УДК 974.01
МРНТИ 19.21.11 https://www.doi.org/10.51889/2959-6017.2024.82.3.007

*Б.Н. Жұмаділ [*1], А.П. Жанысбаева [2]*

[1]с.ғ.м., Л.Н. Гумилев атындағы Еуразия Ұлттық Университеті,
журналистика және саясаттану факультетінің 3-курс докторанты Қазақстан, Астана қаласы,
bolat.zh.n@mail.ru
[2]Ph.D, М.Әуезов атындағы Оңтүстік Қазақстан университеті,
Филология факультетінің аға оқытушысы Қазақстан, Шымкент қаласы,
akniet.zhanysbayeva@mail.ru

АҚПАРАТ АҒЫНЫ АРҚЫЛЫ ЖҰМСАҚ КҮШ САЯСАТЫН ҚОЛДАНЫП ОТЫРҒАН МЕМЛЕКЕТТЕР ТАРАПЫНАН КИБЕРҚАУІПСІЗДІКТІ САҚТАУ: ҚАЗАҚСТАН МЫСАЛЫНДА

Аңдатпа

Киберқауіпсіздік ұғымы мемлекеттің ұлттық деңгейдегі қауіпсіздігіне тікелей байланысты феномен. Ғаламтор желісі, әлеуметтік желілер немесе кез келген ақпарат таратушы көздер белгілі бір әлеуметтік топтарға әсер ету үшін қолданылады. Егер ақпараттық басқару немесе ықпал ету сырт мемлекеттен келсе онда бұл жұмсақ күш стратегиясының бір бөлігі саналады. Сөйте тұра цифрлық технологияларды толық көлемде қолдану қазіргі қоғамның ажырамас бөлігіне айналды. Ал ақпараттық технологиялар мемлекет-тік басқарудың барлық дерлік салаларында: экономика, білім, денсаулық, саяси, әкімшілік және т.б. қолданылады. Әлемнің осындай цифрландыру жүйесіне жаппай көшуі әр мемлекеттің ұлттық деңгейде өз деректерін кибершабуылдардан қамтамасыз ету өзекті мәселеге айналып отыр. Әлемнің озық мемлекет-тері мемлекетті ақпараттандыруда және деректерді пайдалануда қауіп төндіретін кибершабуылдармен күресу мақсатында кешенді стратегиялық жұмыстарын әлдеқашан бастаған. Соған қарамастан кибер-шабуылдың саны күн сайынғы дамуға сәйкес азайған емес. Керісінше қауіпсіздікті қастамасыз ету жаңа деңгейге өткен, әрі күрделене түскен. Осы тұста Қазақстанның да өз халқы мен мемлекеттік аппаратта-рын шабуылдардан қорғау мақсатында жұмыс жасауы әлі де тиісті деңгейге жеткен жоқ. Оған себеп және кедергі болатын мәселелер мен оның шешу жолдарына ұсыныстар осы мақалада талданатын болады.

Кілт сөздер: *жұмсақ күш, ақпарат ағыны, ақпараттық басқару, киберқауіпсіздік, Қазақстандағы киберқауіпсіздік.*

Жұмаділ Б.Н.[*1], Жанысбаева А.П.[2]*

[1]докторант 3-курса Евразийского национального университета им. Л.Н. Гумилева, факультет Журналистики и политологии Казахстан, г.Астана, bolat.zh.n@mail.ru
[2]Ph.D, старший преподаватель Южно-Казахстанского университета им. М.Ауэзова, факультет Филологии, Казахстан, г.Шымкент, akniet.zhanysbayeva@mail.ru

ПОДДЕРЖАНИЕ КИБЕРБЕЗОПАСНОСТИ ГОСУДАРСТВАМИ С ИСПОЛЬЗОВАНИЕМ «МЯГКОЙ СИЛЫ» ПОСРЕДСТВОМ ИНФОРМАЦИОННОГО ПОТОКА: НА ПРИМЕРЕ КАЗАХСТАНА

Аннотация

Понятие кибербезопасности – явление, напрямую связанное с национальной безопасностью государства. Интернет, социальные сети или любой другой источник информации используются для воздействия на определенные социальные группы. Если информационный контроль или влияние исходит от иностранного государства, это считается частью стратегии мягкой силы. Однако полноценное использование цифровых технологий стало неотъемлемой частью современного общества. А информационные технологии используются практически во всех сферах государственного управления: экономике, образовании, здравоохранении, политике, управлении и т. д. Массовый переход мира на такую систему цифровизации становится актуальным вопросом для каждого государства по защите своих данных от кибератак на национальном уровне. Передовые страны мира уже начали

комплексную стратегическую работу по борьбе с кибератаками, создающими угрозу использованию информации и данных государством. Однако количество кибератак не уменьшается в соответствии с ежедневным развитием. Наоборот, пренебрежение безопасностью вышло на новый уровень и усложнилось. На данный момент усилия Казахстана по защите своего народа и государственного аппарата от нападений еще не достигли должного уровня. В этой статье будут проанализированы проблемы, которые вызывают и предотвращают это, и предложены решения.

Ключевые слова: мягкая сила, информационный поток, управление информацией, кибербезопасность, кибербезопасность в Казахстане.

Zhumadil B.N.[*1], Zhanysbayeva A.P.*[2]

[1]*3rd year doctoral student of L.N. Gumilyov Eurasian National University, Faculty of Journalism and Political Science, Kazakhstan, Astana, bolat.zh.n@mail.ru*
[2]*Ph.D, senior lecturer at M.Auezov South Kazakhstan University, Faculty of Philology, Kazakhstan, Shymkent, akniet.zhanysbayeva@mail.ru*

MAINTAINING CYBER SECURITY BY STATES USING SOFT POWER THROUGH INFORMATION FLOW: KAZAKHSTAN AS AN EXAMPLE

Abstract

The concept of cybersecurity is a phenomenon directly related to the national security of the state. The Internet, social networks or any other source of information are used to influence certain social groups. If information control or influence comes from a foreign state, it is considered part of a soft power strategy. However, the full use of digital technologies has become an integral part of modern society. And information technologies are used in almost all areas of public administration: economics, education, healthcare, politics, management, etc. The massive transition of the world to such a digitalization system is becoming an urgent issue for every state in protecting its data from cyber attacks at the national level. The world's leading countries have already begun comprehensive strategic work to combat cyber attacks that pose a threat to the use of information and data by the state. However, the number of cyber attacks is not decreasing according to the daily development. On the contrary, the disregard for safety has reached a new level and become more complex. At the moment, Kazakhstan's efforts to protect its people and state apparatus from attacks have not yet reached the required level. This article will analyze the problems that cause and prevent it and propose solutions.

Keywords: soft power, information flow, information management, cybersecurity, cybersecurity in Kazakhstan.

Кіріспе.

Ақпарат және интернет ағымы заманында өмір сүріп жатқан әрбір қоғамның өзара байланысы ақпараттық ресурстар арқылы іске асатыны белгілі. Қазіргі кезде әрбір мемлекеттің кез келген сайттарына кіру қолжетімді әрі шығу көзінің дұрыс-бұрыстығына қарамай кез келген ақпаратты алуға болады. Бұл жерде ақпарат таратушы әрбір тарап тек өзінің көздеген нысанасына жету үшін атсалысатындықтан, ақпараттың шынайы әрі қауіпсіз таралуына ешкім кепіл бере алмайды. Дегенмен өз ықпалын орнатқысы және күшейткісі келетін мемлекет, ұйым немесе топтар осы тұрғыда жұмсақ күш саясатын пайдаланады.

Жұмсақ күш ұғымын саясаттанушы Джозеф Най 1990 жылы «Soft Power» [1] еңбегінде алғаш атап өткені белгілі. Кейінірек бұл ұғымды «The Paradox of American Power: Why the World's Only Superpower Can't Goit Alone» еңбегінде кеңінен талдайды[2]. Яғни, саясаттанушы бұл терминнің анықтамасын «қатты күш» саясаты ұғымымен салыстырады. Қатты күш – мемлекеттік биліктің басқаларға қарсы қолданатын материалдық күші болса, жұмсақ күш – елдің басқаларға мәжбүрлеу немесе күштеу арқылы емес, өзіне еліктіру және сендіру арқылы рухани тұрғыда әсер ету мүмкіндігін білдіреді [3].

Жұмсақ күш елдің мәдениетінен, құндылықтарынан, саясаттарынан және институттарынан туындауы мүмкін және халықаралық қатынастарды қалыптастыруға және дипломатиялық мақсаттарға да жетуге көмектеседі.Демек, дәстүрлі биліктің күші азайып бара жатқан кезеңде әскери күш секілді билікті қолданудың тиімділігі азайып, керісінше жұмсақ күшті пайдалану маңыздылығы артады [4]. Мұндағы жұмсақ күшті тиімді пайдалану – өзге мемлекеттермен немесе ұйымдармен берік қатынас орнатудың бір құралы ретінде ақпараттық технологиялар мен коммуникацияның мүмкіндіктерін атап өтеді.

Осы тұрғыда қазіргі кезде көптеген мемлекеттер интернет күшін пайдалана отырып ақпарат ағыны арқылы жұмсақ күш саясатын ұстанып отырғаны жасырын емес. Яғни, ақпараттық жұмсақ күшті қолдана отырып ақпаратты, идеяларды, мәдениетті және құндылықтарды тарату арқылы әсер етуді көздейді. Мұнда қоғамдық дипломатия, мәдени өзара алмасулар, білім беру бағдарламалары, бұқаралық ақпарат құралдарымен жұмыс және белгілі бір идеологияны немесе әңгімені насихаттау сияқты әрекеттер кіруі мүмкін [5]. Ол елдің идеялары мен құндылықтарының тартымдылығын пайдалана отырып, қандай-да бір түсініктерді қалыптастыруға, қарым-қатынас орнатуға және ұлттық мүдделерді ілгерілетуге бағытталады.

Өзектілігі. Ақпараттық және коммуникациялық құралдарды пайдалану аясының кеңеюі әсерінен қауіпсіздікті қамтамасыз ету феномені туындайды. Әсіресе қазіргі өте жылдам даму үдерісінде жүрген қоғам үшін қауіпсіздікті бір табан алға қою басты назарға алынып отыр. Себебі, ақпараттың кеңінен таралуы әсерінен мемлекет өз халқын, ұйымдарын немесе мемлекеттік, аумақтық және аймақтық деңгейдегі кез келген топтарды сырттан келетін қауіп-қатерлерден қорғай отырып, қажетсіз және сапасыз мазмұндағы ақпаратты тұтынуды алдын-алу шараларын қолдануды жетелі зерттеу өзекті болып отыр.

Материалдар және Методология.

Материалдар. Ғылыми зерттеу мақаланы жазуға Қазақстан Республикасының «Ақпараттандыру» туралы заңының деректері, ақпараттық қауіпсіздік туралы тұжырымдамасы, сондай-ақ киберқауіпсіздік туралы Концепциясы материалдары пайдаланылды. Сонымен қатар, тақырыптың теориялық бөлімін зерделеу мақсатында Американдық саясаткер-зерттеушілердің еңбектері және Қазақстандағы ақпараттық ағындар мен киберқауіпсіздік деңгейін нақты сандар арқылы салыстыра көрсету негізінде отандық әрі шет елдік тәуелсіз зерттеуші институттардың мәліметтері жинақталып, аталмыш зерттеу жұмысын дайындауға пайдаланылды.

Методология.

Ақпараттық қауіпсіздік ұғымы туралы түсінік әр жерде әр қалай түсіндіріледі. Дегенмен Қазақстан Республикасының «Ақпараттандыру» туралы заңына сәйкес ақпараттық қауіпсіздік дегеніміз – электрон-дық ақпараттық ресурстардың, ақпараттық жүйелер мен ақпараттық-коммуникациялық инфрақұрылым-ның сыртқы және ішкі қатерлерден қорғау жағдайы [6].

Мемлекет өз территориясында ақпараттық қауіпсіздікті қамтамасыз ету үшін заңды түрде әрекет ететін нақты қадамдар жасайды. Мұнда адам, топ, ұйым немесе мемлекеттік деңгейдегі ұйымдардың қауіпсіздігі, бостандығы және азаматтық конституциялық құқықтар кешенді түрде қарастырылады. Оны іске асыру үшін техникалық, бағдарламалық, құқықтық тәртіп секілді құралдарды жүйелі түрде қолда-нады. Осыған орай Қазақстан Республикасы да өз территориясында өмір сүріп жатқан кез келген тұлға немесе ұйымның ақпараттық қауіпсіздігін қамтамасыз ету негізі Қазақстан Республикасының Конституциясы мен «Қазақстан Республикасының Ұлттық қауіпсіздігі туралы» 1998 жылғы заңдарынан бастау алады. Сонымен қатар, Қазақстан Республикасының 1999 жылғы «Мемлекеттік құпиялар туралы», 1999 жылғы «Терроризмге қарсы күрес туралы», 2003 жылғы «Электрондық құжат және электрондық цифр-лық қолтаңба туралы», 2003 жылғы «Ақпараттандыру туралы» және 2005 жылғы «Экстремизмге қарсы іс-қимыл туралы» заңнамалары ақпараттық қауіпсіздікті жан-жақты қамтамасыз ету мақсатында әзірленді [7].

Демек, кез келген қоғамның, мемлекеттің әлеуметтік тобының немесе жеке адамның қауіпсіз дамуы олардың ақпараттық қауіпсіздігіне тікелей байланысты. Өйткені ақпараттық орта – қоғамның бірден-бір бөлігі. Әрбір қоғам ақпараттық қауіпсіз орта қалыптастыруы керек. Бұл жердегі ақпараттық қауіпсіз орта – мемлекеттің, қоғамның, әлеуметтік топтың, жеке адамның өмірін сақтау үшін ақпараттық ресурстардың қауіпсіздігін қамтамасыз ету, ақпараттық қауіптерге, адамдардың жеке және қоғамдық санасы мен психикасына жағымсыз ақпараттық әсерлерге қарсы тұру қабілеті.

Бақылау және талқылау.

Ақпараттық қауіпсіздікті қамтамасыз етудегі стратегияның басты мақсаты –тұтынушының құпия-лығы мен оның жеке бас деректерінің таралмауын сақтау, антивирустық бағдарламаларды қамтамасыз ету, құқықтық жауапкершілік күшін арттыру, құрылғыларда пайда болған кез келген өзгерістерді бақылау және ақау туындаған сәтте оны шешудің жолын әзірлеу.

Қазақстанда отандық ақпараттандыру көздерінен бөлек шет елдік ақпараттық құралдары әдетте батыс мемлекеттерінен келеді. Сондықтан ақпарат таратудағы қауіп-қатерлер мен проблемалар да осы ресурс көздерінен шығу ықтималдылығы жоғары.

Қазақстандағы өмір сүретін халықтыңақпарат алатын негізгі ресурс көздері - әлеуметтік желілер (45,7%) және интернет сайттары (42,8%). Сондай-ақ елдің ішінде және сыртында орын алып жатқан оқиғаларды да теледидар арқылы (30,4%), туыстарымен, достарымен, таныстарымен және жұмыстағы

әріптестерімен (22,1%) сөйлесу арқылы біледі. Халықтың 6,5%-ы баспа БАҚ-ты, ал 3,9%-ы ғана радионы ақпарат көзі ретінде қолданады.

Халықтың басым көпшілігі теледидар арналарындағы көрсетілетін жаңалықтарға сенетініне қарамастан, Қазақстандағы негізгі ақпарат көзі – әлеуметтік желілер.

Әлеуметтік желілерді қолдануда көш бастап тұрған платформалардың бірі - Instagram. Бұл желіні қолданушылар ақпаратты жазбаша мәтін, видео, фото түрінде жариялай алады. Одан кейін Facebook. Бұл желіні пайдаланушылар әдетте ұзақ мәтінді жазбалар жариялайды. Дегенмен соңғы кезде трендке кірген, ақпаратты қысқа түрде тарататын TikTok желісі жас буын арасында кеңінен қолданылып жүр.

Мұнан да басқа әлеуметтік желілердің кез келген түрлері негізгі дереккөз бола алады. Мәселен Facebook желісінде шынымен де көптеген БАҚ-та пайда болмайтын жақсы, сенімді ақпарат бар. Және бұл әлеуметтік желілер өте маңызды ақпарат көзі бола алады[8].

Сонымен қатар, ақпараттық ресурстардан келетін қауіп-қатерлер тек ақпараттың шынайы-жалғандығына ғана қатысты емес, сондай-ақ тұтынушылардың дербес деректерін бұзуға, ұрлауға бағытталған іс-әрекеттер де жатады.

Сарапшылардың пайымдауынша, Қазақстан үшін жиі кездесетін киберқауіптер әлеуметтік секторға кибершабуылдар (жеке деректерге шабуыл жасау), вирустық шабуылдар, мемлекеттік секторға шабуыл жасау, фишингтік шабуылдар, алаяқтық, мемлекеттік емес салаларға залал келтіру, сондай-ақ қаржы секторына жасалған шабуылдар жатады.

Әсіресе соңғы жылдары қарқынды дамып келе жатқан цифрландыру жүйесі – ақпараттық қауіпсіздікке қауіп тудыратын бірден-бір жолы. Мәселен, М.Губайдуллина өз зерттеуінде цифрландыруды қорғалмаған әрі ашық дереккөзі ретінде санады [9]. Оның пікірінше, халықаралық аренадағы дипломатия-лық қарым-қатынастар аясында мемлекеттің цифрландыру жүйесін қолдануы оның ұлттық қауіпсіздігіне нұқсан келеді. Дегенмен Э.Вильборг, К.Хедстрем және Х.Ларссонның тұжырымдауы бойынша цифрлан-дыру саясаты мемлекеттік қызметтерді көрсетудің өнімділігін арттыра отырып оның ашықтығын көрсе-теді [10]. Цифрландыру халық үшін жылдам, қызметтерді онлайн жүзеге асыра алатын әрі төлемдерді онлайн төлеуге болатын, жылдам ақпарат бере алатын ыңғайлы құрал саналады. Күнделікті өмірде мемлекеттің кез келген азаматы әртүрлі анықтамаларды, теңгерімдерін тексеру, онлайн сауда жасау секілді кез келген қызмет түріне қол жеткізіп отыр. Бұл тұрғыда цифрландыру оң нәтижелерді көрсете алады.

Цифрландыру өзініңоң ықпалына қарамастан жүйені бұзу, дербес деректерге қол жеткізу секілді шабуылдарға көптеп ұшырайды. Бұл әрекет заманауи қоғамда – кибершабуыл деп аталады. Ақпарат тұтынушы кез келген адам, топ, ұйым, тіпті мемлекеттік құпияны сақтаушы дербес сайттар да кибершабуылға тап болуы мүмкін. Кибершабуыл жасайтын ақпараттық заң бұзушылар мемлекеттің өз адамдары немесе шет елдік азаматтар да болуы мүмкін. Сол себепті, жоғарыда атап өткендейақпарат ағыны заманында жұмсақ күштің қолына тап болып кибершабуылға ұшырап жатқан тараптар аз емес. Бұл жағдайға бірінші кезекте жауапты – мемлекет. Және кибершабуыл түрлеріне қарай ол істі заңмен қудалау міндетті.

Осы тұста НАТО-ның бұрынғы қолбасшысы Джеймс Дж. Ставридис ақпараттық қауіпсіздік туралы білдірген ойының маңыздылығын атап өткен дұрыс: «Мені түнде (НАТО күштерінің қолбасшысы ретінде) ұйықтатпайтын бір нәрсе бар. Ол – киберқауіпсіздік. Киберқауіпсіздік ұлттық мүдделеріміздің ең жоғары деңгейлерінен: медицина, білім, жеке қаржы жүйелері арқылы келеді...» [11]. Мұндағы киберқауіпсіздік – бұл электрондық түрдегі ақпараттың және оны өңдеуге, сақтауға, сыртқы және ішкі қауіптерден тасымалдауға арналған ортаның, яғни ақпараттандыру саласындағы ақпараттық қауіпсіздіктің жай-күйі [12].

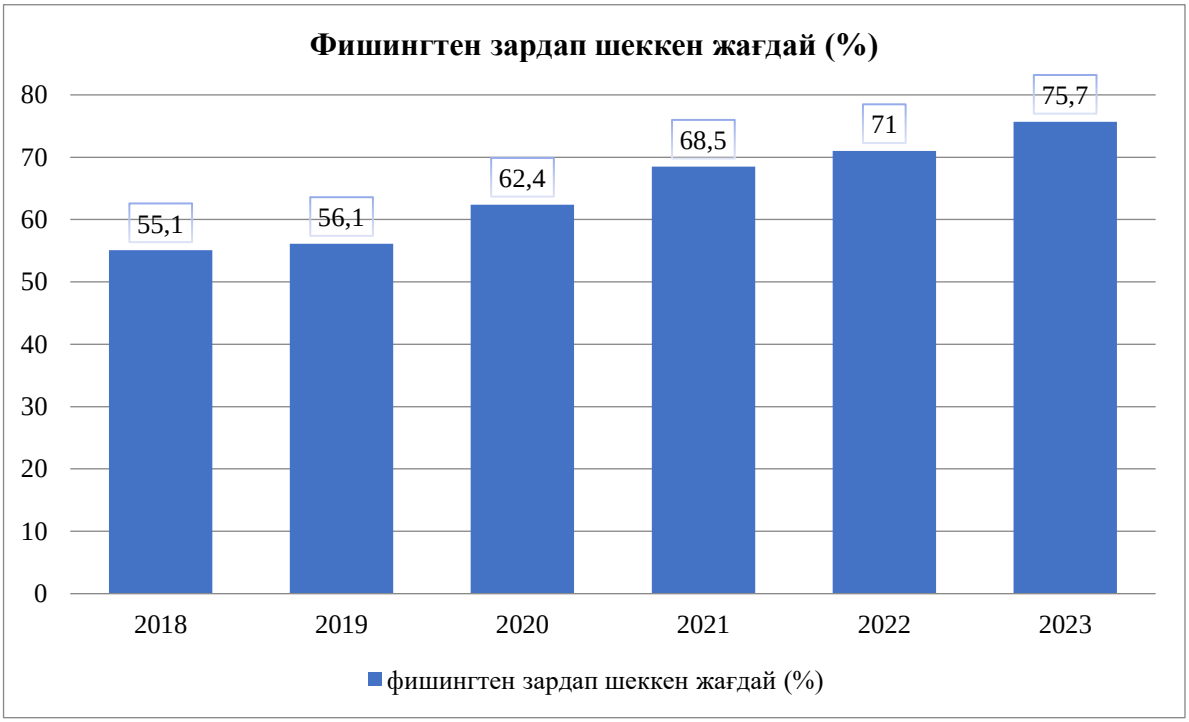
Қазақстан ақпараттық қауіпсіздікті қамтамасыз ету жөнінде заңнама қабылданымен іс жүзінде кибершабуылдан зардап шеккен адамдар мен ұйымдар саны аз емес. Керісінше ол жыл сайын артып келеді. Мәселен 2023 жылғы статистика бойынша кибершабуылдан зардап шеккендердің саны бойынша Қазақстан әлем бойынша 7-орынды тізгіндеді.Олардың қатарында қарапайым халықтан бастап ірі ұйымдарға дейін бар [13].

Олардың көпшілігі, яғни жиі шабуыл жасайтын сайттар – ботнеттер. Ботнет немесе зомби желісі – зиянкестерге иелерінің хабарынсыз басқа адамдардың құрылғыларын қашықтан басқаруға мүмкіндік беретін зиянды бағдарламамен зарарланған компьютерлер желісі. Ботнеттерді пайдалана отырып, шабуылдаушылар спам жібере алады, вирустар таратады, компьютерлер мен серверлерге шабуыл жасай алады және басқа да қылмыстарды жасай алады.

Ақпараттық шабуыл жасайтын кеңге таралған тағы бір кибер қылмыс түріне – фишинг жатады. Бұл компьютерлік алаяқтықтың негізгі мақсаты – интернет пайдаланушылардың шоттары мен банктік ақпаратын ұрлау.

Аталмыш фишинг шабуылы 2022 жылдың бірінші ширегін 2023 жылдың бірінші ширегімен салыстыратын болсақ 12%-ға артқан. Ал жалпы корпоративтік сектордағы фишинг шабуылдары 120%-ға өсті.

Ал Statista мәліметі бойынша жаһандық ұйымдардың төлем бағдарламаларынан зардап шеккен жағдайларының өсуін мына сандардан көруге болады (1-сурет):



1-сурет. Statista мәліметі бойыншафишингтен зардап шеккендер саны (%)

2023 жылғы кибершабуылдардың басым бөлігі компьютерлерге зиянды вирустардыңшабуылынан орын алған. Оның алдыңғы жылдың өзінде саны 3 мыңға жетті, яғни жыл сайынғы өсім 71,2% көрсеткішті көрсетті.

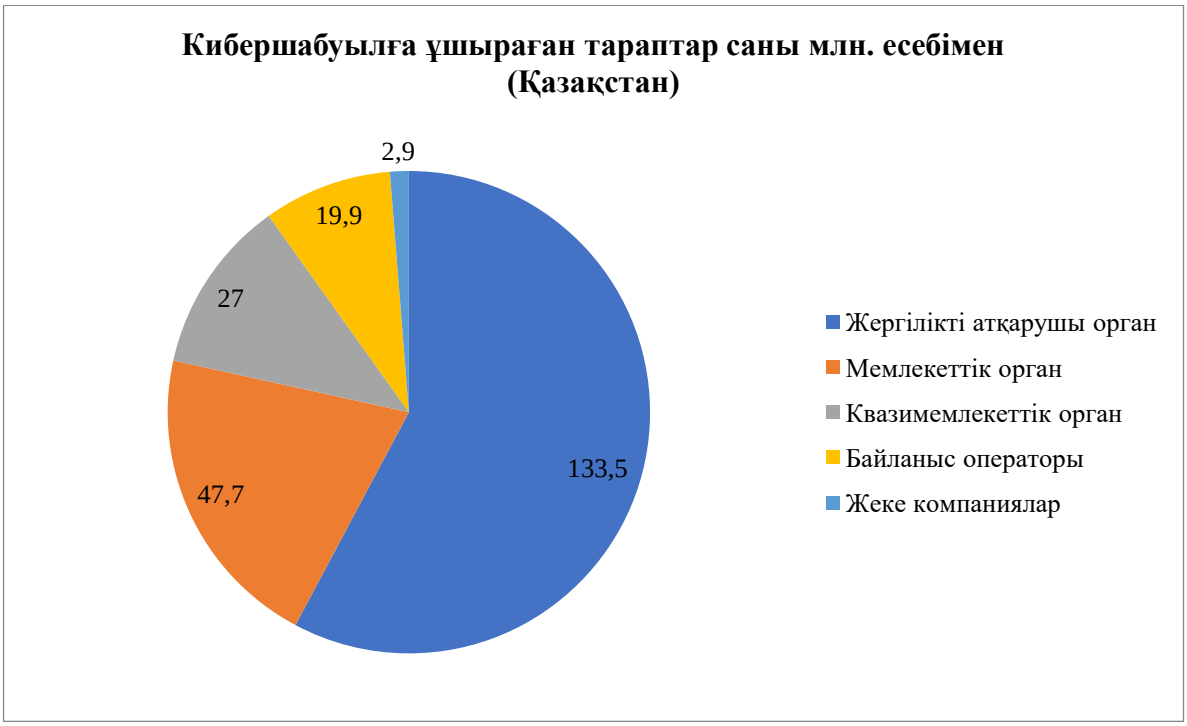
Ботнеттер (3 мың жағдай), интернет-ресурсқа кіре алмау (813 жағдай), фишинг (628 жағдай), рұқсат-сыз сайтқа кіріп кету және интернет-ресурстың мазмұнын өзгерту (317 жағдай), қызмет көрсетуден бас тарту (118 жағдай) сияқты жағдайлары да жиі байқалды [14].

Кибершабуылдың түр-түріне қарамастан, оның жыл сайынғы арту себебін тек көлемі жағынан ғана түсіндіру мүмкін емес. Себебі жоғарыда келтірілген 2018 жылғы статитика мен 2023 жылғы статистика арасында цифрлық даму жағынан елдің киберқауіпсіздігін қамтамасыз етуде көп өзгерістер мен алға даму орын алды. Кибершабуылдан қорғайтын көптеген құралдар пайда болып арнайы жүйе де құрылды. Дегенмен хакерлер де бір орында қалмайтыны белгілі, олар да ақпарат пен қаржыларға қол жеткізудің жаңа жүйесін жетілдіріп отырады. Яғни жоғарыдағы бір фишингтен көріп отырған статистика киберқауіпсіздікті қамтамасыз етудің тиімдігі, болмаса тиімсіз екендігін көрсетпейді, керісінше қорғаушы тарап пен шабуыл жасаушы тараптың өз нысанасына жетуде қаншалықты алға ілгерілеп жатқанын көрсетеді.

Қазақстаннның қылмыстық істер жөніндегі статистикасында кибер жабуылдан зарттап шеккен тараптар туралы ақпараттар кездеспейді, немесе олардың саны өте аз деңгейде тіркеледі. Мысалы, Қазақстан Республикасының Бас Прокуратурасының қылмыстық істер жөніндегі статистикасында 2022 жылы кибершабуылдан зардап шеккен 85 іс тіркелсе, одан кейінгі жылы оның саны небәрі 142-ге көтерілген [15]. Мұндағы басты назарға алатын нәрсе – аталмыш тіркелген құқық бұзушылық ақпаратқа немесе ақпараттық жүйеге заңсыз қол жеткізу бойынша орын алған.

Қазақстан қызмет көрсету саласы тұрғысынан заманауи цифрландыру жүйесін толықтай тұтынып отырған мемлекет. Әсіресе, онлайн қызмет көрсету мен банкингтік жүйені қарапайым халық кеңінен қолданады. Демек, ақша айналымы жүрген жерде кибершабуылдаушылардың да көз тігетіні сөзсіз. Оған қоса Қазақстан шет елдік ресурстарға қол жеткізе алатындықтан елдің кибершабуылшыларды еліктірері анық. 2023 жылы кибершабуылдың кез келген түріне тап болған кез келген тұтынушы жалпы

саны 223 миллионнан астам кибершабуылға ұшыраған. Кибершабуыл жасаушы тараптардың басым көпшілігі – АҚШ, Украина, Қытай, Ресей, Польша мемлекеттері [16].



2-сурет. Кибершабуылға ұшыраған тараптар саны

Айта кету керек, киберқауіпсіздік саласы Қазақстанда даму сатысында және бұл салада отандық мамандар аз. Алайда бұл тек Қазақстан үшін ғана проблема емес. Бүгінгі таңда көптеген елдер киберқауіпсіздік саласында жоғары білікті мамандардың тапшылығын сезінуде.

Осыған байланысты, ең алдымен, Республикада киберқауіпсіздікті қамтамасыз етудің келесі элемент-терден тұратын тиімді жүйесін құру қажет: заңнамалық, әдістемелік, кадрлық және осы жүйелердің жұмыс істеу механизмі.

Киберқауіпсіздікті қамтамасыз ету үшін тек материалдық-техникалық емес, сонымен қатар осы салада жоғары білікті мамандары бар нормативтік-құқықтық база болуы қажет. Көптеген зерттеушілер киберқауіпсіздікті қамтамасыз ету үлкен инвестицияны қажет ететінін атап өтеді, өйткені кез келген елде сандық деректердің қауіпсіздігін халықаралық және ұлттық деңгейде қамтамасыз ету қажет.

Сондай-ақ, мемлекет түрлі кибершабуылдарды алдын алу үшін келесідей шараларды ұстану керек:

3-сурет. Кибершабуылды алдын алу шаралары

1. Халықты киберқауіпсіздік туралы ұғыммен хабардар ету және білім беру: қарапайым халық арасында азаматтардың, бизнестің және мемлекеттік органдардың құпия сөздерді пайдалану, фишинг әрекеттерін тану және бағдарламалық құралды жүйелі түрде жаңарту сияқты бастапқы базалық білімді қалыптастыру.

2. Киберқауіпсіздікті қамтамасыз ететін инфрақұрылымға инвестиция салу: маңызды жүйелер мен желілерді қорғау үшін желіаралық қалқандарды, шабуылды анықтау жүйелерін және шифрлау протокол-дарын қоса алғанда, сенімді киберқауіпсіздік инфрақұрылымын дамыту үшін ресурстар бөлу маңызды.

3. ЫІнтымақтастық орната отырып қауіпсіз деңгейде ақпарат алмасу: мемлекеттік органдар, жеке сектор ұйымдары және халықаралық серіктестер арасында киберкеңістікте жауапты мінез-құлық нормаларын ілгерілету сияқты киберқауіптермен күресу үшін арнайы ынтымақтастықты дамыту.

4. Оқиғаларды алын алу: кибершабуылдарды тиімді азайту және қалпына келтіру үшін инциденттерге әрекет ету жоспарларын әзірлеу және үнемі жаңартып отыру керек.

5. Киберқауіпсіздікті зерттеу мен әзірлеу үшін қаржы бөлу: дамып келе жатқан қауіптерден ілгері болу үшін киберқауіпсіздіктің инновациялық технологиялары мен әдістерін зерттеу және оларды әзірлеу үшін ресурстарды бөлу керек.

6. Мемлекеттермен жеке серіктестік орнату: киберқауіпсіздік мүмкіндіктерін арттыру, озық тәжірибемен бөлісу және пайда болған қауіптерді бірлесіп шешу үшін мемлекеттік органдар мен жеке сектор ұйымдары арасындағы серіктестікті дамыту.

7. Үздіксіз мониторинг және бағалау: әлеуетті қауіптерді олар кибершабуылға ұласпас бұрын анықтау және азайту үшін киберқауіптер мен осалдықтарды үздіксіз бақылау мен бағалауды жүзеге асыру.

Жаһандық әлемде цифрландырудың қарқынды өзгеріп жатқан тенденцияларына байланысты осындай толықтырулар қарастырылған заңды әзірлеуге тура келеді. Бұл жылдам өзгеретін әлемнің талабы және Қазақстан жаһандану кезеңіндегі өзгерістер мен цифрлық трансформация жағдайларын елеусіз қалдыра алмайды. Дегенмен,2015 жылғы «Ақпараттандыру туралы» заң қабылданғаннан бері оған 15 реттен астам өзгерістер мен толықтырулар енгізілген, «Қазақстан Республикасының Ұлттық қауіпсіздігі туралы» заңына да өзгерістер мен толықтырулар енгізілгенін атап өткен жөн.

Алайда, жоғарыдағы көрсетілген статистиканы негізге ала отырып, мемлекеттік қызметшілердің басым бөлігі Республиканың құқықтық актілеріне өзгерістер мен толықтырулар енгізумен ғана айналысқанынкөруге болады. Киберқауіпсіздікті жақсарту үшін Қазақстан киберкеңістіктегі ықтимал қауіптерді анықтау үшін бірыңғай үкіметтік желіні енгізген озық мемлекеттердің тәжірибесін қарастыра алады. Бұл механизм оларға кибершабуылдар қаупін болдырмау үшін стратегия мен заңнамалық базаны әзірлеуге көмектесті [17]. Осылайша, Қазақстанның киберқауіпсіздік туралы заң жобасында келесі 4 негізгі бағытты қамтығаны дұрыс:

- Маңызды ақпараттық инфрақұрылымды кибершабуылдардан қорғауды күшейту.

- Киберқауіпсіздік қатерлері мен оқиғаларының алдын алуға және оларға әрекет етуге дайын болу.

- Кибер инциденттер туралы ақпаратты ортақ пайдалану үшін негіз жасау.

- Отандық бизнесті ынталандыру және қолдау мақсатында киберқауіпсіздік қызметтерін жеткізушілер үшін клиентке бағытталған лицензиялау жүйесін құру. Сондай-ақ лицензиялауға жеңіл тәсілді енгізу.

Жалпы, кибершабуылдар мен басқа елдердің ақпараттық қабылдауға әсері цифрлық дәуірдегі технология, геосаясат және қоғамдық пікір арасындағы күрделі өзара әрекеттесуді көрсетеді. Тиімді киберқауіпсіздік шаралары, дипломатиялық араласу және халықаралық ынтымақтастық осы динамикаларды басқару және зиянды кибер әрекеттердің ақпараттық қабылдау мен жаһандық тұрақтылыққа әсерін азайту үшін өте маңызды.

Басқа елдерден келетін интернет-ресурстардың ықтимал қауіптерінен қорғау үшін келесі шараларды ұстанған дұрыс:

1. Қауіпсіз және сенімді дереккөздерді пайдалану: ақпаратқа қол жеткізу, бағдарламалық құралды жүктеп алу және онлайн транзакцияларды жүргізу үшін беделді және танымал веб-сайттарды, платформа-ларды және қолданбаларды пайдалану.

2. Вирустарға тосқауыл қоятын бағдарламаларды қолдану: зиянды әрекеттерді, соның ішінде шетелдік көздерден шыққандарды анықтау және блоктау үшін құрылғыларда заманауи антивирустық бағдарламалық құралды, брандмауэрлерді және зиянды бағдарламаларға қарсы бағдарламаларды ұстау. Белгілі осалдықтарды түзету үшін операциялық жүйелер мен қолданбаларды үнемі жаңартып отыру.

3. Электрондық хаттар мен сілтемелерден сақ болу: Электрондық хаттарды, тіркемелерді ашқанда немесе белгісіз немесе күтпеген жіберушілерден, әсіресе шет елдерден келген сілтемелерді басқанда абай болу. Олар фишинг әрекеттері болуы мүмкін немесе құрылғыны бұзуға немесе құпия ақпаратты ұрлауға арналған зиянды бағдарламаларды қамтуы мүмкін.

4. Деректерді шифрлау: құпия деректер мен коммуникациялар көзін шифрлау, әсіресе ақпаратты желіде бөліскенде немесе басқа елдерде орналасқан жеке тұлғалармен немесе ұйымдармен байланысқан-да құпиялықты қорғау және деректерге рұқсатсыз кіруді болдырмас үшін қауіпсіз байланыс арналары мен шифрлауды пайдалану.

5. Жеке ақпараттың ашылуын шектеу: жеке ақпаратты ұрлау, киберталдау немесе шетелдік көздерден туындауы мүмкін онлайн қудалаудың басқа түрлері қаупін азайту үшін жеке ақпаратты, әсіресе жалпыға қолжетімді платформалар мен әлеуметтік медиа желілерінде ашуды барынша азайту.

6. Сандық ізді бақылауда ұстау: Сандық ізді және онлайн тіркелген кез келген күдікті әрекетке немесе рұқсатсыз кіруге, әсіресе, бөгде ұйымдардың кедергілері немесе кибер шабуылдарын үнемі бақылау.

7. Хабарлы және білімді болу: киберқауіпсіздіктің ең жақсы тәжірибелері, пайда болатын қауіптер және зиянды әрекеттер, соның ішінде басқа елдерден әрекет ететіндер қолданатын дамып келе жатқан тактикалар туралы хабардар болу.

Осы белсенді шараларды қабылдау және қырағы болу арқылы адам өз деректерін және цифрлық активтерді басқа елдердегі интернет ресурстарынан туындайтын ықтимал қауіптерден жақсырақ қорғай алады және ұлттық қауіпсіздік тұтастығын сақтауға септігін тигізеалады.

Жоғарыдағы талдауларға қарай отырып, киберқауіпсіздікті қамтамасыз ету үшін ұйымдастыру және басқару тәсілін кешенді түрде құру қажет екенін анық көруге болады. Сонымен, киберқауіпсіздік – командалық жұмыс және ондағы әрбір жауаптының өз рөлі бар. Үкімет IT-шешімдерді енгізуге қоғамды, квазимемлекеттік және жеке секторларды тарта отырып, Қазақстанда киберқауіпсіздікті дамытуды бастау мүмкіндігін қарастыруы қажет. Сондай-ақ, киберқауіпсіздік – мемлекет пен жоғарыда аталған мүдделі тараптармен қатар, жеке тұлғаның да жауапкершілігі.

Киберқауіпсіздік тұжырымдамасын жүзеге асыру аясында ең алдымен қоғамды киберкеңістікте болып жатқан өзгерістер туралы ақпараттандыру қажет. Бұл сәтсіздіктердің алдын алудың ең тиімді әдістерінің бірі деп саналады. Сонымен бірге, оның трансұлттық сипатын ескере отырып, үкіметтің киберқылмыспен күресудегі күш-жігерін күшейту керек.

Республикадағы заңнама нормалары мен құқық қорғау органдары мен соттарының қызметін киберқауіпсіздікке қатысты мәселелер тұрғысынан қарастырғаны жөн. Жоғарыда аталған іс-шаралар Қазақстанның халықаралық аренадағы мәртебесі мен тұрақтылығын IT-индустрияның сенімді хаб орталығы ретінде жақсартуға да ықпал етеді. Дегенмен, бұл мақсаттарға жету үшін алыс-жақын серіктестермен, ғылыми мекемелермен, үкіметтермен және үкіметтік емес салалық серіктестермен, сондай-ақ интернет-провайдерлермен тығыз жұмыс істеу қажет.

Қорытынды.

Қорытындылай келе, киберқауіпсіздік пен ақпараттық жұмсақ күш өзара байланысты екенін көруге болады, өйткені киберқауіпсіздіктің тиімді тәжірибелері елдің беделін арттыра алады, жаһандық қабылдауға әсер етеді және цифрлық домендегі құндылықтары мен мүдделерін ілгерілетеді. Киберқауіп-сіздікке инвестиция салу және киберкеңістікте жауапты мінез-құлықты ілгерілету арқылы елдер әлемдік деңгейдегі өздерінің стратегиялық мақсаттары мен мүдделерін ілгерілету үшін ақпараттық жұмсақ күшті пайдалана алады. Ал ақпарат ағыны арқылы жұмсақ күшті пайдаланатын мемлекеттердің киберқауіп-сіздікті сақтауы олардың мүдделерін қорғауға, цифрлық кеңістікте тұрақтылық пен қауіпсіздікті қамтамасыз етуге және халықаралық аренадағы беделін сақтауға көмектеседі.

Пайдаланылған әдебиеттер тізімі:

1. Joseph S. Nye, Jr. Soft Power. - Slate Group, LLC. - 1990. - pp. 153-171.

2. Nye J. Jr. The paradox of American power: why the world's only superpower can't go it alone. – N.Y.: Oxford University Press. – 2002.

3. Nye J.Jr. Soft power: the means to success in world politics. PublicAffairs.– Political Science. – 2009. – 208 p.

4. Anne-Marie Slaughter.The Chessboard and the Web: Strategies of Connection in a Networked World. – New Haven, CT, Yale University Press. – 2017. – 304 pp.

5. Crocker, Chester A.; Hampson, Fen Osler; Aall, Pamela R. leashing the dogs of war: conflict management in a divided world. – US Institute of Peace Press. – 2007. – p. 13.

6. Қазақстан Республикасының 2015 жылдың 24 қарашасындағы №418-V ҚРЗ «Ақпараттандыру туралы» Заңы. URL: https://adilet.zan.kz/kaz/docs/Z1500000418

*7. "Қазақстан Республикасының ақпараттық қауіпсіздік тұжырымдамасы туралы" Қазақстан Республикасының Президенті Жарлығының жобасы туралы Қазақстан Республикасы Үкіметінің 2006 жылғы 21 қыркүйектегі N 894 Қаулысы. URL: https://adilet.zan.kz/kaz/docs/P060000894_*

8. Социологическое исследование по медиапотреблению и медиаинформационной грамотности в странах центральной Азии. – 2021.URL: https://www.m-vector.com/uploads/files//64912ca4a6ede.pdf

9. Губайдуллина М. Внешнеполитическая деятельность и дипломатия в современных условиях транспарентного информационного пространства // International Relations and International Law Journal. – 2018. – Т. 79, №3 – С. 14-22.

10. Wihlborg E., Hedstrom K., Larsson H. E-government for all Norm-critical perspectives and public values in digitalization // Proceedings of the 50th Hawaii International Conference on System Sciences. – 2017. – С. 2549-2559.

11. Cybersecurity and Digital Business Risk Management. URL: https://www.gartner.com/en/information-technology/insights/cybersecurity

12. Постановление Правительства Республики Казахстан от 30 июня 2017 года № 407. Об утверждении Концепции кибербезопасности ("Киберщит Казахстана"). URL: https://adilet.zan.kz/rus/docs/P1700000407

13. Kaspersky CyberSecurity Weekend. URL:
https://forbes.kz/actual/technologies/kaspersky_kazahstan_zanyal_sedmoe_mesto_v_mire_po_kolichestvu_kiberatak/

14. Опасность из глубин интернета: количество кибератак в РК увеличилось на 56%. URL: https://energyprom.kz/ru/articles-ru/society-ru/opasnost-iz-glubin-interneta-kolichestvo-kiberatak-v-rk-uvelichilos-na-56/

15. В Казахстане растёт число кибер-преступлений. URL: https://wfin.kz/publikatsii/kazakhstan-v-tsifrakh/91787-v-kazakhstane-rastjot-chislo-kiber-prestuplenij.html

16. Основные страны – источники кибератак на Казахстан назвали в государственной технической службе. URL: https://informburo.kz/novosti/osnovnye-strany-istocniki-kiberatak-na-kazaxstan-nazvali-v-gosudarstvennoi-texniceskoi-sluzbe

17. Постановление Правительства Республики Казахстан от 12 декабря 2017 года № 827. Утратило силу постановлением Правительства Республики Казахстан от 17 мая 2022 года № 311. Об утверждении Государственной программы "Цифровой Казахстан". URL: https://adilet.zan.kz/rus/docs/P1700000827

References:

1. Joseph S. Nye, Jr. Soft Power. - Slate Group, LLC. - 1990. - pp. 153-171.

2. Nye J. Jr. The paradox of American power: why the world's only superpower can't go it alone. – N.Y.: Oxford University Press. – 2002.

3. Nye J.Jr. Soft power: the means to success in world politics. PublicAffairs.– Political Science. – 2009. – 208 p.

4. Anne-Marie Slaughter.The Chessboard and the Web: Strategies of Connection in a Networked World. – New Haven, CT, Yale University Press. – 2017. – 304 pp.

5. Crocker, Chester A.; Hampson, Fen Osler; Aall, Pamela R. leashing the dogs of war: conflict management in a divided world. – US Institute of Peace Press. – 2007. – p. 13.

6. Kazakhstan Republikasyn 2015 zhyldyn 24 karashasyndagi No.418-V KRZ "Akparattandyru turaly" Zany. URL: https://adilet.zan.kz/kaz/docs/Z1500000418

*7. "Kazakhstan Republikasyn akparattyk kuipsizdik tuzhyrymdamasy turaly" Kazakhstan Republikasyn President Zharlygyn zhobasy turaly Kazakhstan Republikasy Ukimetin 2006 zhylgy 21 kyrkuyektegi N 894 Kaulysy.URL: https://adilet.zan.kz/kaz/docs/P060000894_*

8. Sociological research on media consumption and media information literacy in Central Asian countries. – 2021.URL: https://www.m-vector.com/uploads/files//64912ca4a6ede.pdf

9. Gubaidullina M. Foreign policy and diplomacy in modern conditions of a transparent information space // International Relations and International Law Journal. – 2018. – Vol. 79, No. 3 – pp. 14-22.

10. Wihlborg E., Hedstrom K., Larsson H. E-government for all Norm-critical perspectives and public values in digitalization // Proceedings of the 50th Hawaii International Conference on System Sciences. – 2017. – C. 2549-2559.

11. Cybersecurity and Digital Business Risk Management. URL: https://www.gartner.com/en/information-technology/insights/cybersecurity

12. Resolution of the Government of the Republic of Kazakhstan dated June 30, 2017 No. 407. On the approval of the Cybersecurity Concept ("Cybersecurity of Kazakhstan"). URL: https://adilet.zan.kz/rus/docs/P1700000407

13. Kaspersky CyberSecurity Weekend. URL: https://forbes.kz/actual/technologies/kaspersky_kazahstan_zanyal_sedmoe_mesto_v_mire_po_kolichestvu_kiberatak/

14. Danger from the depths of the Internet: the number of cyber attacks in the Republic of Kazakhstan increased by 56%. URL: https://energyprom.kz/ru/articles-ru/society-ru/opasnost-iz-glubin-interneta-kolichestvo-kiberatak-v-rk-uvelichilos-na-56/

15. The number of cybercrimes is growing in Kazakhstan. URL: https://wfin.kz/publikatsii/kazakhstan-v-tsifrakh/91787-v-kazakhstane-rastjot-chislo-kiber-prestuplenij.html

16. The main source countries of cyber attacks on Kazakhstan were named in the state technical service. URL: https://informburo.kz/novosti/osnovnye-strany-istocniki-kiberatak-na-kazaxstan-nazvali-v-gosudarstvennoi-texniceskoi-sluzbe

17. Resolution of the Government of the Republic of Kazakhstan dated December 12, 2017 No. 827. It became invalid by the Decree of the Government of the Republic of Kazakhstan dated May 17, 2022 No. 311. On the approval of the State program "Digital Kazakhstan". URL: https://adilet.zan.kz/rus/docs/P1700000827