туындатып отырғандығы жасырын емес.

3. Ғаламтордағы мол ақпаратпен белсенді жұмыс жасау барлық психологиялық процестермен байланысты когнитивті салаларда, білім беру мен сыни ойлауда өзгерістер туындатады. Ғаламтордың ақпараттық және білім беру қызметтері арасындағы айырмашылықтарды айқындап алғанымыз дұрыс. Білімгерлердің білім берудегі Интернетті оқу тапсырмалары мен емтихандарға дайындалудың жалғыз сенімді дереккөзі деп түсінуі қате пікір. Іздестіру сайттары көп жағдайда ақпараттардың қысқаша іріктелген топтамасын ұсынып, өзге сайттарға сілтеме беру арқылы қызығушылықты басқа арнаға бұрады.

4. Балалар мен жастардың әлеуметтену процесінде сапалық өзгерістер орын алады. Ғаламтор бүгінде әлеуметтену қызметін ақпараттану заманындағы отбасы, ата-аналар, мектеп ықпалының әлсіреуіне байланысты атқарып келеді. Бұл мәселеге байланысты автордың бірнеше ғылыми мақалалары жарық көрген болатын [19, 20, 21].

Киберқауіптерді алдын алудың бірі ретінде әлеуметтік желілер контентін басқару саналады. Бүгінде халықтың басым бөлігі, әсіресе жастар уақыттың басым бөлігін әлеуметтік желілерде өткізеді. Қазіргі таңда

әлеуметтік желілер адамдар санасында бейнелер, түсініктер мен мінез-құлық тәртібін қалыптастыратын еліктірудің қарымды құралы саналады.

Қазіргі таңда әлеуметтік желілердегі қоғамдық пікір қалыптастырудағы ақпараттардың басты тақырыптары мыналар: *қоғамдық қауіпсіздік мәселелері* (полиция қызметкерлері мен азаматтар арасындағы түсініспеушіліктерді желіге қою, соңғы кезде көбейіп кеткен педофилдер, өзгенің жеке бас бостандығын сыйламау, кәмелетке толмағандарға қарсы қылмыстар және т.б.); *қоғамдық этикалық құндылықтар мәселелері* (суицид, жат қылықтарға, құмар ойындарға бағыныштылық, тұлғаға қарсы зорлық-зомбылық көріністері, жағымсыз кейіпкерлер қалыптастыру); *педагогикалық мәселелер* (мектеп мұғалімдері мен оқушылар арасындағы қарым-қатынас, ҰБТ кезіндегі сенсациялық жаңалықтар мен құлық-сұмдықтарды ақпараттандыру, мектеп бітірушілердің тест жауаптарын таратуы).

Сондықтан болар осыдан екі жыл бұрын Қазнет пайдаланушылары Қазақстан Республикасының әлеуметтік желілер туралы Заңын қабылдау туралы бастаманы қызу талқылады. Виртуалды кеңістіктегі кез келген қимылдарды қатаң бақылауға қарсы топтар Қазақстанның авторитарлық елдер ізімен жүреді деген пікірде. Басым бөлігі арнайы заң қабылдамай, ҚР «Бұқаралық ақпарат құралдары туралы» Заңға әлеуметтік желілерге қатысты бақылау құзіреттілігін ұсынды. Сонымен қатар, ғаламторды белсенді пайдаланушылар ойынша, интернетте орын алып жатқан қылмыстарды алдын алуда қазақстандық құқық қорғау органдарының күштері жеткілікті. Қазақстан Республикасы Ішкі істер министрі Қ.Н. Қасымов бір сөзінде криминалды полиция базасында «К» арнайы бөлімшесі құрылғандығы туралы да айтқан болатын. Министр соңғы жылдары елімізде киберқылмыстың саны артып кеткендігіне де назар аудартты. Мәлімет бойынша 2014 жылы 21 қылмыстық іс қозғалса, 2015 жылдың өзінде 66-ға жетіп отыр [22].

Бүгінде алдыңғы қатарлы елдер тәжірибесінде онлайн режимдегі контенттерді өңдейтін және талдайтын арнайы киберорталықтар жұмыс жасайды. Бұл орталықтар бір мезгілде миллиондаған адамдарға ықпал ететін контенттерді орасан зор жылдамдықта таратумен айналысады. Мұндай киберорталықтар жаңалықтарда пікірлер білдірумен, троллингпен, ақпараттарды жолдаумен айналысады. Олардың әрекеттерін ғаламтордағы қарапайым қолданушылардан ажырату қиынға соғады.

Қоғамдық пікірді қалыптастыру бағытында ақпаратты жаппай беру және қолданушылардан алынған мәліметтерге дәйексіз сенімі арқылы жүреді. Киберботтар үгіт-насихаттық жарнамалар, түсініктемелер және ақпараттық таратылымдар секілді өзге әдістер арқылы ұйымдастырылатын фильмдер, мультфильмдер, ойындар тұрғындар мінез-құлқы тәртібін қалыптастырады. Киберқауіпсіздік саласындағы қазіргі таңдағы күрделі мәселе ретінде жасырып әлеуметтік-мәдени қатерлердің орын алуы жатады. Бұл мәдени белгілер жүйесін жоюға әкелетіндігін ескерсек, мәдени құндылықтарды сақтауға бағытталған әрекеттерді әзірлеуге қатысу қажет.

Питсбург университетінің профессоры Кимберли С. Янг (Kimberley S. Young) кибертәуелділіктің бес түрін бөліп көрсетеді: *киберсексуалды бағыныштылық* – порносайттарға құштарлықты жеңе алмайтын тәуелділік; *виртуалды танысуларға әуестік* – желідегі таныстары мен достарының тым артықтығы; *желіге байланған мұқтаждық* – құмарлық онлайн ойындарға қызығушылық, үздіксіз сатып алу немесе аукциондарға қатысу; *шамадан тыс ақпаратты иелену* (мұқтажға ие web-серфинг) – желідегі шексіз саяхат, мәліметтер базасы мен іздеу сайттарында ақпараттар ізденісі; *компьютерге бағыныштылық* – компьютерлік ойындарға тәуелділік [23].

Заманауи психиатрияда сананың виртуалдануы түсінігі зерттеу нысанына айналды. Сананың виртуалдануы қоғамды басқарудың тарихи деңгейінде орын алады. Виртуалды шындықтың үш негізгі сипаттамалық белгілерін бөліп көрсетуімізге болады: *материалдық емес ықпал ету* (контенттің затқа тән ықпал етуі); *параметрлердің шарттылығы* (нысандар жасанды және өзгермелі); *тұрақсыздық* (кіру/шығу еркіндігі тоқтату және жаңартуды қамтамасыз етеді) [24].

Ғаламтордың заманауи қоғамды виртуалдандырудағы рөлі төмендегідей деген ойдамыз:

- ғаламтор адамдар арасындағы тілдесудің көлденең байланысын орнатады;
- ғаламтор ақпаратты мәжбүрлеп ұсынбайды, тек өз еркімен қабылдауды ұсынады;
- ғаламтор кез келген адамның ақпараттық үрдістерге қатысуына мүмкіндік береді;
- ғаламтор манипуляциялау технологияларын жасырын түрде жүргізеді;
- ғаламтор адамның еркін ойлауына мүмкіндік береді, бірақ құқықтық нормаларды сақтауды пайдаланушыға жүктейді;
- ғаламтор ақпараттық өзара қимылдардың жаңа саласын қалыптастырады және қоғамдық

қатынастардың жаңа түрлерінің қалыптасуына ықпал етеді. Қорытынды

Ғаламторға алғаш енген адам Бүкіләлемдік жүйе құрылымы, оның пайдалы қызметтері және пайдаланушының желіде күтіп тұрған қауіпсіздіктері туралы ақпараттарды білмейді. Қоғамда азамат Интернетті пайдалануды көздесе, оның жеке мәселесі деген ұғым қалыптасқан. Бірақ бұл қате түсінік деп ойлаймыз. Берілген мәселені шешу үшін қолданушыларға ықтимал қатерлер туралы тиімді түрде мәлімет бергеніміз жөн деген пікірдеміз. Ғаламтор қолданушы түрлі кибер қимылдар жүргізу арқылы оның қаржылық, құқықтық жағымсыз зардаптары туралы ақпаратты білуі керектігін ескергеніміз жөн.

Беріліп отырған зерттеу жұмысының тақырыбы – өте күрделі және ерекшеліктері ұшан-теңіз. Ел тұрғындарын ғаламтор желісіндегі киберқауіпсіздік туралы ақпараттық қолдау жасау және дамытуға бағытталған көптеген шаралар өткізу қажеттілігі байқалып отыр.

Біріншіден, киберқауіпсіздік туралы өзекті ақпараттарды жеткізу тетіктерін әзірлеу және енгізу қажет. Әрбір қолданушы ғаламтор желісін пайдалануда ықтимал қатерлер туралы ақпараттар мен қауіпсіздікке қатысты ұсыныстармен танысуы тиіс деп ойлаймыз. Әсіресе, бұл жаңадан желіге қосылған немесе ғаламторды толықтай түсінбеген азаматтарды кибертәрбиелеуге жол ашады.

Екіншіден, желіде жұмыс жасауды көздеген қолданушыларға арнайы оқыту курстарын әзірлеу қажеттілігі байқалады. Бұл зейнет алды азаматтар үшін өз тиімділігін көрсететіндігі анық. Сонымен қатар, әлеуметтік желілерге жаңадан тіркелген азаматтар үшін маңыздылығы жоғары.

Үшіншіден, тұрақты түрде қатерлер туралы ақпараттарды жинау жүйесін әзірлеу керек. Бұл мәселеге қатысты ұғымдарды бекіте түсетіндігіне сеніміміз мол.

Төртіншіден, алаяқтықпен айналысатын сайттардың қара тізімін жасау және тұрғындарға ұсыну қажет. Ғаламтор пайдаланушылар Интернет-адресі білу арқылы аталмыш ресурстарға енуден бас тартады.

Бесіншіден, мектеп, колледж және жоғары оқу орындарына, кейбір білім беру бағдарламаларына ақпараттық қауіпсіздік және ақпараттық технологиялардың құқықтық негіздерін оқыту тетіктерін әзірлеу қажеттілігі байқалады. Заманауи тәжірибе көрсеткендей, берілген мәселе алдағы уақытта өз өзектілігін жоғалтпайды.

Алтыншыдан, ғаламтор желісіндегі қауіпсіздікті қамтамасыз етуге бағытталған және кеңес беретін ақпараттық портал әзірлеу

қажет. Баршаға қол жетімді порталда жас ерекшеліктері мен ықтимал мүдделеріне сай мынадай ақпараттар орналастырылуы қажет деп ойлаймыз: компьютер жүйесі мен ғаламтор желісіндегі қауіпсіздік бойынша негізгі сұрақтарға жауаптар; алаяқтық қимылдар және белгілерінің кең тараған түрлері туралы ақпарат; алаяқтықпен айналысатын сайттардың белгілері; компьютердің зақымдануы, бұғатталуы, бопсалаушылық секілді т.б. қалыптасқан жағымсыз ахуалдан шығу жолдары бойынша ұсыныстар; дағдарысты жағдайда жәрдем беретін қол жетімді ұйымдар туралы ақпарат.

Аталған ұсыныстарды жүзеге асыру қоғам үшін маңызды. Мәселен, құқық қорғау органдары ақпараттық технологиялар саласындағы қылмыстар бойынша алдын алу жұмыстарын жүргізе алады.

Интернет-провайдерлер пайдаланушы азаматтарға жұмыс жасау бойынша қамқорлық дәрежесін арттыра түседі.

Ғаламторда белсенді пайдаланушылар онлайн қаржылық ұйымдарына сенімі артылып, еліміздің қаржылық құрылымдарына жаңаша көзқарастар қалыптасады. Азаматтардың киберқауіпсіздік туралы ақпараттану және қорғану деңгейі артады.

Сөйтіп, заманауи адамға шынайы өмірден бөлінген санамен өмір сүру қолайлылық әкелетіндей. Қоршаған үдерістер және құбылыстармен шынайы қатынастарды қалпына келтіру нақты айқындалған әлеуметтік технологиялар арқылы жүзеге асуы мүмкін. Киберқауіпсіздік мәселелерін шешу киберкеңістіктегі ақпараттық ағындарды ажыратумен қатар, адамзат санасы, оның мәдени құндылықтарын қалыптастыру арқылы орын алады. Қоғамның мәдени белгілерін қалыптастыратын киберкеңістікті басқару қатынасы тәжірибесін сезіну және технологиялық жағынан қолдануды ескеру қажет.

ӘДЕБИЕТТЕР ТІЗІМІ

1. Қазақстанның Үшінші жаңғыруы: жаһандық бәсекеге қабілеттілік. Қазақстан Республикасының Президенті Н.Ә. Назарбаевтың Қазақстан халқына Жолдауы // Егемен Қазақстан. – 2017. – 31 қаңтар.
2. По количеству интернет пользователей Казахстан оказался на 43 месте // <http://webdream.kz/> [Электронный ресурс] – Режим доступа: <http://webdream.kz/po-kolichestvu-internet-polzovatelej-kazakhstan-okazalsya-na-43-meste/>
3. Solms R., Niekerk J. From information security to cyber security // Computers & Security. – 2013. – Vol. 38. – P. 97-102. - <http://dx.doi.org/10.1016/j.cose.2013.04.004>
4. Bob-Harb E., Debbabi M., Assi C. A novel cyber security capability: Inferring Internet-scale infections by correlating malware and probing activities // Computer Networks. – 2016. – Vol. 94. – P. 327-343. - <http://dx.doi.org/10.1016/j.comnet.2015.11.004>
5. Bendovschi A. Cyber-Attacks – Trends, Patterns and Security Countermeasures // Procedia Economics and Finance. – 2015. – Vol. 28. – P. 24-31. - [http://dx.doi.org/10.1016/S2212-5671\(15\)01077-1](http://dx.doi.org/10.1016/S2212-5671(15)01077-1)
6. Singhal A. Data warehousing and data mining techniques for cyber security. - New York: Springer, 2007. – 157 p. - ISBN - 978-0-387-26409-7.
7. Кларк Р.А., Нейк Р.К. Третья мировая война. Какой она будет? высокие технологии на службе милитаризма. - СПб: Питер, 2011. - 336 с. - ISBN - 978-5-459-00308-6.
8. Hsu D.F., Marinucci D. Advances in cyber security: technology, operations, and experiences. - New York: Fordham univ. press, 2013. - 257 p. - ISBN -978-0-8232-4456-0.
9. С 2014 года издание журнала приостановлено // <http://lawinfo.ru/> [Электронный ресурс] – Режим доступа: <http://lawinfo.ru/catalog/magazines/pravovye-voprosy-svjazi/>
10. Зефилов С.Л., Щербакова А.Ю. Управление инцидентами кибербезопасности. - Пенза: Изд-во ПГУ, 2012. – 102 с. - ISBN - 978-5-94170-559-7.
11. Кудинов Э., Дьяков М., Ялтонский В. Выжить в цифровом мире. Иллюстрированные советы от «Лаборатории Касперского». – СПб.: Питер, 2015. – 144 с. – ISBN – 978-5-496-01905-7.
12. Проблемы кибербезопасности информационного общества / Труды института системного анализа Российской академии наук. – М.: КомКнига, 2006. – 280 с. – ISBN – 978-5-484-00960-2.
13. Биекенов Н.А. Некоторые проблемы обеспечения кибербезопасности в Республике Казахстан // Право и государство. – 2013. - №4. – С. 29-31.
14. Қаратаева Л. Ақпараттық қауіпсіздік vs киберқауіпсіздік: мағынасы мен мазмұны // Адам және қоғам. – 2014. - №1. – 15-23 бб.
15. Мауленов Г.С. Кибербезопасность // Сардар. – 2014. – №3. – С. 42-46.
16. Казахстан подвергся массовой кибератаке // <http://nv.ua/> [Электронный ресурс] – Режим доступа: <http://nv.ua/world/countries/kazakhstan-podvergsja-massirovannoj-kiberatake-562733.html>
17. Пять банков Казахстана предупредили клиентов о возможных кибератаках на их счета // <http://today.kz/> [Электронный ресурс] – Режим доступа: <http://today.kz/news/finansyi/2017-03-11/737919-pyat-bankov-kazahstana-predupredili-klientov-o-vozmozhnyih-kiberatakah-na-ih-scheta/>
18. Казахстан: Кибермошенники эксплуатируют социальную инженерию из-за бездействия государства и компаний // <https://digital.report/> [Электронный ресурс] – Режим доступа: <https://digital.report/kazakhstan-kibermoshenniki-ekspluatiruyut-sotsialnuyu-inzheneriyu-iz-za-bezdeystviya-gosudarstva-i-kompaniy/>

19. Насимов М.Ө. Қазіргі заманғы медиакөшістіктегі азаматтық журналистика // Л.Н. Гумилев атындағы ЕҰУ Хабаршысы. Гуманитарлық ғылымдар сериясы. – 2015. - №5 (108). II бөлім. – 326-332 бб.
20. Насимов М.Ө. Интернет кеңістігіндегі киберәлеуметтендірудің өзекті мәселелері // әл-Фараби. – 2016. - №1 (53). – 104-117 бб.
21. Насимов М.Ө. Жастардың киберәлеуметтендірілуінің өзекті мәселелері // «Жастар саясатын қалыптастыру және жүзеге асырудың ерекшеліктері» атты жастардың өзекті мәселелері бойынша халықаралық ғылыми-тәжірибелік конференцияның материалдары. – Астана: Л.Н. Гумилев атындағы Еуразия ұлттық университеті, «Жастар» ғылыми-зерттеу орталығы, 2016. – 125-129 бб.
22. В Казахстане хотят принять закон о социальных сетях // mail.ru [Электронный ресурс]. – Режим доступа: <https://news.mail.ru/inworld/kazakhstan/politics/22447670/>
23. Янг К.С. Диагноз – интернет зависимость // Электронный ресурс. – Режим доступа: <http://www.narcom.ru/ideas/common/15.html>
24. Иванов Д.В. Виртуализация общества. – СПб.: Петербургское востоковедение, 2000. – 96 с. - С. 18. - ISBN 5-85803-154-4.

ВОЕННЫЕ ДОКТРИНЫ СТРАН СНГ: ОБЩЕЕ И ОСОБЕННОЕ

УДК 327:355 (47-57)

Аннотация. Автором статьи проводится сравнительный анализ военных доктрин стран - участниц Содружества Независимых Государств. Актуальность проблемы углубления военно-политического сотрудничества обусловлена общей историей, идентичностью внешних и внутренних угроз национальной безопасности. В результате комплексного анализа выявлены общие и специфические положения военных доктрин стран Содружества, а также проанализированы место и роль военно-политического сотрудничества во внешнеполитической стратегии каждого участника СНГ. Показано влияние внутренних и внешних факторов на формирование национальных подходов к сотрудничеству в военно-политической сфере на пространстве СНГ.

Ключевые слова. Военная доктрина, военно-политическое сотрудничество, безопасность, национальные интересы.

Аңдатпа. Мақала авторы Тәуелсіз Мемлекеттер Достастығына қатысушы елдердің әскери доктриналарын салыстырады. Әскери-саяси ынтымақтастықты тереңдету мәселесінің өзектілігі жалпы тарихпен, ұлттық қауіпсіздікке сыртқы және ішкі қауіптердің сәйкестілігімен түсіндіріледі. Кешенді талдаудың нәтижесінде Достастық елдерінің әскери доктриналарының жалпы және нақты ережелері анықталды, сондай-ақ әрбір ТМД-ның сыртқы саяси стратегиясында әскери-саяси ынтымақтастықтың орны мен рөлі талданды. ТМД кеңістігіндегі әскери-саяси саладағы ынтымақтастыққа ұлттық көзқарастарды қалыптастыруға ішкі және сыртқы факторлардың әсері көрсетілген.

Тірек сөздер. Әскери доктрина, әскери-саяси ынтымақтастық, қауіпсіздік, ұлттық мүдделер.

Abstract. The author of the article compares the military doctrines of the countries participating in the Commonwealth of Independent States. The urgency of the problem of deepening military-political cooperation is conditioned by the common history, the identity of external and internal threats to national security. As a result of a comprehensive analysis, the general and specific provisions of military doctrines of the Commonwealth countries were revealed, and the place and role of military-political cooperation in the foreign policy strategy of each CIS member was analyzed. The influence of internal and external factors on the formation of national approaches to cooperation in the military-political sphere in the CIS space is shown.

Keywords: Military doctrine, military-political cooperation, security, national interests.

JEL код: H 56, D74. E 62

Р. Р. ЧУКАЛОВА¹

¹докторант Академии государственного управления
при Президенте Республики Казахстан

Ухудшение обстановки в мире, наличие непрекращающихся локальных конфликтов, а также периодически возобновляемые очаги напряженности на постсоветском пространстве актуализируют необходимость

рассмотрения вопроса о способности постсоветских государств обеспечить собственную безопасность в среднесрочной и долгосрочной перспективе. И в этом контексте важно проведение анализа военных доктрин стран-участниц СНГ, поскольку именно в них