ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ПРЕЗИДЕНТІНІҢ ЖАНЫНДАҒЫ
МЕМЛЕКЕТТІК БАСҚАРУ АКАДЕМИЯСЫ

Басқару институты

Қолжазба құқығында

Ахметов Айдан Нурланович

ҚАЗАҚСТАН ЭКОНОМИКАСЫН ЦИФРЛАНДЫРУ ЖАҒДАЙЫНДА АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУДІ БАҒАЛАУ

«7М041 – Бизнес және басқару» дайындық бағыты бойынша
«Экономика» білім беру бағдарламасы

Экономика магистрі дәрежесін алуға арналған
магистрлік жоба

Ғылыми жетекшісі _____ Л.М. Сембиева, э.ғ.д.

Жоба қорғауға: «_____» _____ 2023 ж. жіберілді

Басқару институтының директоры _____ З.С. Гаипов, с.ғ.д.

Астана, 2023

Мазмұны

Нормативтік сілтемелер

Бұл магистрлік жобада келесі нормативтік құжаттарға сілтемелер қолданылды:

Қазақстан Республикасының «Ақпараттандыру туралы» 2015 жылғы 24 қарашадағы № 418-V ҚРЗ Заңы;

Қазақстан Республикасы Үкіметінің «Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарды бекіту туралы» 2016 жылғы 20 желтоқсандағы № 832 Қаулысы;

Қазақстан Республикасы Үкіметінің «Киберқауіпсіздік тұжырымдамасын («Қазақстанның киберқалқаны») бекіту туралы» 2017 жылғы 30 маусымдағы № 407 Қаулысы;

Қазақстан Республикасы Үкіметінің «Цифрлық Қазақстан «Мемлекеттік бағдарламасын бекіту туралы» 2017 жылғы 12 желтоқсандағы № 827 Қаулысы;

Қазақстан Республикасы Үкіметінің «Киберқауіпсіздік тұжырымдамасын («Қазақстанның киберқалқаны») іске асыру жөніндегі 2022 жылға дейінгі іс-шаралар жоспарын бекіту туралы» 2017 жылғы 28 қазандағы № 676 Қаулысы;

Қазақстан Республикасының «Дербес деректер және оларды қорғау туралы» 2013 жылғы 21 мамырдағы № 94-V Заңы.

Белгілер мен қысқартулар

АЖ	– ақпараттық жүйе;
АКТ	— ақпараттық-коммуникациялық технологиялар;
АҚ	– ақпараттық қауіпсіздік;
АҚҰҰО	– ақпараттық қауіпсіздіктің ұлттық үйлестіру орталығы;
АР	– ақпараттық ресурстар;
БҰҰ	– Біріккен Ұлттар Ұйымы;
ЕҚЫҰ	– Еуропадағы қауіпсіздік және ынтымақтастық ұйымы;
ҚР	– Қазақстан Республикасы;
ҚР ЦДИАӨМ	– Қазақстан Республикасы Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігі;
РБ	– республикалық бюджет;
ХҚИ	– халықаралық қаржы институттары;
«МТҚ» АҚ	– «Мемлекеттік техникалық қызмет» акционерлік қоғамы;
«ЦҚ» МБ	– «Цифрлық Қазақстан» мемлекеттік бағдарламасы;
KZ-CERT	– Ұлттық компьютерлік инциденттерге әрекет ету қызметі.

Кіріспе

Зерттеу тақырыбының өзектілігі және көтерілген мәселесі. Соңғы жылдары Қазақстанда цифрландыру технологиялары сәтті түрде енгізіліп келеді. Атап айтар болсақ, цифрлық технологиялардың еліміздің экономикасын дамытудағы маңыздылығы артып келеді. Кез келген қоғам дамуының заманауи кезеңі оның тіршілігінің барлық аяларын қарқынды түрде ақпараттандырумен сипатталады. Сол себепті ақпараттық технологиялардың дамуы және оларды кеңінен қолдану әлем дамуының және соңғы онжылдықтардағы ғылыми-техникалық революцияның жаһандық тенденциясы болып табылады. Ақпараттық технологияларды қолдану экономиканың бәсекеге қабілеттілігін арттыру және мемлекеттік басқару органдары мен жергілікті өзін-өзі басқару органдары жұмысының тиімділігін арттыру үшін орасан зор маңызға ие. Сол себепті мемлекеттік билік органдарын ақпараттандыру еліміздің Үкіметінің алдына қойылған басым міндеттердің бірі болып табылады. Қазақстандағы ақпараттық технологиялардың жеткіліксіз дамуы ақпараттандыру саласындағы нормативтік-құқықтық актілердің жетілмегендігімен, ақпараттық технологияларды әзірлеу мен пайдалануда кадрлардың төмен дайындығымен және басқа да себептермен қиындай түседі. Сондай-ақ цифрлық экономиканың өзекті мәселелерінің бірі – киберқауіпсіздік.

Ақпараттық қауіпсіздік Қазақстанда ұлттық қауіпсіздіктің ажырамас бөлігі ретінде қарастырылады және еліміздің ақпараттық кеңістігін, сондай-ақ адам мен азаматтың, қоғам мен мемлекеттің ақпараттық салада рас әрі болуы мүмкін ықтимал потенциалды қауіп-қатерден қорғау жағдайы деп түсіндіріледі. Дәл осындай қорғау кезінде еліміздің тұрақты дамуы мен ақпараттық егемендігі қамтамасыз етіледі.

Жалпы қабылданған түсініктегі ақпараттық қауіпсіздік – ақпараттың құпиялылығын, толыққандылығын және қолжетімділігін қорғау. IT-дің қарқынды дамуының ағымдағы тенденциясы мемлекеттік құрылымдар қызметінің тиімділігін арттыра түсуде. Қазіргі уақытта әлем интеллектуалды цифрлық шешімдерді барлық жерде қолданумен «инновациялық» болашаққа қарқынды түрде бағыт алып, дамып келеді. Мемлекеттік секторда бұл көптеген өндірістік процестерді автоматтандыру мен жетілдіруге әкеледі. Мұндайда сәйкесінше киберқауіптер деңгейі де қарқынды түрде артады. Өз зерттеуінде Д.Н. Карпова секунд сайын 12 Интернет пайдаланушы кибершабуылдарға тап болатынын, жыл сайын 500 млн. киберинциденттер орын алатынын, олардың шығыны $100 миллиард АҚШ долларына тең келетінін атап өтті [1]. Жаһандық әлемде орын алып жатқан өзгерістер Қазақстанда Үкімет деңгейінде киберқауіпсіздікті қамтамасыз етудің өзекті мәселелерін растайды. Осы мақсатта санкцияланбаған қолжетімділік фактілерін азайту, «электрондық үкіметтің» ақпараттандыру нысандарында бар ақпаратты жойылудан қорғау және арам ниетті әрекеттердің алдын алу үшін ақпараттық қауіпсіздік мәселелерін шешуге кешенді көзқарасты ұстану қажет.

Тұрақты сын-қатерлер және қазіргі заман тренді желілік технологияларды

және қолданылатын технологиялық жабдықтардың қуаттылығын дамыту қажеттілігін, ақпараттық кеңістікті кеңейтуді, ақпараттық қауіпсіздікті қамтамасыз етудің және қауіп-қатерлерге әсер етудің жоғары деңгейіне қолжетімділік қажеттілігін айғақтайды. Әдетте ақпараттандырудың даму қарқыны ақпараттық қауіпсіздік бойынша жасалып жатқан мүмкін болар шаралардың барлығын озып түседі.

Осылайша, ақпараттық қауіпсіздікті қамтамасыз ету проблемалары мемлекеттік аппаратта АКТ-ні қолдану және цифрландыру салаларын дамытумен параллель не ілгері жүру қажеттілігін түсінуіміз қажет. Сол себепті мемлекеттің ең жоғары деңгейінде ақпараттық қауіпсіздікті қамтамасыз ету жөнінде қолданыстағы мемлекеттік шараларды кешенді бағалаудың айтарлықтай қажеттілігі туындайды.

Зерттеу мақсаты. Ақпараттандыру және байланыс аясындағы әлеумет пен мемлекеттік ақпараттық қауіпсіздігі, сонымен қатар ақпараттық-коммуникациялық технологиялар саласын пайдалануда азаматтардың жеке өміріне қолсұғылмаушылықты қорғау бойынша инциденттер санын төмендетуге мүмкіндік беретін ұсынымдар әзірлеу.

Зерттеу нысаны еліміздің ақпараттық қауіпсіздігін қамтамасыз етуге бағытталған мемлекеттік органдар функциялары болып табылады.

Зерттеу негізіне келесі **гипотеза** қойылған: АКТ пайдаланушыларының саны көп болған сайын ақпарат қауіпсіздігі қатері көп болады және ақпараттық қауіпсіздікке жұмсалатын инвестициялар деңгейі жоғары болған сайын ақпараттық қауіпсіздікті қамтамасыз ету деңгейі жоғары болады.

Әдебиетке шолу

Бүгінгі таңда халық пен кез келген ұйымдардың жұмысына қазіргі заманғы цифрлық технологияларды әзірлеуге және ендіруге негізделген цифрлық экономиканы қалыптастыру кезеңі жүріп жатыр. Үлкен деректерді талдауды жетілдіру, ұялы телефондарды кеңінен қолдану, Интернеттің дамуы, Интернетте заттардың пайда болуы жеке өңірлер мен елдер деңгейінде де, әлемдік деңгейде де әлеуметтік-экономикалық мәселелерді шешуі қажет инновациялық элементтер болып есептеледі. Цифрлық технологияларды дамытудың қазіргі жағдайында процестердің жылдамдай түсуі немесе күрделенуі экономикалық қызмет субъектілерін ақпараттық қауіпсіздік жөнінде ойлануына алып келеді. Азаматтардың және ұйымдардың жеке деректерін ұрлау материалдық залал әкеліп қоймайды, сонымен қатар беделге нұқсан келтіреді.

Ақпараттық қауіпсіздікті қамсыздандыру жөнінде заңнаманың теориялық-әдіснамалық көзі, негізі Қазақстан Республикасының 2050 жылға дейінгі Ұлттық қауіпсіздік стратегиясы болып табылады. Ол ұлттық қауіпсіздік жағдайын анықтайтын ақпараттандыру, телекоммуникация және байланыс секілді маңызды салаларда технологиялық артта қалуды еңсеру қажеттілігін, мемлекеттік және әскери басқару жүйелерінде, сондай-ақ экологиялық қауіпті өндірістерде және аса маңызды нысандарда ақпараттық қауіпсіздік технологияларын әзірлеу және ендіру қажеттілігін, сонымен қатар жаһандық ақпараттандыру желілері мен жүйелері бар ұлттық ақпараттық инфрақұрылымды үйлестіру үшін жағдай жасауды қамтамасыз ету қажеттілігін белгілейді [2].

Контрагенттердің қызметіне қандай да бір сенімнің жоғалуы кез келген қызмет түрінің тіпті қажет етілмейтін нәтижесі болып есептеледі. Сондықтан ақпараттық қауіпсіздікті қамтамасыз ету бойынша проблемалар мемлекеттік деңгейде де, жеке ұйымдар деңгейінде де реттестіруді керек етеді.

Ғылыми әдебиетте «ақпараттық қауіпсіздік» біржақты түсіндірілмейді. Т.А. Мартиросян өз еңбектерінде атап өткендей, ақпараттық қауіпсіздік – тұлғаны, қоғамды және мемлекетті ақпараттық аяда болуы мүмкін ішкі және сыртқы қауіптерден қорғау жағдайы [3]. Көп жағдайда осы секілді позиция О.А. Федотовта кездеседі. Оған сәйкес ақпараттық қауіпсіздік – мемлекеттің ұлттық мүдделерінің (тұлғаның, қоғамның және мемлекеттің өмірлік маңызды мүдделерінің теңдестірілген негізде) ақпараттық аяда ішкі және сыртқы қауіптерден қорғалу жағдайы [4].

А.В. Кисляковскийдің пікірінше, «...ақпараттық қауіпсіздік тұжырымдамалық сипатқа ие және ақпараттық ресурстардың (ақпараттың) қауіпсіздігін, басқа сөзбен айтқанда, физикалық және заңды тұлғалардың өзара және мемлекетпен қарым-қатынасы қауіпсіздігін қолдау міндеттерінің кешенін шешуді болжайды. Ақпараттық процестерді компьютерлендірудің қазіргі жағдайындағы ақпараттың қауіпсіздігі құнды ақпаратты заңсыз және жиі қылмыстық пайдаланудың алдын алу үшін, әсіресе отандық компьютерлік

жүйелердің халықаралық компьютерлік желілерге кіруіне байланысты маңызды болып табылады» [5].

Т.А. Полякованың пікірінше, ақпараттық қауіпсіздік жеке тұлғаның, қоғамдастықтың және елдің теңгерімді қызығушылықтарының жиынтығын қамтитын ақпараттық саладағы ұлттық қызығушылықтардың ішкі және сыртқы қауіптерден қорғалу жағдайы ретінде қарастырылады, бұл автордың пікірінше, Ақпараттық қоғамды даму стратегиясында белгіленген ақпараттық аядағы ұлттық қауіпсіздікті қамсыздандыру қағидатына сәйкес келеді [4].

В.Д. Курушин және В.А. Минаев ақпараттық қауіпсіздік түсінігінің астарында азаматтардың, ұйымдар мен мемлекеттің мүдделері үшін оның қалыптасуы мен дамуын қамтамасыз ететін қоғамның ақпараттық ортасының қорғалу жағдайын түсіндіреді [6].

Біздің түсінуімізше, ақпараттық қауіпсіздік – ақпараттық саладағы жеке тұлғаның, қоғамның және мемлекеттің қорғалу жағдайы. Бұл барлық мүдделі субъектілерді қажетті ақпарат көлемімен қамтамасыз етуге, тиісті ақпараттың әлеуметтік пайдалылығын қамтамасыз етуге, сонымен қатар барлық мүдделі субъектілердің қажетті ақпарат көлеміне қолжетімділікті қамсыздандыруға жағдай жасайды Ақпараттық қауіпсіздіктің доктринасы елімізде ақпараттық қауіпсіздігі деп дербес тұлғаның, қоғамдастықтың және тұтастай мемлекеттің теңгерімді қызығушылықтарының жиынымен анықталатын оның ақпараттық саладағы ұлттық қызығушылықтарының қорғалу жағдайы түсінілетінін айқындайды.

Ақпараттық шабуылдар әлемдік ауқымға ие болуы мүмкін. 2017 жылдың мамыр айында 150-ден астам елде компьютерлер WannaCry вирустық бағдарламасын жұқтырды. Бұл Ұлыбританияның Ұлттық денсаулық сақтау қызметін (NHS), испандық Telefonica телекоммуникациялық компаниясын, американдық FedEx логистикалық компаниясын, Германияның Deutsche Bahn ең ірі теміржол операторын және басқа да көптеген ірі компанияларды зақымдады. Nissan Motor және Renault автомобиль концерндерінде бірнеше орындарда өндіріс уақытша тоқтауға мәжбүр болды [7].

Экономиканың әртүрлі субъектілері арасындағы жоғары цифрлық өзара тәуелділік жағдайында қауіпсіз ақпараттық ортаны құру тұрақты цифрлық экономиканы қалыптастырудың баламалы элементі болмаса да ажырамас бөлшек болып есептеледі [8]. Ақпараттық қауіпсіздікті қамтамасыз ету тұрғысынан көптеген цифрлық технологиялардың ең аз бақыланатын бағыттары үлкен деректер, заттар Интернеті және жасанды интеллект технологиялары болып табылады. Қазірдің өзінде Amazon, Apple және Google сынды ірі ұйымдар жасанды сананы пайдалану негізінде, цифрлық платформалар құрды, ал Facebook әлеуметтік желісі DeepTex технологиясын іске асырды. Бұл технологияның негізінде әлеуметтік желіні пайдаланушылардың мінез-құлық ерекшеліктерін хабарламалар арқылы тану мүмкіндігі пайда болды [8]. Цифрлық технологиялардың потенциалды артықшылықтары, әлбетте, маңызды, бірақ оларды енгізу халықтың жеке ақпаратының қауіпсіздігіне қауіп төндіреді және

деректердің кішкене болса да таралып кетуі инновациялар мен жалпы экономикаға деген сенімге нұқсан келтіреді.

Жеке ақпаратты таралып кету салдарына алаңдаушылық цифрлық технологиялармен тура немесе қосалқы байланысы бар мәліметтерді ұрлау жағдайларының орын алуымен тығыз байланысты. Орын алған бұл жағдайлардың басым бөлігі цифрлық ортадағы әлеуметтік-экономикалық қызмет негізіндегі ақпараттың құпиялылығы, тұтастығы және қолжетімділігі саясатын бұзумен тікелей байланысты.

Бұл бұзушылықтар уақыт өте келе олардың салдарын жою жағынан көбейе, жиілене және күрделіне түсуі ғажап емес. Ақпараттық қауіпсіздікті бұзу пайдаланушылар жеке ақпаратты ұсынған компаниялардың әртүрлі қулық әрекеттерінен де туындайды. Мысалға, Канадада 2017 жылы осы секілді шағымдар екі жыл бұрынғы шағымдармен салыстырғанда 49%-ға көбірек тіркелді [9]. Бұл жағдайда ақпараттың таралып кетуі пайдаланушылардың ұсынылатын өнімдер, қызметтер және оларды сатып алу шарттары жөнінде қате ұрынуларына, сондай-ақ белгілі бір онлайн платформалардағы ақпаратты қорғаудың төмен деңгейіне байланысты болады.

Экономиканы цифрландыру жағдайында ақпараттық қауіпсіздік бұзушылықтары санының арта түсуі цифрлық технологияларды қолдану ауқымының ұдайы күрделенуімен және өсуімен байланысты. Соңғы жылдары ірі ұйымдар да, шағын да ұйымдар бизнеске жиі әрі күрделі ақпараттық бұзушылықтарға ұшырады [10]. Ірі компанияларда қолданылатын цифрлық технологиялар біртіндеп, уақыт өткен сайын сол ұйымдардың негізгі құндылықтарының біріне айнала бастады, сондықтан саяси немесе экономикалық мақсаттарда орын алып жатқан өнеркәсіптік шабуылдар жағдайлары сирек кездеспейді. Мысал келтірер болсақ, 2014 жылы Sony Pictures Entertainment-те ақпаратқа шабуыл жасап, ұрлау жағдайы белгілі болды, және тиісінше ұйымның дәл сол уақытта мүлдем жарияланбаған фильмдері, маркетинг және сату бөлімдерінің мәліметтері, барлық қызметкерлердің электрондық хаттары және басқа да осы секілді құпия ақпараттар ашық қолжетімді болды [11].

Ұлыбританияда жүргізілген зерттеу нәтижелері көрсеткендей, компания неғұрлым үлкен болса, соғұрлым ол ақпараттық қауіпсіздік құқықтарының бұзылуымен, шабуылдармен жиірек кездеседі: әртүрлі ақпараттық шабуылдарға ұшырайтындардың 84%-ы орта және ірі деңгейдегі кәсіпорындар болып табылады. Сондай-ақ назар аударарлық жайт, ұйымдардың 16%-ы ақпараттың таралып кету жағдайларының болғандығына сенімді емес, яғни мұқият назар аударуды қажет ететін белгісіздіктің үлесі басым [12].

Кез келген ақпараттық шабуылдардың экономикалық алып келер шығындарын болжау қиынға соғады. Өйткені кейбір компаниялар ақпараттық қауіпсіздік құқықтарының бұзылу жағдайларын, егер ол коммерциялық құпияны ұрлаудың заңды салдарларымен байланысты болмаса, хабарламауға тырысып жатады. Әртүрлі мәліметтердің жоғалуы, таралып кетуі көптеген кері, жағымсыз нәтижелерге әкеледі деп толық сеніммен айтуымызға болады. Мысал келтірер

болсақ, іскерлік имиджге нұқсан келтіру, бәсекеге қабілеттіліктің күрт төмендеуі, алаяқтық жағдайындағы әртүрлі есептелмеген, жоспарсыз қаржылық шығындар, өндірістік жоспарлардың, жеткізілімдердің бұзылуы, сондай-ақ жоғалған ақпаратты қалыпқа келтіру қажеттілігіне байланысты шығындардың арта түсуі.

М. Ысқақов өзінің ақпараттық қауіпсіздік мәселелері жөніндегі зерттеуінде әртүрлі бағалаулар бойынша орын алған жайтты анықтаудың орташа уақыты 100 күнді құрайтынын атап өтті. Бұл шабуылдаушыны ақпараттық-коммуникациялық инфрақұрылымға және одан кейінгі іс-қимылдарға бекіту үшін жеткілікті болып табылады. Ақпараттық қауіпсіздікті қамтамасыз ететін мамандар әрдайым ақпараттық қауіпсіздік қатерлері мен орын алған жағдайларға практикалық жауап беру дағдыларына ие бола бермейді және көп жағдайда оқиға анықталғаннан кейін қабылданатын шаралар жөнінде жалпы түсінікке ие болады. Киберполигонның құрылуы мен жұмыс істеуін ұсынады [13].

Зерттеу әдістері

Магистрлік жобада жүйелеу, синтездеу, жалпылау, регрессиялық, сандық, салыстырмалы және статистикалық талдау секілді ғылыми танымның жалпы ғылыми әдістері қолданылды.

Әдебиеттерге шолу бөлімінде ақпараттық қауіпсіздік бойынша қолданыстағы әдебиеттерге жан-жақты шолу жасады. Шолу ақпараттық қауіпсіздікке байланысты мәселелерді қарастыратын тиісті академиялық журналдарды, кітаптарды және басқа жарияланған материалдарды анықтауды қамтиды.

Зерттеу барысында жеке деректердің таралып кету жағдайын анықтау мақсатында эксперимент әзірленді және жүргізілді.

Сандық талдауда деректердің заңдылықтары мен тенденцияларын зерделеу үшін соңғы 10 жылдағы ақпараттық қауіпсіздік жағдайларының, эксперименттердің және зерттеудің өзге де сандық әдістерінің статистикасы қолданылды.

Қолда бар мәліметтер негізінде сызықтық регрессияны қолдана отырып, алдағы 3-5 жылға болжам жасалды. Сондай-ақ ақпараттық қауіпсіздікті және ақпараттық қауіпсіздік инциденттерін қамтамасыз ету үшін жұмсалған қаражатқа корреляция жүргізілді.

Интернет желісін пайдаланушылар санына, ақпараттық қауіпсіздік жағдайларына және халықтың цифрлық сауаттылығына корреляциялық талдау жасалды.

Жалпылау және синтездеу әдістері экономиканы цифрландыру шеңберінде ақпараттық қауіпсіздікті қамтамасыз етудің шетелдік тәжірибесін жүргізу кезінде қолданылды.

Жүйелік әдіс басқа да теориялық және әдіснамалық тәсілдермен қатар осы магистрлік жобаны зерттеу нәтижелері бойынша қорытынды жасау кезінде қолданылды.

Талдау және зерттеу нәтижелері

Еліміздің экономикасын цифрландыру соңғы жылдары мемлекеттік саясаттың приоритеттегі бағыттарының бірі болып есептеледі. Оның мақсаты заманауи цифрлық технологиялар мен инновациялық шешімдерді енгізу арқылы елдің бәсекеге қабілеттілігін жақсарта түсу және халықтың өмір сүру деңгейін арттыру болып табылады.

2017 жылы «Цифрлық Қазақстан» мемлекеттік бағдарламасы бекітілді, ол өз алдына елімізде цифрлық экономиканы дамыту үшін жайлы ортаны құру міндетін қояды [14]. Бағдарламаның негізгі бағыттары келесілерді қамтиды:

– Цифрлық инфрақұрылымды дамыту. Бағдарлама аясында цифрлық орталықтар желісін құру, кең жолақты Интернетке қолжетімділікті кеңейту және байланыс сапасын жақсарту жоспарланды;

– Бизнесте цифрлық технологияларды ілгерілету. Бағдарлама цифрлық технологиялар саласындағы кәсіпкерлікті қолдауды, оның ішінде инкубаторлар мен акселераторларды құруды, стартаптарды қаржыландыруды және цифрлық экономиканы дамыту үшін іс-шаралар өткізуді көздеді;

– Электрондық үкіметті дамыту. «Цифрлық Қазақстан» бағдарламасы электрондық мемлекеттік қызметтерді енгізуді, азаматтар мен мемлекеттік органдар арасындағы қарым-қатынас сапасын жақсартуды, сондай-ақ бюрократиялық рәсімдерді қысқартуды көздеді;

– Цифрлық мәдениетті дамыту. Бағдарлама шеңберінде халықтың цифрлық сауаттылығын арттыруға, сондай-ақ білім беруде цифрлық технологияларды дамытуға бағдарланған шаралар кешенін ұйымдастыру жоспарланды;

– Цифрлық денсаулық сақтауды дамыту. «Цифрлық Қазақстан» бағдарламасы электрондық медициналық карта жасауды және телемедицинаны енгізуді қоса алғанда, денсаулық сақтауға цифрлық технологияларды енгізуді де көздейді.

Қазақстанды цифрландырудың даму жолын бірнеше кезеңге бөлуге болады. 1990 жылдар – цифрландырудың басталған уақыты. Осы кезеңде Қазақстанда алғашқы компьютерлік желілер мен Интернет-қоғамдастық дами бастады. 1994 жылы Алматыда алғашқы қазақстандық «Kaznet» компьютерлік желісі құрылды. Осы кезеңде алғашқы қазақстандық Интернет-ресурстар, оның ішінде «Kazakhstan Online» және «Zamana» порталдары құрылды. 2000 жылдар – цифрлық инфрақұрылымды дамыту. Осы кезеңде «Электрондық Қазақстан» мемлекеттік бағдарламасы құрылды, ол елдегі цифрлық инфрақұрылымды дамыту үшін негіз болды. Мемлекеттік портал, «egov.kz» электрондық үкімет құрылды. 2010 жылдар – цифрлық экономиканың дамуы. Осы кезеңде Қазақстан цифрлық экономиканы, оның ішінде өмірдің түрлі салаларында жаңа технологияларды енгізуді белсенді дамыта бастады. «Цифрлық Қазақстан» мемлекеттік бағдарламасы іске қосылды, ол өз алдына цифрлық экономика құру және инновациялық технологияларды дамыту міндетін қояды. 2010 жылдар – цифрлық экономиканың дамуы. Осы кезеңде Қазақстан цифрлық экономиканы,

оның ішінде өмірдің түрлі салаларында жаңа технологияларды енгізуді белсенді дамыта бастады. «Цифрлық Қазақстан» мемлекеттік бағдарламасы іске қосылды, ол өз алдына цифрлық экономиканы құру және инновациялық технологияларды дамыту міндетін қояды.

2020 жылдар ақпараттық қауіпсіздікті нығайту. Бұл кезеңде киберқауіптер мен осалдықтардың көбеюіне байланысты ақпараттық қауіпсіздікке назар күшейе түсті. Елде АҚҰҰО құрылды, сонымен қатар киберқауіпсіздік саласындағы бірқатар заңдар мен нормативтік құжаттар қабылданды.

Бүгінгі күні Қазақстан өзінің цифрлық экономикасын дамытуды жалғастыруда және медицина, білім беру, мемлекеттік басқару, көлік және т.б. сияқты өмірдің әртүрлі салаларында жаңа технологияларды белсенді енгізе түсуде [15].

2017 жылғы 12 желтоқсанда бекітілген «Цифрлық Қазақстан» мемлекеттік бағдарламасында ақпараттық-коммуникациялық технологиялар аясында ақпараттық қамсыздандыруды қамтамасыз ету осы бағдарламаның негізгі бағыттарының бірі болып табылады [14]. Сондай-ақ Мемлекет Басшысының 2017 жылғы 31 қаңтардағы «Қазақстанның Үшінші жаңғыруы: жаһандық бәсекеге қабілеттілік» атты Қазақстан халқына Жолдауын іске асыру жөніндегі шаралар туралы» Қазақстан Республикасы Президентінің 2017 жылғы 15 ақпандағы № 422 Жарлығын іске асыру мақсатында Қазақстан Республикасының Үкіметі Киберқауіпсіздік тұжырымдамасын («Қазақстанның киберқалқанын») бекітті [16].

Ақпараттық-коммуникациялық технологиялардың дамуы «Төртінші өнеркәсіптік революция» (Индустрия 4.0) дәуірімен тығыз байланысты. Оған толық автоматтандырылған өндірістер тән. Бұл өндірістер барлық процестерді нақты уақыт режимінде және өзгеретін сыртқы жағдайларды ескере отырып басқарады. «Индустрия 4.0» негізгі технологиялары келесі технологиялардың болып табылатындығы сөзсіз:

- бұлтты есептеулер;
- үлкен деректер;
- робототехника, жасанды интеллект және машиналық оқыту;
− киберқауіпсіздік;
- виртуалды және кеңейтілген шындық;
- заттар Интернеті;
- кванттық есептеу.

Жоғарыда аталған бағыттар елдерді «Индустрия 4.0» дәуіріне көшуге алып келеді және өндіріс тиімділігінің жаңа деңгейін қамтамасыз етеді.

Қазіргі уақытта киберқауіпсіздік мәселесі ұлттық деңгейдегі саясаткерлердің назарын талап етеді. Көптеген елдер электрондық үкімет арқылы өз қызметтерін көрсете отырып, цифрлық технологияларды [17] енгізеді және ілгерілетеді. Бұл болып жатқан өзгерістер саясаткерлерді киберкеңістікте қауіпсіздікті қамтамасыз ету мәселелері жөнінде ойлануға және шешім қабылдауға мәжбүр етеді. Инновациялық АКТ-ны кеңінен қолдану цифрлық деректердің кибершабуылдарға осалдығы қаупін арттырады. Киберқауіпсіздікті

қамтамасыз ету елдің ұлттық және экономикалық қауіпсіздігіне әсер ететін мемлекеттік басқарудағы приоритеттегі бағыттарының бірі болып есептеледі. Осы кезеңде Қазақстан, көптеген басқа да мемлекеттер секілді, электрондық үкімет порталы арқылы дәстүрлі мемлекеттік қызметтерді цифрлық қызметтерге ауыстыра отырып, цифрлық трансформация кезеңін бастан өткеруде.

Бұл бөлімде Қазақстанның ресми нормативтік-құқықтық және басқару құжаттарына сәйкес ақпараттық қауіпсіздікті қамтамасыз етудің қолданыстағы тетігіне талдау жүргізілді. Бұл талдау Цифрлық Қазақстан мемлекеттік бағдарламасының призмасы арқылы жүргізілгенін атап өту қажет, өйткені цифрландырусыз цифрлық технологияларды қамтамасыз ету мәселелері өзекті болмайды. Бүгінгі таңда цифрлық технологиялар мемлекеттік қызметтер көрсету мақсатында мемлекеттік органдар тарапынан ғана емес, сондай-ақ жеке сектор тарапынан да қарқынды қолданылады. Күн сайын цифрландыру саласында жаңа технологияларды енгізу үдемелі қарқынмен дамып келеді және бұл болып жатқан құбылысты елемеу мүмкін емес. Бүгінгі таңда цифрландыру бизнес пен қоғамның барлық аспектілерін қамтуда. АКТ-ны енгізу және қолдану миллиондаған адамдардың өмірінің ажырамас бөлігіне айналды.

Технологиялар білім беру, денсаулық сақтау, қаржы, сауда және қоғам өмірінің өзге де салаларындағы жаңа цифрлық қызметтердің негізінде өмір сүру жағдайларын жақсартты. Жаһандану кезеңінде көптеген елдер цифрлық технологияларды белсенді енгізе түседі. Қазақстан да жаһандану ағымында инновациялық технологияларды қолданып келеді. Көрсеткіш ретінде 2017 жылдың соңында қабылданған, 2018-2022 жылдары іске асырылатын «Цифрлық Қазақстан» мемлекеттік бағдарламасын [14] және «Цифрландыру, ғылым және инновациялар есебінен технологиялық серпіліс» ұлттық жобасын [18] атауымызға болады.

«ЦҚ» МБ негізгі мақсаты «цифрлық экожүйені прогрессивті дамыту арқылы халықтың өмір сүру сапасын және ел экономикасының бәсекеге қабілеттілігін арттыру» болып табылады [14]. «ЦҚ» МБ-да 17 міндет белгіленген, олардың бірі АКТ саласындағы АҚ-ны қамтамасыз ету, сондай-ақ жоғары оқу орындарында мамандар даярлау, сондай-ақ қайта даярлау және біліктілігін арттыру арқылы халықтың цифрлық сауаттылығын арттыру болып табылады [14]. Белгіленген 17 міндетке қол жеткізу мақсатында республика Үкіметі ақпараттық-коммуникациялық қызметтерді қолдана отырып, мемлекеттік қызметтер көрсетуді жақсартуға бағытталған бірқатар жұмыстар жүргізді. Сонымен қатар Қазақстанның мақсаты 2022 жылға қарай халықтың цифрлық сауаттылық деңгейін 83%-ға арттыру болып табылады. Ақпарат ретінде келтірер болсақ, бұл көрсеткішке 2020 жылы қол жеткізілді [19]. Өз зерттеулерінде П. Клименко мен И. Клименко «ЦҚ» МБ-ны іске асыру цифрлық экономикаға көшу шеңберінде дамыған елдермен ашық ынтымақтастыққа Қазақстанның маңызды және тиімді шешімі болып табылатынын атап өтті [20]. Қазақстан цифрландыру саласында дұрыс бағытта келе жатқанын атап өтуге болады. Сонымен қатар цифрлық технологияларды енгізу идеясын Р. Мұсабаев, Б. Қасымжанов, Г. Қалиева және В. Ибраева [21] зерттеулері қолдай түседі.

Жоғарыда аталған зерттеушілердің пікірінше, цифрлық технологияларды қолдану мемлекеттің жергілікті тұрғындармен өзара байланысы, қарым-қатынасы жақсарта түседі.

Қазақстандағы ақпараттық қауіпсіздіктің жағдайы

Қазіргі цифрлық әлемде киберқылмыс әлемдік экономиканың өсуіне негізгі қауіп-қатер болып табылады. Интернеттегі азаматтардың мінез-құлық мәдениетін арттыру, ақпараттық қауіпсіздік, сондай-ақ киберқылмыспен күресудің жалпы әлемдік ережелерін тарату мұндай қылмыстармен күресуге көмектеседі. Ақпараттық қауіпсіздік, сондай-ақ Интернеттің маңызды инфрақұрылымын басқару мәселелері «Үлкен жиырмалықтың» кездесулерінде, БҰҰ алаңында, көптеген елдердің телекоммуникация және ақпараттық технологиялар министрлерінің кездесулерінде үнемі талқыланады.

Әр жыл сайын БҰҰ Халықаралық электр байланысы одағының (International Telecommunication Union) эксперттері «Жаһандық киберқауіпсіздік индексі» (Global cybersecurity Index) тақырыбында киберқауіпсіздік деңгейі бойынша мемлекеттердің рейтингісін әзірлейді. Сәйкесінше баяндамада ITU мамандары әлемнің барлық мемлекеттерінің компьютерлік қауіпсіздігін бес өлшем бойынша бағалайды: құқықтық, техникалық, ұйымдастырушылық дайындық, ынтымақтастыққа дайындық, елдің білім беру және зерттеу потенциалын дамыту. Зерттеудің ең өзекті нұсқасы 2020 жылы шығарылды.

Біздің еліміз киберқауіпсіздік деңгейі бойынша елдер рейтингінде 194 елдің ішінде 38-ші орынды иеленуде. Бұл өте жақсы нәтиже. Рейтингті құрастыру кезінде сарапшылар бес негізгі критерийді назарға алды: киберқауіпсіздік және киберқылмыс мәселелерімен айналысатын құқықтық жүйелер мен құрылымдардың болуы; киберқауіпсіздік саласындағы техникалық мүмкіндіктер; мемлекеттік деңгейде киберқауіпсіздікті дамыту саясаты мен стратегияларын үйлестіру институттарының болуы; ақпараттық қауіпсіздік саласындағы әлеуетті күшейтуге ықпал ететін ғылыми-зерттеу, білім беру және дайындық бағдарламаларының, сондай-ақ сертификатталған мамандар мен мемлекеттік мекемелердің болуы; серіктестіктердің, ынтымақтастық тетіктерінің және ақпарат алмасу жүйелерінің болуы. Халықаралық индекстер бөлігінде **рейтингтік жеңістерге** негізінен заңнамалық базаны стандарттарға сәйкестендіру есебінен қол жеткізілді. Практикалық жоспарда әлде де бірқатар шешілмеген мәселелер сақталуда.

Нәтижесінде киберқауіпсіздік тұрғысынан ең дамыған елдердің ондығына көшбасшы елдермен қатар Малайзия, Оман, Эстония, Маврикий, Австралия, Грузия, Франция және Канада кірді. Ресей Жапония, Норвегия және Ұлыбританиядан озып, он бірінші орынға ие болды, олар одан әрі үш позицияға орналасты. Үндістан 25-ші орында, Германиядан бір позиция жоғары, ал Қытай тізім бойынша 34-ші орынды иеленді [22].

Бүгінгі таңда Қазақстанда 40-қа жуық компания, сондай-ақ 19 жеке қауіпсіздік операциялық орталығы (SOC), компьютерлік инциденттерге ден

қоюдың 3 тобы (CERT), 7 жеке аккредиттелген сынақ зертханасы, 8 жоғары оқу орны және киберқауіпсіздік мәселелерімен айналысатын 25 орта оқу орны бар.

Бізде 85 дәлелденген бағдарламалық жасақтама мен электронды өнім жеткізушілері, сондай-ақ ұлттық үйлестіру орталығы және қаржы секторы үшін арнайы ақпараттық қауіпсіздік орталығы бар [19].

Тәжірибе көрсеткендей, ақпараттық жүйелердің өте төмен көрсеткіші ақпараттық қауіпсіздік талаптарына сәйкестігін тексеруді сұрау болып табылады. Өз есебінде Қазақстан Республикасының жоғары аудиторлық палатасы 97 ақпараттық жүйенің, 43 жүйенің ақпараттық қауіпсіздік талаптарына сәйкес келуі бойынша апробациядан өтпегенін атап өтті. Бұл мердігерлер жұмыстардың сапасыз орындалғанын және мемлекеттік органдардың қызметкерлері тиісті бақылауды қамтамасыз етпегенін көрсетеді [23].

Ақпараттық қауіпсіздікті қамсыздандыру проблемаларымен айналысатын Қазақстан Республикасының мемлекеттік органдары:

Қазақстан Республикасы Ұлттық қауіпсіздік комитеті;

ҚР ІІМ Криминалдық полиция департаментінің киберқылмысқа қарсы күрес орталығы;

ҚР ЦДИАӨМ ақпараттық қауіпсіздік комитеті;

ҚР СІМ Халықаралық қауіпсіздік департаменті.

Мемлекеттік органдардың міндеттері келесі кестеде көрсетілген (1-кесте).

1-кесте – Мемлекеттік органдардың міндеттері

№ р/с	Мемлекеттік органдар	Міндеттер
1	Қазақстан Республикасы Ұлттық қауіпсіздік комитеті	Үкіметтік байланыс желілерінің, республикалық қорғалған байланыс желілерінің және ұлттық қауіпсіздік органдарының қорғалған байланыс желілерінің ақпараттық қауіпсіздігін қамтамасыз ету
2	ҚР ІІМ Криминалдық полиция департаментінің Киберқылмысқа қарсы күрес орталығы	Тыйым салынған контентті анықтау және қылмысқа қарсы іс-қимыл мақсатында ақпараттық-телекоммуникациялық желілердегі деректерді талдау; Киберқылмыстарды тергеу.
3	ҚР ЦДИАӨМ ақпараттық қауіпсіздік комитеті	1) ақпараттандыру, дербес деректер және оларды қорғау салаларындағы ақпараттық қауіпсіздік саласындағы мемлекеттік саясатты, сондай-ақ электрондық құжат және электрондық цифрлық қолтаңба туралы Қазақстан Республикасының заңнамасын және электрондық цифрлық қолтаңбаны сақтау тұрғысынан электрондық құжат пен электрондық цифрлық қолтаңбаны жүзеге асыру; 2) мемлекеттік органдардың, жеке және заңды тұлғалардың ақпараттық қауіпсіздігін қамтамасыз етуді мониторингілеу;

1– кесте– жалғасы

		3) ақпараттық қауіпсіздік инциденттерінің, оның ішінде әлеуметтік, табиғи және техногендік сипаттағы төтенше жағдайлар, төтенше немесе соғыс жағдайы енгізілген жағдайларда алдын алу және оларға жедел ден қою; 4) өз құзыреті шеңберінде еліміздің нормативтік құқықтық базасының сақталуын бақылауды қамтамасыз ету; 5) өз құзыреті шеңберінде Комитетке тапсырылған басқа да міндеттерді іске асыру.
4	ҚР СІМ Халықаралық қауіпсіздік департаменті	Халықаралық ақпараттық қауіпсіздік саласындағы халықаралық ұйымдармен ынтымақтастықты дамытудың неғұрлым перспективалы және басым бағыттарын айқындау жөнінде басшылыққа ұсыныстар енгізу.
Ескертпе – автормен әзірленген		

Аталған мемлекеттік органдар біздің елімізде ақпараттық қауіпсіздікті қамтамасыз етумен айналысады. Қазақстан цифрлық кеңістікті белсенді қарқынмен меңгеруде. 2017 жылы «Цифрлық Қазақстан» мемлекеттік бағдарламасы бекітілді [14], сол жылы Қазақстан киберқауіпсіздік Тұжырымдамасын («Қазақстанның киберқалқаны») бекітті [16].

«Цифрлық Қазақстан» мемлекеттік бағдарламасы шеңберінде ақпараттық қауіпсіздікті қамтамасыз ету бойынша іс-шаралар кешені келесі кестеде берілген (2-кесте).

2-кесте – Ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі іс-шаралар кешені

Іс-шара	**Атауы**	**Өлшем бірлігі**	**Барлығы**	**Қаржыландыру көзі**	**Бюджеттік бағдарламаның коды және атауы**
78	Үлкен деректерді талдау үшін технологиялық орталық құру			ХҚИ	
79	Зиянды кодты зерделеу лабораториясын жабдықтау	мың теңге	44 221	РБ	001 «Ұлттық қауіпсіздікті қамтамасыз ету»
80	Ақпараттық қауіпсіздік құралдарын зерделеу зертханасын жарақтандыру	мың теңге	1 037 363	РБ	001 «Ұлттық қауіпсіздікті қамтамасыз ету»

2–кесте–жалғасы

81	Ақпараттық қауіпсіздік саласындағы сынақ зертханасын жарақтандыру	мың теңге	184 473	РБ	001 «Ұлттық қауіпсіздікті қамтамасыз ету»
82	АҚ-ны қамтамасыз ету, Интернеттің қазақстандық сегментінің «электрондық үкімет» ақпараттандыру объектілерін, сондай-ақ ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілерін қорғау және қауіпсіз жұмыс істеуін мониторингілеу, еліміздің нормативтік құқықтық заңнамасында белгіленген тәртіппен АҚ-ны қамтамасыз ету жөніндегі ортақ шаралар кешенін іске асыра отырып, АҚ инциденттеріне назар аудару мәселелері бойынша сала арасындағы үйлестіруді іске асыру	мың теңге	3 472 670	РБ	001 «Ұлттық қауіпсіздікті қамтамасыз ету»
83	АҚҰҰО-ны құру	мың теңге	28 923 243	РБ	001 «Ұлттық қауіпсіздікті қамтамасыз ету»
84	Ақпараттық қауіпсіздік жөніндегі ұлттық стандарттарды әзірлеу және қабылдау	мың теңге	159 101	РБ	061 «Техникалық реттеу және метрология саласындағы қызметтер»
Ескертпе – автормен әзірленген					

Ақпараттық қауіпсіздікті қамтамасыз ету барысында Қазақстан бірқатар проблемаларға кезікті, олардың ішінде келесі мәселелерге ерекше тоқталып өтуге болады:

– қаржыландыру жеткіліксіз. Іске асыру айтарлықтай қаржылық шығындарды талап етеді, бірақ бұл мақсатқа бюджеттік қаражат жеткіліксіз болуы мүмкін, бұл барлық қажетті шараларды жүзеге асыруды қиындатады;

– кадрлардың біліктілігі жеткіліксіз. Қазақстан киберқауіпсіздік саласында кадрлық базаны дамыта бастағанына қарамастан, жоғары білікті мамандардың тапшылығы әлі де бар. Бұл киберқауіпсіздікке жауапты қызметкерлердің кәсіби дайындығының жеткіліксіздігіне әкелуі мүмкін. Саланың алдын-ала бағалауы бойынша 10 мыңға жуық маман қажет, қазірде 2 мың ғана маман бар.

– заманауи технологиялардың болмауы. Киберқауіпсіздікке заманауи технологияларды енгізу бойынша белсенді жұмыс жүргізгеніне қарамастан, Қазақстан өзінің киберинфрақұрылымын барлық қауіп-қатерлерден толық қорғауға әлі мүмкіндігі жоқ. Мемлекеттік органдарда ақпаратты қорғау құралдарын орнату үшін ақпараттық-коммуникациялық инфрақұрылым ең төменгі жүйелік талаптарды қанағаттандырмады;

– ведомстволар арасындағы үйлестіру жеткіліксіз. Әртүрлі ведомстволар мен ұйымдар ақпаратты қорғаудың әртүрлі жүйелері мен тәсілдерін қолдана алады. Бұл әртүрлі құрылымдар арасындағы үйлестіру мен өзара әрекеттесуді қиындатады, бұл киберинфрақұрылымның осалдығын арттыруы мүмкін;

– киберқауіптер туралы ақпараттың жетіспеушілігі. Киберқауіптер және олардың әдістері туралы толық ақпараттың болмауы киберинфрақұрылымның әлсіз қорғалуына әкелуі мүмкін. Ақпараттың жетіспеушілігі киберқауіптерге қарсы тиісті шараларды әзірлеуді қиындатады;

– азаматтардың киберқауіпсіздік қатерлері туралы хабардар болмауы [24].

Қазақстан Республикасында ақпараттық қауіпсіздікті қамсыздандыруға арналған жалпы шығындар келесі суретте көрсетілген (1-сурет).

1-сурет – 10 жылда ақпараттық қауіпсіздікке кеткен шығындар

Ескертпе – автормен әзірленген

Бұл IT саласына жұмсалатын шығындардың жалпы құрылымындағы ақпараттық қауіпсіздікті қамтамасыз ету шығындарының үлесі. Біздің елімізде бұл шамамен 1%-ыд құрайды, әлемде бұл пайыз шамамен 10%-ды құрайды.

Қазақстан Республикасының «Электрондық үкіметі»

Үкіметтің тапсырмасы бойынша «Зерде» Ұлттық инфокоммуникациялық холдингі» АҚ «Ұлттық ақпараттық технологиялар» АҚ-мен бірлесіп Қазақстанның ақпараттық құрылымдарына, атап айтқанда «Электрондық үкіметке» кең көлемді зерттеу жүргізді.

Қазақстан Республикасының ЦДИАӨМ министрі Бағдат Мусин атап өткендей, 32 дерекқорда адамдардың тұрғылықты мекенжайы сақталады – бұл ретте бұл деректердің барлығы әр жолы бастапқы енгізілді. Осылайша, деректердің қайталануы бар бірнеше ақпараттық жүйе бірден анықталды. Деректерді әртүрлі көздерде сақтау ақпараттық қауіпсіздікке қауіп төндіреді.

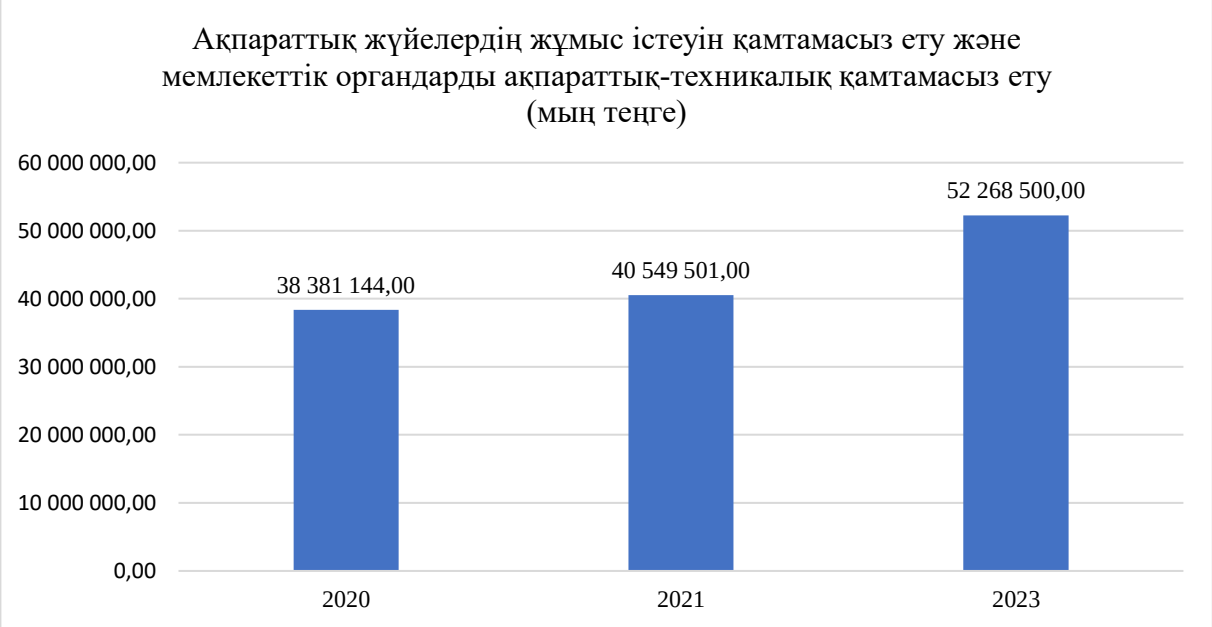
Зерттеу қорытындысы бойынша елімізде 572 ақпараттық жүйе бар, оның 100-ден астамы ведомстволық бағынысты ұйымдардың қатарында қалыптасты. Тағы 100-ге жуық АЖ жасырылған, болашақта бұл анықталатын болады.

Сондай-ақ ақпараттық ресурстарды тиімсіз кәдеге жарату байқалады, онда бір жүйеге жедел жадтың белгілі бір мөлшері, процессор қуаты сақталады, нәтижесінде ол әрдайым қолданыла бермейді.

Талдау көрсеткендей, 178 ақпараттық жүйені, оның ішінде орталық мемлекеттік органдардың ақпараттық жүйелерін есептен шығаруға болады. Себептері: функционалдың басқа АЖ-ға көшуі, деректердің моральдық ескіруі,

қызметтердің қайталануы және басқа ұйымдарға берілуі. [25].

ҚР ЦДИАӨМ-нің осы есептеріне сәйкес, Қазақстан Үкіметі жыл сайын мемлекеттік органдар мен ұйымдар пайдаланатын ведомствоаралық ақпараттық жүйелердің қалыпты қызмет етуін қамсыздандыруға шамамен 53 миллиард теңге жұмсайды. Айта кететін жайт, бұл сома **жүйелердің дамуын емес,** олардың жұмыс істеуін қамтамасыз етуге ғана қатысты.



2-сурет – АЖ-ны сүйемелдеуге арналған шығындар

Ақпараттық қауіпсіздік инциденттері

Ұлттық компьютерлік инциденттерге назар аудару қызметі ақпараттық қауіпсіздік инциденттері бойынша статистика жүргізеді. 2022 жылдың қорытындысы бойынша ақпараттық қауіпсіздік оқиғалары 2011 жылмен салыстырғанда 4578,8 есеге өсті. Мұның бірқатар объективті себептері бар. Мысалы, Интернет желісін, дербес компьютерлерді, гаджеттерді, есептеу техникасы құралдарын, смартфондарды және т.б. пайдаланушыларды ұлғайту. Ақпараттық қауіпсіздік инциденттерінің статистикасы келесі кестеде берілген (3-кесте) [26].

3-кесте – Ақпараттық қауіпсіздік инциденттерінің статистикасы

Ақпараттық қауіпсіздік оқиғаларының статистикасы	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**	**2021**	**2022**
Ботнеттер	0	325	11295	14209	17150	18959	22899	17724	17300	12670	4304	2194

АР-ға қолжетімділіктің болмауы	0	0	0	0	0	0	1065	797	1075	2937	1959	1258
Компьютерлік вирустар, желілік құрттар, трояндар	1	104	569	295	120	114	360	313	409	2500	11923	10869
Қызмет көрсетуден бас тарту (DoS/DDoS-атака)	0	7	5	19	21	10	43	42	201	290	264	218
Рұқсатсыз қол жеткізу және мазмұнды өзгерту	1	253	253	563	503	1336	915	1082	258	293	272	407
Интернет желісіндегі фишинг	1	94	244	348	195	128	106	199	883	1392	658	1242
Қалған оқиғалар	1	31	77	361	386	1593	1429	292	682	3971	4393	2127

Ескертпе – кесте автормен 26 дереккөз деректері негізінде құрастырылды

2011 жылдан 2016 жылға дейінгі кезең ішінде инциденттер саны айтарлықтай тұрақты болды және жылына 20 мың жағдайдан аспады. 2017 жылы ботнеттермен байланысты инциденттердің айтарлықтай өсуі байқалды, бұл 23 мыңға жуық жағдайға жетті. 2018-2019 жылдары инциденттер саны азайды, бірақ әлі де жоғары деңгейде қалды, жылына шамамен 17 мың жағдайды құрады. 2020 жылдан бастап инциденттер саны айтарлықтай төмендеп, 2022 жылы тек 2 мың ботнетті құрады. 2011 жылдан 2016 жылға дейін Интернет-ресурстарға қолжетімділіктің жоқтығы тіркелмеді. 2017 жылы қолжетімділіктің мыңнан астам жағдайы тіркелген кезде күрт өсу байқалды. 2018 жылдан 2022 жылға дейін инциденттер саны айтарлықтай жоғары деңгейде қалды және жылына 800-ден 2900-ге дейін болды. Вирустар мен трояндарға қатысты инциденттер саны бүкіл кезеңде жеткілікті жоғары болды. Алайда 2011 жылы тек бір жағдай тіркелді, ал 2012 жылы 104 жағдай тіркелді. 2013 жылдан 2016 жылға дейін инциденттер саны өте жоғары болды, бірақ 2012 жылмен салыстырғанда аз. 2017-2018 жылдары ақпараттық ресурстарға қолжетімділіктің болмауына байланысты инциденттер саны азайды, бірақ 2019 жылы қайтадан өсе бастады. 2020 жылы 2500-ге жуық жағдайға жеткен инциденттердің күрт өсуі байқалды, ал 2021 жылы 11923 жағдайға дейін одан да үлкен өсім болды.

Dos/DDoS шабуылдарымен байланысты инциденттер саны бүкіл кезеңде салыстырмалы түрде төмен болды. Алайда 2011 жылы бір DOS шабуылы тіркелді, ал 2012 жылы 7 жағдай тіркелді. 2013 жылдан 2016 жылға дейін

инциденттер саны өте төмен деңгейде болды. Алайда 2017 жылы 40-тан астам жағдай тіркелген кезде күрт өсім болды. 2018 жылдан бастап инциденттер саны көбейе бастады және 2020 жылы 290 жағдайдың шыңына жетті. 2021 және 2022 жылдары инциденттер саны азайды, бірақ әлі де жоғары деңгейде қалды, жылына шамамен 200 жағдайды құрады. Рұқсат етілмеген қолжетімділікке және мазмұнды өзгертуге байланысты инциденттер саны бүкіл кезең ішінде өте жоғары деңгейде болды. 2011 жылы бір жағдай, ал 2012 жылы 253 жағдай тіркелді. 2013 жылдан 2016 жылға дейін инциденттер саны өте жоғары болды, әсіресе 2016 жылы 1300-ден астам жағдай тіркелді. 2017-2019 жылдары инциденттер саны азайды, бірақ 2020 жылы қайтадан өсе бастады. 2021 жылы инциденттердің саны 2020 жылмен бірдей болды, бірақ 2022 жылы 407 жағдайға дейін күрт өсті.

Интернеттегі фишинг жағдайлары 2011-2014 жылдар аралығында көбейіп, 2014 жылы 348-ден астам жағдай тіркелген шыңына жетті. 2015 жылдан 2017 жылға дейін жағдайлардың саны азайды, бірақ 2018 жылдан бастап жаңа өсім басталды және 2019 жылы 800-ден астам жағдай тіркелді. 2020 жылы оқиғалар саны 1392-ге дейін өскен инциденттер санының күрт өсуі байқалды. Бұл COVID-19 пандемиясына байланысты пайдаланушылардың онлайн белсенділігінің артуына байланысты болуы мүмкін. 2021 жылы жағдайлардың саны азайды, бірақ әлі де 650 жағдайдан жоғары деңгейде қалды.

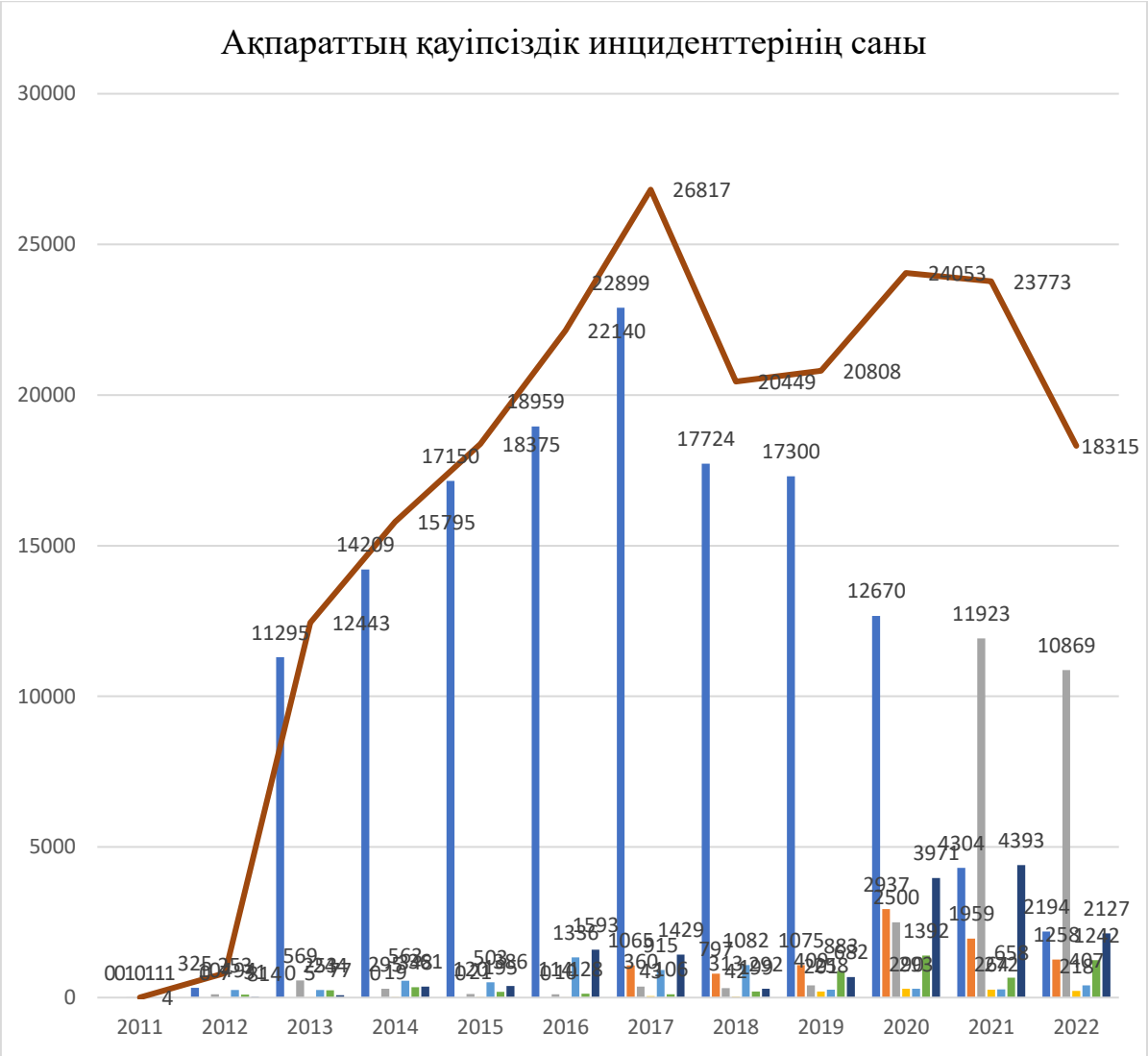
2011-2022 жылдар аралығындағы ботнеттермен, АР-ға қолжетімділіктің жоқтығымен, компьютерлік вирустармен, фишингпен және DoS/DDoS-шабуылдармен байланысты емес ақпараттық қауіпсіздік инциденттерінің статистикасын талдау келесі нәтижелерді көрсетеді:

Басқа санаттарға жатпайтын ақпараттық қауіпсіздік инциденттерінің саны 2013 жылдан 2014 жылға дейін айтарлықтай өсті, 2014 жылы 361-ден астам инцидент тіркелген көрсеткішке жетті. 2015 жылдан 2017 жылға дейін инциденттер саны азайды, бірақ 2018 жылдан бастап жаңа өсім басталды. 2019 жылы 680-ден астам жағдай тіркелді, ал 2020 жылы олардың саны 3971-ге дейін өсті. 2021 жылы басқа санаттарға жатпайтын инциденттер саны 4300 жағдайдан асып, көбейе берді.

Болжам бойынша, жағдайлардың көбеюі шабуылдаушылардың ақпараттық қауіпсіздік оқиғаларының басқа санаттарымен байланысты емес шабуылдар мен осалдықтардың жаңа әдістерін қолдануына байланысты.

Алайда, «қалған инциденттер» санаты өте кең және инциденттердің нақты түрлері туралы толыққанды ақпаратты қамтымайтынын атап өткен жөн, сондықтан қосымша ақпаратсыз толыққанды талдау жасау қиын.

Көрнекі түрде келесі картинаны көруге болады (3-сурет).



3-сурет – Ақпараттық қауіпсіздік инциденттерінің саны

Ескертпе – график автормен жасалған

Статистика көрсеткендей, ақпараттық қауіпсіздік оқиғасы тек өсуде. y = ax+b сызықтық регрессия формуласын қолдана отырып, ол алдағы 5 жылға болжам жасалды:

1) A коэффициенті Yср.-bXср. ретінде есептеледі (Yср. және Xср. – сәйкесінше белгілі y және x мәндерінің үлгілерінен алынған сандардың арифметикалық орташа мәні).

2) B коэффициенті формула бойынша анықталады:

$$b = \frac{\sum(x - Xср.)(y - Yср.)}{\sum(x - Xср.)^2}$$

Есептеулер келесі нәтижелерді көрсетті: ақпараттық қауіпсіздікті бұзу жағдайлары саны: 2023 жылы – 28921, 2024 жылы – 30757, 2025 жылы – 32594, 2026 жылы – 34430, 2027 жылы – 36267. Картина келесідей болды (4-сурет).

4-сурет – Ақпараттық қауіпсіздік инциденттерінің 5 жылдық болжамы
Ескерпе – автормен әзірленген

Сондай-ақ мемлекеттің ақпараттық қауіпсіздік шығындары мен ақпараттық қауіпсіздік инциденттерінің санына салыстырмалы талдау жасады. Мұндай картинаны келесі суреттен анық көруге болады (5-сурет).

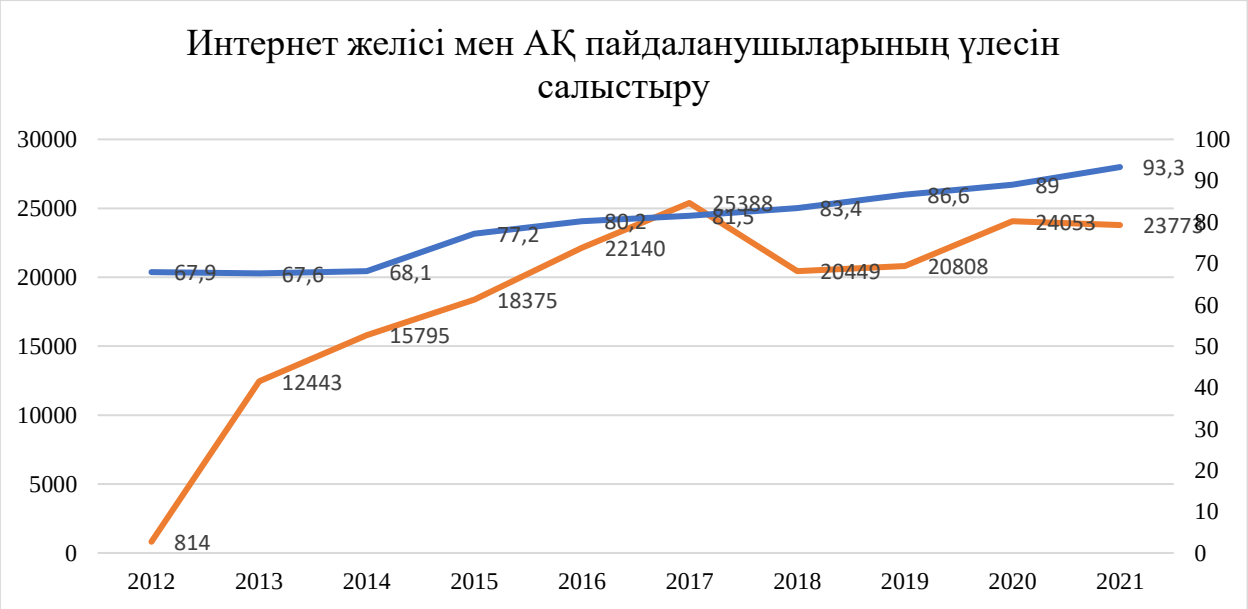
5-сурет – АҚ шығындарын салыстыруды талдау және АҚ инциденттерінің саны

Ескертпе – автормен әзірленген

Ақпараттық қауіпсіздік шығындары мен ақпараттық қауіпсіздік оқиғаларының корреляция коэффициенті (Pearson) 0,314546051-ге тең, бұл екі айнымалы арасындағы әлсіз оң корреляцияның бар екендігін көрсетеді. Бұл дегеніміз, ақпараттық қауіпсіздік шығындарының өсуі ақпараттық қауіпсіздік инциденттерінің көбеюімен бірге жүруі мүмкін, бірақ бұл айнымалылар арасындағы байланыс өте жоғары емес.

Алайда корреляция міндетті түрде айнымалылар арасындағы себеп-салдарлық байланысты көрсетпейтінін есте сақтаған жөн. Мысалы, ақпараттық қауіпсіздік инциденттерінің көбеюі ақпараттық қауіпсіздік шығындарының артуына әкелуі мүмкін, өйткені мемлекет тәуекелдің жоғарылауына байланысты осы салаға көбірек көңіл бөлуге мәжбүр.

Осы зерттеу барысында Интернет желісін пайдаланушылардың үлесіне және ақпараттық қауіпсіздік оқиғаларының санына корреляциялық талдау жасалды. Келесі нәтижені көруге болады (6-сурет).



6-сурет. Интернет пайдаланушыларының үлесін және АҚ инциденттерінің санын салыстыруды талдау

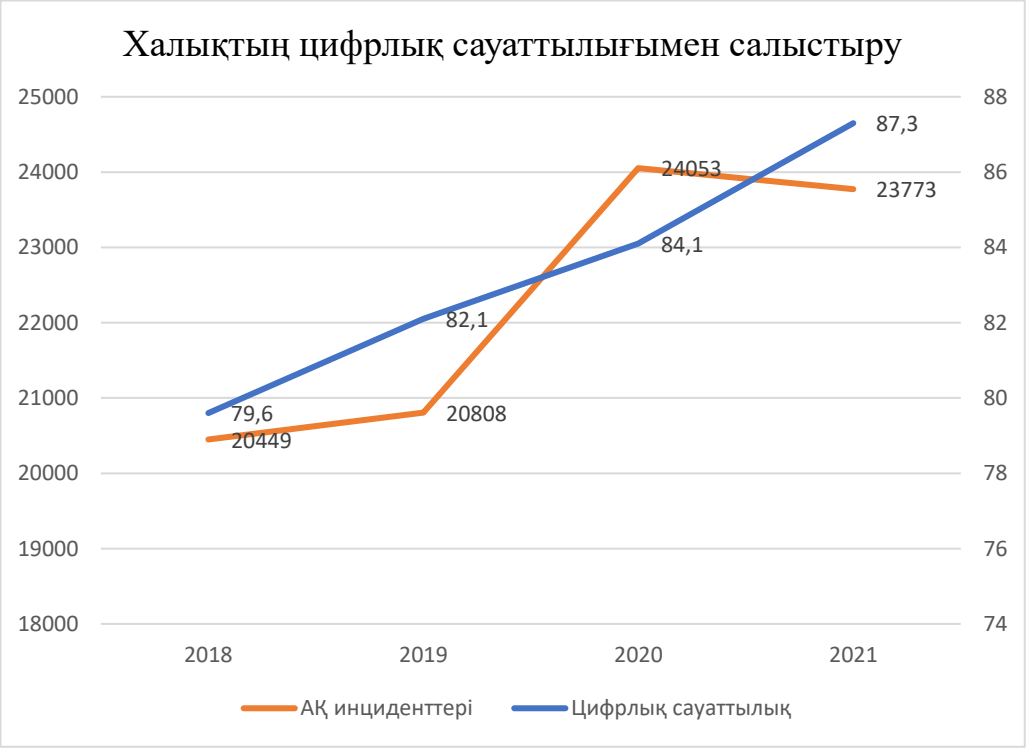
Ескертпе – автормен әзірленген

Біз талдаған деректер Ақпараттық қауіпсіздік инциденттерінің саны Интернет желісін пайдаланушылардың үлесінің артуымен бірге артып келе жатқанын көрсетеді. Пайдаланушы үлесі мен АҚ инциденттерінің саны арасындағы корреляция коэффициенті 0,78 құрайды, бұл осы айнымалылар арасындағы жеткілікті күшті оң байланысты көрсетеді.

Алайда тек осы мәліметтер негізінде пайдаланушылар үлесінің артуы мен АҚ инциденттерінің саны арасында себеп-салдарлық байланыс орнату мүмкін емес. Интернет пайдаланушыларының көбеюі, Интернет технологияларындағы осалдықтардың артуы, пайдаланушылардың қауіпсіздік ережелерін сақтамау және басқа факторлар сияқты басқа факторлар да АҚ инциденттерінің санына әсер етуі мүмкін.

Толыққанды талдау жасау үшін АҚ инциденттерінің санына әсер етуі мүмкін басқа факторларды одан әрі талдау және олардың уақыт өте келе АҚ инциденттері санының өзгеру динамикасына әсерін бақылау қажет.

Елімізде халықтың цифрлық сауаттылығының статистикасы тек 2018 жылдан бері жүргізіліп келеді. Зерттеу барысында бұл көрсеткішті ақпараттық қауіпсіздік инциденттерімен салыстыруға шешім қабылданды (7-сурет).



7-сурет – халықтың цифрлық сауаттылығын салыстыруды талдау және АҚ инциденттерінің саны

Ескертпе – автормен әзірленген

Деректер цифрлық сауаттылық деңгейінің артуымен ақпараттық қауіпсіздік инциденттерінің саны да артып келе жатқанын көрсетеді. Сандық сауаттылық пен АҚ инциденттерінің саны арасындағы корреляция коэффициенті 0,86 құрайды, бұл осы айнымалылар арасындағы жеткілікті күшті оң байланысты көрсетеді. Бұл жағдайда біз кері кореляцияны алғымыз келеді.

Алайда, алдыңғы мысалдағыдай, цифрлық сауаттылық деңгейі мен ақпараттық қауіпсіздік инциденттерінің саны арасында тек осы мәліметтер

негізінде себеп-салдарлық байланыс орнату мүмкін емес. Жаңа технологиялардың дамуы, желідегі қауіптердің жоғарылауы, қолданбалар мен қызметтердегі осалдықтар сияқты басқа факторлар да инциденттер санына әсер етуі мүмкін.

Толыққанды талдау жасау үшін АҚ инциденттерінің санына әсер етуі мүмкін басқа факторларды да талдап, олардың цифрлық сауаттылық деңгейімен және басқа факторлармен өзара әрекеттесуін анықтау қажет. Сонымен қатар жалпы тенденцияларды анықтау және ақпаратты қорғау әдістерін жақсарту үшін әрбір нақты АҚ инциденттері себептері мен жағдайларын талдауға болады.

Ақпараттық қауіпсіздікті қамтамасыз ету саласында қабылданатын шаралар

Қазақстанда ақпараттық қауіпсіздікті қамтамасыз ету үшін көптеген шаралар қабылданды. Нормативтік-құқықтық база жетілдірілді. Көптеген НҚА, «Ақпараттандыру туралы», «Дербес деректер және оларды қорғау туралы» заңдар, «Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптар» туралы Үкімет Қаулысы қабылданды, ақпараттық қауіпсіздік жөніндегі халықаралық стандарттар және т. б. сәйкес келтірілді [27-29].

Қазақстанда 2016 жылы Ақпараттық қауіпсіздік комитеті құрылды, ол елдегі ақпараттық қауіпсіздікті қамтамасыз ету бойынша шараларды үйлестірумен айналысады. Сонымен қатар көптеген мемлекеттік органдардың өздерінің Ақпараттық қауіпсіздік қызметтері бар.

Ақпараттық-коммуникациялық инфрақұрылым дамыды. Қазақстанда АҚҰҰО, ақпараттық қауіптердің мониторингімен және оларға ден қоюмен айналысатын ақпараттық қауіпсіздіктің жедел орталықтары құрылды. Сондай-ақ ұлттық доменді басқару орталықтары мен DDoS шабуылдарынан қорғау орталықтары құрылды.

Білім және хабардарлық. Қазақстанда халықтың және ақпараттық қауіпсіздік саласындағы мамандардың хабардарлығын арттыру бойынша іс-шаралар жүргізілуде. Сонымен қатар жоғары оқу орындары мен колледждер ақпараттық қауіпсіздікке байланысты мамандықтарды ұсынады.

Халықаралық ұйымдармен ынтымақтастық. Қазақстан БҰҰ, ЕҚЫҰ және басқалары секілді халықаралық ұйымдармен ақпараттық қауіпсіздік және киберқылмыспен күрес мәселелері бойынша белсенді ынтымақтасады.

Жалпы, Қазақстан ақпараттық қауіпсіздікті қамсыздандыру мақсатында кең ауқымды шаралар қабылдауда, алайда, басқа елдердегідей, бұл проблема өзекті болып қала береді және одан әрі жетілдіру мен жақсартуды талап етеді.

«Киберқалқан» туралы

Қазақстан өзінің «Қазақстанның киберқауіпсіздігі» ұлттық киберқауіпсіздік тұжырымдамасын бекітті және іске асыруға кірісті [16]. Жаңа технологиялар мен электрондық қызметтер күнделікті өмірдің ажырамас бөлігіне айналды. Біз ақпараттық және коммуникациялық технологияларға барған сайын тәуелді бола отырып, бұл технологиялардың қорғалуы мен қол жетімділігі мемлекеттің басты алаңдаушылығына айналды. 2017 жылдың қаңтарында Тұңғыш Президент Нұрсұлтан Назарбаев Үкіметке Қазақстанның киберқалқанын құруды тапсырды. Бес айдан кейін Үкімет тұжырымдаманы бекітті. Бастапқыда министрлік елдегі киберқауіпсіздік жағдайына негізделген тұжырымдама жобасын жасады. Алайда бұл ретте мемлекеттің мүдделері ғана ескерілді. Содан кейін қоғамдық пікірталастар болды және тұжырымдаманың жобасын кәсіпқойлар тым «біржақты» деп сынға алды.

Киберқауіпсіздік тұжырымдамасының нысаналы индикаторлары («Қазақстанның киберқалқаны») келесі кестеде берілген (4-кесте).

4-кесте – Тұжырымдаманың нысаналы индикаторлары

Индикатор атауы	**2018**	**2019**	**2020**	**2021**	**2022**
Қазақстанның жаһандық киберқауіпсіздік индексі 2017 жылға қарай	0,300	0,400	0,500	0,550	0,600
2018 жылдың базалық кезеңіне ақпараттық қауіпсіздік қатерлері туралы хабардарлықты арттыру		5%	10%	15%	20%
2018 жылы ақпараттық қауіпсіздік саласында қайта даярланған мамандар саны	300	500	600	700	800
2017 жылдың базалық кезеңіне қарай мемлекеттік және квазимемлекеттік салаларда қолданылатын ақпараттандыру және байланыс аясындағы отандық бағдарламалық өнімдердің үлес салмағын арттыру	10%	20%	30%	40%	50%
Деректерді .KZ және .ҚАЗ доменімен Интернет-ресурстармен шифр күйінде ұсынуда отандық қауіпсіздік сертификаттарын пайдаланудың орташа үлесі 2018 жылы 20 % құрайды	20%	40%	60%	80%	100%
Ақпараттық қауіпсіздік мониторингі орталықтарына қосылған Мемлекеттік органдардың ақпараттық жүйелерінің, мемлекеттік органдармен интеграцияланатын мемлекеттік емес ақпараттық жүйелердің, ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілерінің ақпараттық жүйелерінің үлесі	20%	40%	60%	80%	100%

Киберқалқан тұжырымдамасын жүзеге асыруда кездесетін негізгі мәселелерге мыналар жатады:

- азаматтардың киберқауіпсіздік қатерлері туралы хабардар болмауы;
- ақпараттық қауіпсіздік бойынша практикалық мамандардың жетіспеушілігі;
- ақпаратты қорғауға дайын емес инфрақұрылым;
- ұйымдардың ақпараттық қауіпсіздік талаптарын елемеуі;
- бірнеше қарапайым бағдарламалық өнімдерді қоспағанда, мемлекеттік секторға шектеулі сенім;
- электрондық мемлекеттік қызметтер көрсетуге байланысты тәуекелдер.

Ең алдымен, маңызды ақпараттық инфрақұрылымды қорғаудың нақты стратегиясының болмауы. Тұжырымдамада энергетика, көлік және денсаулық сақтау жүйелері сияқты мемлекеттің жұмыс істеуі үшін маңызды жүйелерді қорғаудың нақты шаралары жоқ. Мұндай стратегиясыз тұжырымдама киберкеңістікте ұлттық қауіпсіздікті қорғауға кепілдік бере алмайды.

Екіншіден, тұжырымдама киберкеңістікте Қазақстан алдында тұрған қауіп-қатерлердің жеткілікті егжей-тегжейлі сипаттамасын бермейді. Ол тек киберқылмыс, кибертыңшылық және кибертерроризм сияқты жалпы қауіптер туралы айтады, бірақ нақты мысалдар мен шабуыл сценарийлерін келтірмейді. Мұндай ақпаратсыз тиімді қорғаныс шараларын әзірлеу қиын.

Үшіншіден, тұжырымдама киберқауіпсіздік саласындағы кадрлық әлеуетті дамытуға жеткілікті көңіл бөлмейді. Ол ақпаратты қорғау үшін жаңа құрылымдар мен ұйымдар құруды көздейді, бірақ мамандарды оқыту мен даярлау қажеттілігін көрсетпейді. Бұл құрылған құрылымдардың ұлттық қауіпсіздікті тиімді қорғай алмауына әкелуі мүмкін.

Тұжырымдама басқа елдермен ынтымақтастыққа жеткілікті назар аудармайды, киберқауіптермен күресуге көмектесетін халықаралық ынтымақтастықтың нақты мысалдарын келтірмейді.

Ақпараттық қауіпсіздікті қамтамасыз ету бойынша халықаралық тәжірибе

2017 жылы 150-ден астам елдегі 200 мың ұйым зиянды бағдарламалардың (WannaCry және Petya вирустары) құрбаны болды, олардың мақсаты кейіннен ақша бопсалау үшін компьютерлердегі файлдарды бұғаттауға дейін азайды. 2019 жылы компьютерлік хакерлер (рұқсатсыз кірулер) – British Airways және Marriot Sherwood Hotels, Facebook, Google+ іске асырылды. Бұл киберқауіпсіздік саласындағы бағдарламалық өнімдерді әзірлеуге, ұйымдардың штат санын толықтырған компьютерлік жүйелерді қорғау жөніндегі мамандар топтарын құруға айтарлықтай инвестициялар салуға әкеп соқты.

Ұлыбританияда 2006 жылдан бастап IT саласында қызмет көрсететін ұйымдарды аккредиттеу және жеке тұлғаларды сертификаттаумен айналысатын ақпараттық қауіпсіздік мәселелерін жүргізетін CREST коммерциялық емес ұйымы құрылды. CREST мүшелері жыл сайын аккредиттелген компаниялар болып табылады. CREST-те сертификаттауды қалайтын жеке тұлғаларға да жоғары талаптар қойылады. Олар әртүрлі дәрежедегі емтихандарды тапсырады

(жұмыс тәжірибесін ескере отырып), онда олар IT саласындағы жоғары білікті мамандар ретінде өздерінің білімдерін, дағдылары мен дағдыларын көрсетуі керек. Сертификатталған мамандар үш жыл сайын емтихандарды қайта тапсырады.

Осы ұйымның арқасында Англия Үкіметі үшін киберқауіпсіздік стандарттарын — Cyber Essentials және Cyber Essentials Plus техникалық бағалау және сертификаттау жүйелері әзірленді, бұл зиянды бағдарламалардан, атап айтқанда WannaCry вирусынан қорғауға мүмкіндік береді. Ең бастысы, веб-сайттарды, қосымшаларды, дерекқорларды, серверлерді, компьютерлік желілерді, мобильді құрылғыларды (ноутбуктер, портативті шағын компьютерлер, ұялы телефондар және т.б.) қорғау шараларын әзірлеу [30].

2019 жылы Австралияда кибернетикалық өзара іс-қимыл орталығы құрылды, оның мақсаты әлемдік нарықтарға жаңа тауарлар мен қызметтерді шығару арқылы компанияларды дамыту болып табылады. Оның қызметінің бағыттары ретінде: барлық деңгейдегі IT-сала қызметкерлерін даярлау; ұйымдардың пайдаланылған жабдықтар мен желілік конфигурацияларды қауіпсіздік тұрғысынан тестілеуді тікелей өткізуі және т.б. [22]. Австралия үкіметі киберқылмыспен күресудің стратегиялық бағыттары ретінде мыналарды анықтады: кибершабуылдарға шұғыл әрекет ету үшін мамандар даярлау; мемлекеттік мекемелердің киберқауіпсіздігін нығайту жөніндегі шараларды әзірлеу және енгізу үшін IT-сарапшылар тобын қалыптастыру; мектептерде Интернет-қауіпсіздік сабақтарын енгізу [31].

Бразилия үкіметі 2018 жылы ақпараттық қауіпсіздік стратегиясын әзірледі. Атап айтқанда, 2018 жылдың сәуірінде елдің Ұлттық қаржы кеңесі цифрлық ақпаратты өңдеу, сақтау және пайдалану бойынша мердігерлерді тарту туралы талапты баяндайтын қарар дайындады. Сол жылы «Дербес деректерді қорғау туралы жалпы заң» нормативтік құқықтық актісі шығарылды және 2020 жылдың тамызынан бастап Ақпаратты қорғау жөніндегі ұлттық орган өз жұмысын бастады. Қазіргі уақытта Бразилияда компьютерлік қауіпсіздікті зерттеу, әрекет ету және апаттарды жою орталығы бар (CERT.br), оның мамандары киберқауіптерге жауап береді. Бұл ретте компьютерлік ақпаратты қорғау жөніндегі қызметті жетілдіру бағыты ретінде киберқауіпсіздік проблемалары туралы жұртшылықтың хабардар болу деңгейін арттыру және киберқылмыс құрбандары үшін сенім телефонын құру ұсынылады [32].

ҚХР-да киберқылмыспен күрес белсенді жүргізілуде. 1997 жылдан бастап ҚХР Қылмыстық кодексі компьютерлік қылмыстар үшін жауапкершілікті көздейтін жаңа баптармен толықтырылды. 2017 жылдың маусымынан бастап Қытай Халық Республикасының киберқауіпсіздік туралы Заңы қолданыста болды, ол пайдаланушы деректерін жинауды, сақтауды, өңдеуді реттейді, ақпараттық қауіпсіздік жүйесіне қатысушылардың міндеттерін анықтайды, оларды бұзғаны немесе орындамағаны үшін жазаны қарастырады. Қытай тұрғындары құрбан болған киберқылмыстарға жүргізілген зерттеулер осы әлеуметтік қауіпті әрекеттерді келесі топтарға бөлуге және қорытындылауға мүмкіндік берді:

- банктік немесе төлем онлайн-шоттарына рұқсатсыз қол жеткізу түріндегі нақты активтерді ұрлау (ақшаны жылыстату жалған деректері бар қылмыскердің шоттарына ақша аудару, содан кейін банкоматтар арқылы қолма-қол ақша беру арқылы жүзеге асырылады; немесе ұрланған активтер дүкен карталарын немесе төлем карталарын сатып алу үшін пайдаланылады);

- виртуалды активтерді ұрлау (шотты бұзғаннан кейін активтер басқа шотқа аударылады немесе оны бақылауды қамтамасыз ету үшін пароль мен шот параметрлері өзгереді, ал кейіннен алынған активтер немесе шоттар қара нарықта сатуға қойылады);

-интернет-ресурстарды бұзу;

- хакерлік технологиялар (зиянды бағдарламаларды әзірлеу және іске асыру; киберқылмыстық қызмет тұлғаларын іріктеу және оқыту [33].

ҚХР Үкіметі тарапынан аталған қылмыстарға қарсы іс-қимылдың қабылданып жатқан шараларына қарамастан, бұл бағыт өзекті болып қала береді. Киберқылмыстарға қарсы күрес саласында мамандардың болмауы; осы қоғамдық қауіпті іс-әрекеттер үшін жаза тағайындау кезінде сот төрешілерінің кешірімді ұстанымы; киберқылмыс және оның зияны туралы, сондай-ақ цифрлық ақпаратты қылмыстық қол сұғушылықтардан қорғау шаралары туралы халықтың хабардар болмауы (мектептер мен медициналық мекемелердің компьютерлік жүйелері кибершабуылдардың неғұрлым осал объектілері болып табылды), шын мәнінде, киберқылмыстың дамуына жағдай жасайды. ҚХР Үкіметінің пікірінше, оларды жоюға ақпараттық қауіпсіздік саласындағы жұмыс бағытталуы керек [34].

Қазақстандағы Интернет-алаяқтық

Онлайн-алаяқтық (fline fraud) – киберқылмыскерлердің Интернет пайдаланушысының ақпараттық деректерін немесе қаржы қаражатын иемденуге бағытталған әрекеттері.

Алаяқтар жалған Интернет-дүкен немесе белгілі сайттардың аналогын жасайды, онда тауар немесе қызмет үшін төлем әдістері көрсетілген. Сайттың сенімді екенін анықтау өте қиын. Қызығушылық танытқан өнімді таңдау үшін сатып алушы дүкенге «виртуалды» түседі және, әрине, аталған тауардың шындығында бар-жоғы, сондай-ақ жарияланған сипаттамалар мен фотосуреттер қаншалықты шындыққа сәйкес келетіні белгісіз. Интернет арқылы тауарларды сатып алғанда, толық немесе ішінара алдын-ала төлем жиі қабылданады. Барлық аударылған ақша дүкен иесінің шотына түседі, ол алдын-ала төлем алғаннан кейін тауарды жібермеуі немесе сапасыз немесе басқа түрде жіберуі мүмкін.

Сонымен қатар интернет-ресурстарды анонимизация қызметтерін ұсынатын шетелдік сайттардың көмегімен тіркеуге болады, бұл кейбір жағдайларда алаяқтар туралы сенімді ақпарат алуды қиындатады (8-сурет).

8-сурет – Қазақстандағы Интернет-алаяқтықтар саны

Ескертпе – автормен 35 дереккөз негізінде құрастырылған

2018 жылы интернеттегі алаяқтықтың тек 517 жағдайы тіркелді, бірақ 2021 жылға қарай бұл сан 21 405-ке дейін өсті. Бұл 2018 жылмен салыстырғанда 40 есе көп.

Құқық қорғау органдарының мәліметі бойынша, Интернеттегі алаяқтықтың ең көп таралған әдістері:

-Интернет-хабарландырулар бойынша тауар немесе қызмет үшін алдын ала төлем немесе толық төлем алу;

- пластикалық карта шоттарынан ақша ұрлау;

- әртүрлі жобаларға, ойындарға, инвестицияларға, ставкаларға және т.б. ақша салу;

- азаматтардың дербес деректерін иеленуге арналған фишингтік сілтемелерді пайдалану.

Сызықтық регрессияны қолдана отырып, 2018-2022 жылдардағы Интернет-алаяқтық туралы мәліметтер негізінде олар алдағы үш жылға болжам жасауға тырысты. Нәтижесінде біз осындай деректерді алдық. 2023 жылы 29005 жағдайға, 2024 жылы – 34379 жағдайға, 2025 жылы – 39753 жағдайға дейін ұлғайады (9-сурет).

9-сурет – Интернет-алаяқтық бойынша болжамдар

Ескертпе – автормен әзірленген

Жиі жағдайларда қылмыскерлер өздерін банктердің немесе құқық қорғау органдарының қауіпсіздік қызметінің қызметкерлері ретінде таныстырды және азаматтардың шоттарындағы күдікті операциялар туралы хабарлады. Көптеген азаматтар сеніп, ақшаны алаяқтар көрсеткен шоттарға аударды немесе алаяқтарға өздерінің жеке мәліметтерін өз еркімен берді.

Жәбірленуші бір аймақта, ал шабуылдаушы басқа аймақта болған жағдайлар көптеп кездеседі. Бұл алаяқтықты анықтауды қиындатады. Әдетте, қылмыс тізбегі әдетте күрделі және көптеген сілтемелерден тұрады. Алаяқтар әртүрлі банктік шоттарды, пластикалық карталарды, үшінші тұлғаларға арналған әртүрлі абоненттік нөмірлерді пайдаланады. Айта кететін жайт, мұндай құқық бұзушылықтарды тіркеуді зардап шеккендердің үнсіздігі қиындатады.

Жұмыс тиімділігін арттыру мақсатында Қазақстан Республикасының Ішкі істер министрлігі алаяқтыққа қарсы іс-қимыл бойынша тұрақты негізде ұйымдастырушылық-практикалық шаралар қабылдауда. 2021 жылдан бастап Киберқылмысқа қарсы іс-қимыл жөніндегі 2021-2022 жылдарға арналған ведомстволық бағдарлама іске асырылуда.

Қазақстанда 2021 жылдың қорытындысы бойынша ақпараттық қауіпсіздік мәселелері бойынша халықтың хабардарлығы 75%-ды құрады. Бұл көрсеткіш 2018 жылы 62,9%, 2019 жылы 73,5%, 2020 жылы 78%-ды құрады. 2021 жылы министрлікте ақпараттық қауіпсіздік (киберқауіпсіздік) мәселелерінде азаматтардың хабардарлық деңгейінің 3%-ға төмендеуі пандемия, өзін-өзі оқшаулау режимі және карантиндік шаралар Интернетті тұрақты

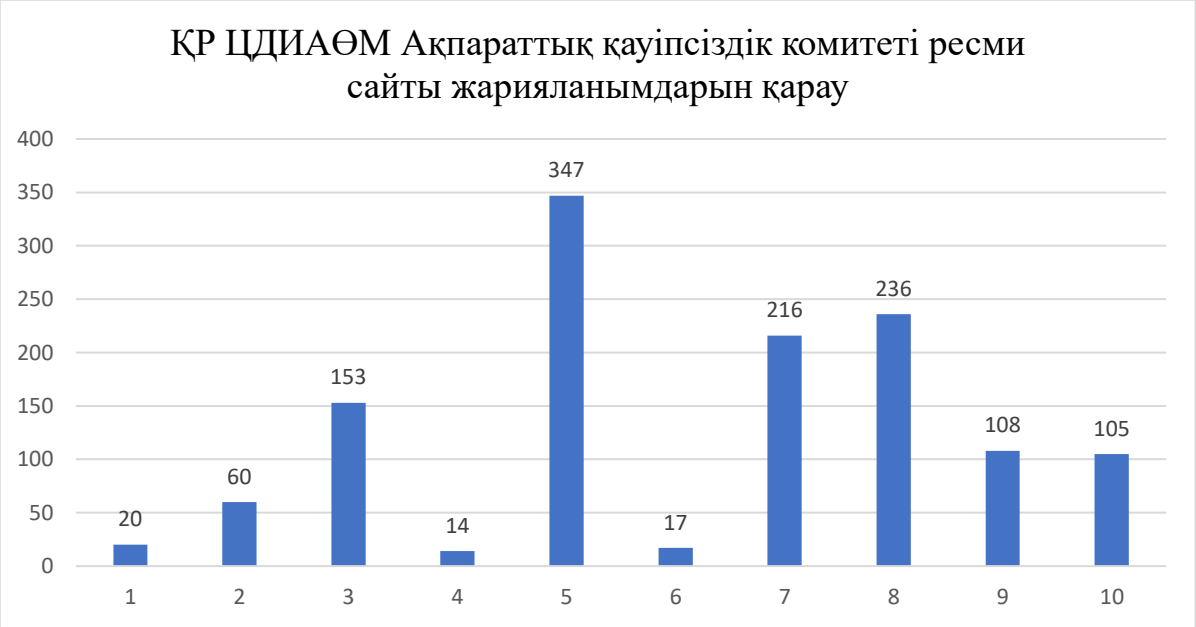
пайдаланушылардың үлесін арттырды деп түсіндіреді. Онлайн қызметке, сондай-ақ, бұрын болмаған бизнестің едәуір бөлігі қосылды. Адамдар белсенді бола бастады, ресми статистика мобильді қосымшаларды пайдаланудың, қашықтан жұмыс істеудің және виртуалды оқытудың қарқынмен артуын көрсетеді. Егер 2020 жылы цифрландыру экономика мен қоғамдық өмірдің көптеген салалары үшін «шок» болса, 2021 жылы күнделікті өмірге айналды [35]. Автор осы тақырыпты зерделеу барысында мемлекеттік органдар мұндай жағдайларда бей-жай қалмауы керек, керісінше киберқылмыстардан қорғау үшін мерзімінен бұрын шаралар қабылдауы керек екенін ерекше атап өтті. Ақпараттық қауіпсіздікке келетін болсақ, мұндай әрекеттер мемлекеттік органдардың сезімталдығы мен жауапкершілігін талап етеді [36] .

Киберқауіптер туралы хабардар болу

Мәжіліс депутаты Екатерина Смышляева атап өткендей, инциденттерге ден қою қызметінің мониторингіне сәйкес, деректердің бұзылуымен болған инциденттердің 95%-ы пайдаланушылар тарапынан қолжетімділікті ерікті түрде беру кезінде орын алады [37]. Соңғы мәліметтер бойынша хабардарлық көрсеткіші 75%-ды құрайды. Неліктен ақпараттық қауіпсіздік инциденттерінің осындай жоғары көрсеткіші бар деген сұрақ туындайды.

Ақпараттық қауіпсіздік комитеті өзінің ресми парақшасында ақпараттық қауіпсіздікті қамтамасыз ету бойынша ақпараттық материалдарды, бейнероликтер, жадынамалар және т.б. жариялайды.

Эксперимент ретінде ҚР ЦДИАӨМ Ақпараттық қауіпсіздік комитеті ресми сайтынан соңғы 10 жарияланым ұсынылды. Қаралым саны 14-тен 347-ге дейін, бұл өте төмен көрсеткіш. Барлық деректер 28.03.2023 жылғы жағдай бойынша (10-сурет).



10-сурет – ЦДИАӨМ Ақпараттық қауіпсіздік комитеті сайтындағы

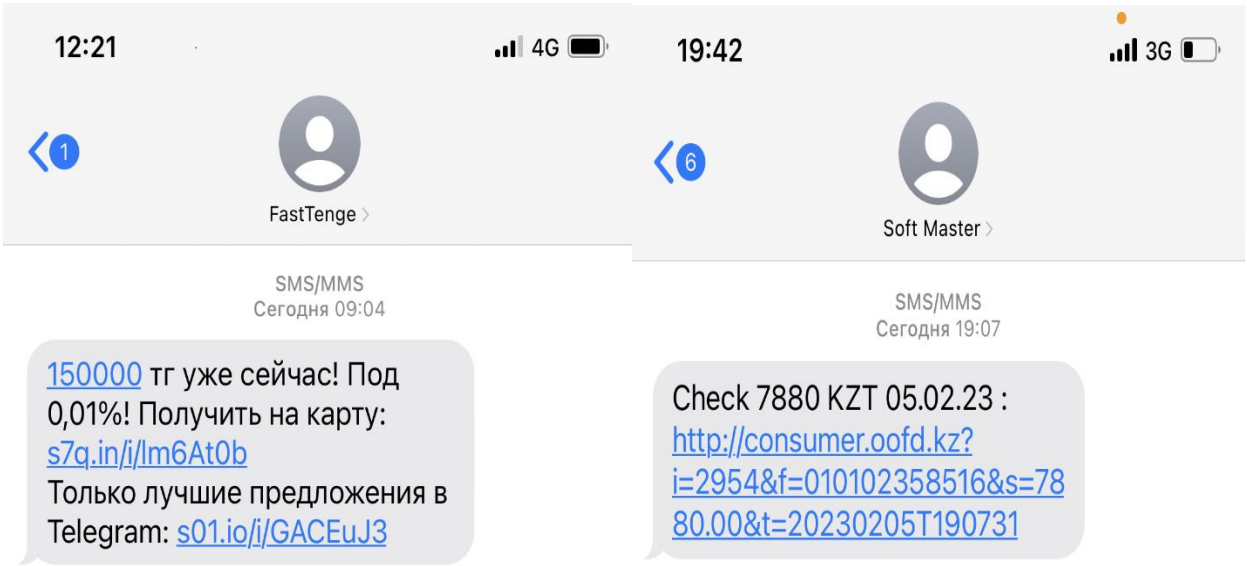
жарияланымдарды қаралым саны

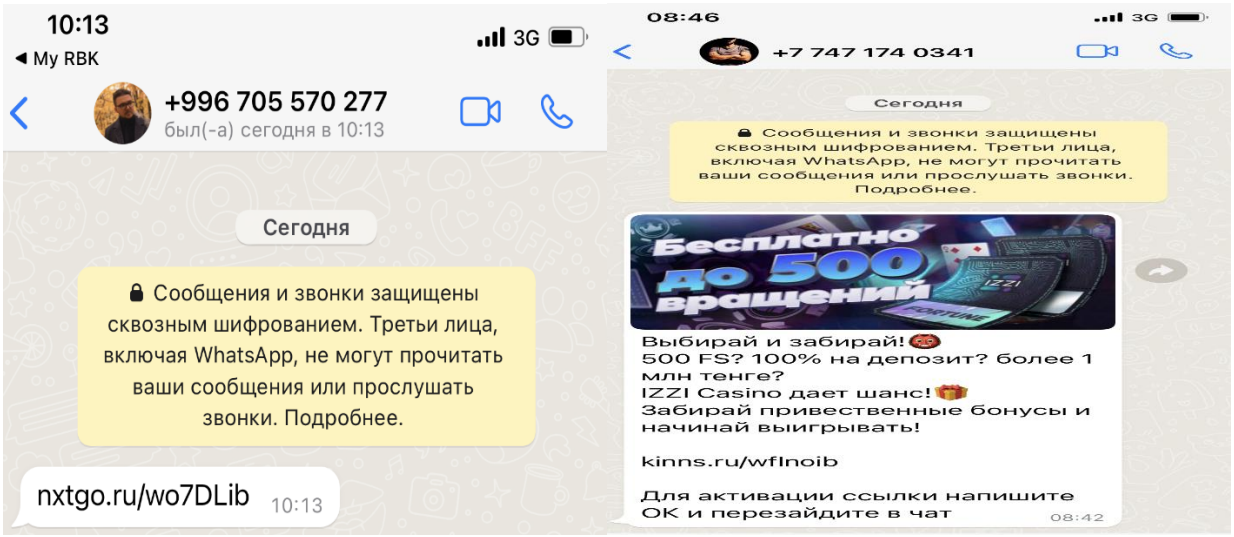
Ескертпе – автормен құрылған

Instagram әлеуметтік желісінде Комитеттің өз парақшасы жоқ, ҚР ЦДИАӨМ 1614 жазылушысы бар. «Мемлекеттік техникалық қызмет» АҚ өз бетінде 2230 жазылушысы бар. Бұл елдегі ақпараттық қауіпсіздікті қамтамасыз ететін негізгі ведомстволар. Статистикаға сәйкес, 6-74 жас аралығындағы Интернет желісін пайдаланушылардың үлесі 92,9% немесе 17 539 104 пайдаланушыны құрайды. Интернет қолданушыларының 0,1%-ы да хабардарлыққа қол жеткізе алмайды.

Мониторингке сәйкес, жоғарыда атап өткендей, деректердің таралып кетуімен болған инциденттердің 95%-ы пайдаланушылардың қолжетімділікті ерікті түрде беру кезінде орын алады. «МТҚ» АҚ жағында орнатылған жабдықтардың Интернетке қолжетімділігінің бірыңғай шлюзі 2023 жылғы ақпанда 7 812 854 кибершабуылды бұғаттады [26].

Сондай-ақ зерттеу жұмысы барысында эксперимент жүргізді. Зерттеу барысында тегін хабарландырулар, мобильді нөмірді көрсете отырып, хабарландыру жарияланды. Кейін түсініксіз сілтемелері бар күдікті ұсыныстар келе бастады (11-сурет).





11-сурет – Күдікті хабарламалардың скриншоты

Ескертпе – Автормен жасалған

Осы бақылаудан кейін жеке деректердің таралып кетуін тегін хабарландыру сайтынан келеді деп сенуге негіз бар. Бұл түр фишингтік алаяқтыққа қолайлы. Фишингтік алаяқтық – Интернет-алаяқтықтың бір түрі, онда алаяқтар жалған электрондық хаттар немесе хабарламалар жібереді, олар өздерін банк немесе мемлекеттік орган секілді заңды тұлға ретінде таныстырып, адамдарды жеке және қаржылық ақпараттарын алып алады.

Ақпараттық қауіпсіздік инциденттерін азайту үшін ұсынылатын шаралар

Бірінші.

Зерттеу көрсеткендей, біздің елімізде 600-ге жуық ақпараттық жүйе бар. Қайталанатын мәліметтер базасы аз емес. Мысалы, 32 дерекқорда еліміздің азаматтарының тұрғылықты мекенжайы сақталған.

Ақпараттық жүйелердің жұмыс қабілеттілігін қамтамасыз етуге республикалық бюджеттен жыл сайын 30-дан 50 млрд. теңгеге дейін жұмсалады. Айта кететін жайт, бұл қаражат тек техникалық қолдауға жұмсалады, дамуға жұмсалмайды. Мемлекеттік құпиялар туралы мәліметтерді құрайтын жүйелерді қоспағанда, көптеген ведомствоаралық ақпараттық жүйелерді бір немесе бірнеше әмбебап **бірыңғай цифрлық платформаларға біріктіру.** Бұл әртүрлі жүйелерді әзірлеу, қолдау, жаңарту және ақпараттық шығындарын азайтады. Бұл жұмысты бастамас бұрын, барлық тараптар келесі мәселелерді зерделеуі керек:

- ақпараттық жүйелердің қандай түрлерін біріктіру керек, олардың сипаттамалары мен бір-бірімен үйлесімділігі қандай;
- қандай деректерді біріктіру керек және олар қалай құрылымдалады және қалай бір-бірімен байланысты болады;
- жаңа бірыңғай платформада пайдаланушылар үшін қандай мүмкіндіктер болуы керек;

- деректердің қауіпсіздігі мен құпиялылығы мәселелері қалай шешіледі;

- жаңа платформаны әзірлеуге және енгізуге қандай бюджет бөлінетін болады және оның жұмысын қолдау үшін қандай ресурстар қажет болады.

Сонымен қатар ақпараттық жүйелерді біріктіру әртүрлі ведомстволар арасында келісуді, сондай-ақ жұмыс процестері мен бизнес логикасындағы өзгерістерді талап етуі мүмкін. Сондықтан ақпараттық жүйелерді бір платформаға біріктіру күрделі және ресурстарды қажет ететін процесс болып табылады, ол байыпты көзқарас пен жоспарлауды қажет етеді.

Күтілетін әсер. Ақпараттық жүйелерді бір платформаға біріктірудің көптеген артықшылықтары болуы мүмкін, мысалы:

- Тиімділікті жақсарту. Деректерді іздеу және талдау уақытын қысқарту, процестерді автоматтандыру және қателіктер қаупін азайту, бұл қызметкерлерге өз жұмысын тезірек және тиімдірек орындауға мүмкіндік береді;

- Басқаруды жеңілдету. Басқаруды жеңілдету, бірнеше жүйелерді басқару және техникалық қызмет көрсету шығындарын азайту, оған тартылған адамдар мен жабдықтардың санын азайту;

- Деректер сапасын жақсарту. Деректерді бір платформаға біріктіру, тексеру және басқару мүмкіндігі, бұл олардың дәлдігін, орындылығы мен толықтығын жақсартуға мүмкіндік береді;

- Шешім қабылдау жылдамдығын арттыру. Ағымдағы деректерге, жиынтық ақпаратқа және аналитикалық құралдарға жылдам қолжетімділік (деректер көрмесі), бұл шешім қабылдау уақытын қысқартуға және сол шешімдердің дәлдігін арттыруға мүмкіндік береді;

- Икемділікті арттыру. Жүйені сыртқы жағдайлардың өзгеруіне оңай бейімдеу мүмкіндігі, бұл мемлекеттік органдарға өзгерістерге, алушылардың қызметтерінің талаптарына және ішкі өзгерістерге икемді жауап беруге мүмкіндік береді;

- Тәуекелдерді азайту. Деректерді қорғауды жақсарту, деректерді қолмен енгізуге және бірнеше жүйеде бірдей ақпаратты қайта енгізуге байланысты қателіктердің ықтималдығын азайту және басқару шешімдерінің сапасын жақсарту.

Жалпы, бірыңғай платформа мемлекеттік органдарға ақпараттық жүйелерді басқару шығындарын азайтуға, деректердің сапасын арттыруға және шешім қабылдауды жеделдетуге көмектеседі, бұл МО-ның бәсекеге қабілеттілігін жақсарта алады.

Екінші.

Тегін жарнаманы орналастыру тәжірибесі көрсеткендей, тегін жарнамалар сайтының көмегімен (kolesa.kz, olx.kz, krisha.kz және т.б.) Қазақстан Республикасы азаматтарының мобильді нөмірлерінің дерекқорын жинау мүмкіндігі бар. Деректердің тарап кетуін болдырмау үшін осындай сайттарда жеке тұлғалардың **телефон нөмірлерін жасыру** ұсынылады.

Сатушымен және сатып алушымен қарым-қатынас жасау үшін жүйелік идентификатор (ID) көмегімен ақпарат алмасу чатының бұрыннан бар функционалын қалдыру қажет Екінші / балама нұсқа, автоматты телефон

станциясы (АТС), ол кіріс қоңыраулар ағынын тіркейді және бағыттайды. Хабарландыруларда жалпы нөмір көрсетіледі және соңғы 4 сан пайдаланушының жеке куәлігі болады. Бұл автоматты телефон станциясы ҚР ІІМ Интернет-алаяқтар нөмірлерінің дерекқорымен интеграциялануы тиіс. Бұл құрал жалған сатып алушылардан қоңырауларды блоктайды және Интернет-алаяқтық санын азайтады.

Күтілетін әсер.

Экономикалық шығындарды азайту. Интернеттегі алаяқтық экономикаға жеке компаниялардың шығындарына да, алаяқтыққа қарсы шығындарға да айтарлықтай зиян келтіреді. Алаяқтықпен күресудің тиімді шаралары экономикалық шығындарды азайтуға, қаржылық тұрақтылықты сақтауға және бизнестің өсуіне ықпал етеді.

Үшінші.

Қызметкерлерге киберқауіпсіздік туралы хабардарлықты арттыру мақсатында оларға киберқауіптерді анықтауға және алдын алуға көмектесу үшін ақпарат беру форматын өзгерту ұсынылады. Ақпараттық қауіпсіздіктің өзекті мәселелерін ескере отырып, YouTube-те таңдалған бейнені көрер алдында және Instagram әлеуметтік желісіндегі мақсат ретінде жарнамалар ретінде танымал платформаларда оқытатын бейнероликтерді орналастыруды қарастыруды ұсынамын. ҚР ЦДИАӨМ Ақпараттық қауіпсіздік комитеті сайтының ресми бетінде орналастырылған бейнероликтер Интернетті пайдаланушылар арасында өте төмен қамтуды көрсетеді.

Жоғарыда атап өткендей, оқытатын бейнероликтердің қамтылуы өте төмен. Instagram әлеуметтік желісінде 12,6 млн қазақстандық қолданушы, ал YouTube-те 12 млн қазақстандық қолданушы бар [38]. Бұл Интернет желісін пайдаланушылардың жалпы санының шамамен 78%-ды құрайды.

100 000 пайдаланушыны қамти отырып, Instagram әлеуметтік желісіндегі жарнаманың құны 390$ немесе 177 060 (18.04.2023 ж.454 теңге бағамы бойынша) тұрады. Жылына бұл сома 2, 125 млн теңгені құрайды.

Youtube-те жарнаманың орташа құны айына шамамен 250 000 теңгені құрайды. Жылдық сома 3 000 000 теңгені құрайды.

Күтілетін әсер.

Қауіпсіздік шараларының күшеюі және алаяқтық әдістері туралы хабардарлықтың жоғарылауы арқылы адамдар интернетті пайдаланған кезде сергек және сақ болады. Бұл алаяқтық шабуылдардың азаюына және алаяқтардың құрбаны болған адамдардың азаюына әкелуі мүмкін.

Қорытынды

Қорытындылай келе, ақпараттық қауіпсіздік қазіргі әлемдегі ең маңызды және өзекті мәселелердің бірі болып табылатынын және ақпарат қауіпсіздігі бизнестің, ұйымдар мен мемлекеттердің табысы үшін маңызды екенін атап өткен жөн. Елімізде ақпараттық жүйелер мен желілерді киберқауіптерден қорғау үшін бірнеше қадамдар жасалды, соның ішінде саясат, ережелер және техникалық шаралар әзірленді. Киберқауіпсіздік тұжырымдамасы («Қазақстанның киберқауіпсіздігі») мұның айқын мысал болып табылады[39].

Қазақстан Республикасының ақпараттық қауіпсіздігімен қамсыздандыру қазіргі қоғамның маңызды аспектісі болып табылады, өйткені цифрлық технологияларды пайдалану соңғы 10-15 жылда кең тарала бастады. Құпия ақпаратты қорғау бүкіл әлемдегі жеке тұлғалар, кәсіпорындар мен үкіметтер үшін үлкен проблемаға айналды. Бұл магистрлік жоба ақпаратты қорғау үшін қолдануға болатын әртүрлі әдістер мен қабылдағыштарды, соның ішінде шифрлауды, қолжетімділікті басқаруды және киберқауіпсіздік шараларын қарастырды. Ол сондай-ақ киберқауіптер қаупін азайту үшін қызметкерлер мен пайдаланушылар арасында хабардарлық пен білім беру мәдениетін құрудың маңыздылығын көрсетеді. Бұл жобаның нәтижелері ақпараттық қауіпсіздік тәжірибесін жетілдіру және құпия ақпаратты рұқсатсыз кіруден және пайдаланудан қорғау бойынша ағымдағы күш-жігерге үлес қосады деп үміттенеміз. Бұл шараларды тиімді жүзеге асыру технологияға деген сенімділікті арттыруға және сайып келгенде, жалпы қоғамға пайда әкелуі мүмкін.

Қазақстан Үкіметі елдің ақпараттық қауіпсіздік саласындағы бастамаларын қадағалау үшін Ұлттық ақпараттық қауіпсіздікті үйлестіру орталығын (ҰҚШҰ) құрды. ҰҚҚУ ақпараттық қауіпсіздік саласындағы саясатты, стандарттар мен нұсқаулықтарды әзірлеуге және енгізуге, сондай-ақ киберқауіпсіздіктерге ден қою шараларын үйлестіруге жауапты.

Қазақстан сондай-ақ ақпараттық қауіпсіздікті қорғау бойынша бірқатар заңнамалық шараларды енгізді. 2015 жылғы «Ақпараттандыру туралы» Заң және 2013 жылғы «Дербес деректер және оларды қорғау туралы» Заң деректерді қорғау мен жеке өмірге қол сұғылмаушылықтың құқықтық негізін қамтамасыз етеді. Үкімет сонымен қатар Киберқауіпсіздік тұжырымдамасын («Қазақстанның киберқауіпсіздігі») қабылдады, ол олардың қауіпсіздігін қамтамасыз ету үшін ақпараттық технологиялар мен деректерді беру желілерін пайдалануды реттейді.

Диссертациялық жұмыс барысында атап көрсетілгендей, жыл сайын БҰҰ Халықаралық телекоммуникация Одағының (International Telecommunication Union) эксперттері «Жаһандық киберқауіпсіздік индексі» тақырыбында киберқауіпсіздік деңгейі бойынша мемлекеттердің рейтингін құрады. Соңғы бағалау 2020 жылы жүргізілді. Нәтижесінде Қазақстан 38-орынға ие болды.

Сонымен қатар Қазақстан ақпараттық қауіпсіздік саласында өзінің техникалық мүмкіндіктерін жетілдіру бойынша қадамдар жасады. Елде ақпараттық қауіпсіздік мамандары үшін оқыту және сертификаттау

бағдарламаларын ұсынатын киберқауіпсіздік академиясы құрылды. Мерзімдік киберқолдау жүргізіледі, оның мақсаты мемлекеттік органдардың, ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі бөлімшелердің, аса маңызды объектілердің ақпараттық қауіпсіздіктің жедел орталықтарының туындайтын қауіп-қатерлерге қарсы тұруға дайындығын тексеру болып табылады. Үкімет сонымен қатар өзінің ақпараттық жүйелері мен желілерін қорғау үшін брандмауэр, интрузияны анықтау жүйелері және шифрлау сияқты әртүрлі техникалық шараларды енгізді.

Осы атқарылған жұмыстарға қарамастан, киберқауіпсіздік Қазақстанда айтарлықтай ірі проблема болып қала беруде. Еліміз көптеген танымал кибершабуылдардан, соның ішінде атап айтар болсақ, мемлекеттік органдар мен қаржы институттарынан құпия деректерді ұрлаудан аман қалды. Сол себепті Үкімет пен жеке сектор ұйымдары дамып келе жатқан киберқауіптерге қарсы тұру мақсатында ақпараттық қауіпсіздік шараларын жетілдіруді жалғастыруы керек.

Деректердің қорғалу жағдайын бағалау тәжірибесінен байқағанымыздай, халықаралық индекстер бөлігінде рейтингтік жеңістерге көбіне заңнамалық база стандарттарына сәйкестендіру есебінен қол жеткізілді. Практикада біршама шешілмеген мәселелер сақталуда. Компаниялар өздерінің IT жүйелерін динамикалық түрде түрлендіреді, десе де, киберқауіпсіздікке жеткілікті назар ауыдарылмауда. Ақпараттық қауіпсіздік бойынша білікті мамандардың тапшылығы байқалуда.

Пайдаланылған дереккөздер тізімі

1 Карпова Д., Киберпреступность: глобальная проблема и ее решение // Власть. – 2014. - №08. – С. 192.

2 Қазақстан Республикасы Ұлттық экономика министрінің «Қазақстан Республикасының Ұлттық қауіпсіздік стратегиясын әзірлеу, мониторингтеу, іске асыру, бағалау және бақылау жүргізу әдістемесін бекіту туралы» 2021 жылғы 1 қыркүйектегі № 82 бұйрығы // https://adilet.zan.kz/kaz/docs/V2100024227

3 Мартиросян Т.А. Правовое обеспечение информационной безопасности РФ: Автореф. дис. ... канд. юрид. наук. М., 2005. С. 10.

4 Федотова О.А. Административная ответственность за правонарушения в сфере обеспечения информационной безопасности: Автореф. дис. ... канд. юрид. наук. М., 2003, С. 11.

5 Кисляковский А.В. Административно-правовое обеспечение информационной безопасности: Дис. ... канд. юрид. наук. М., 2003, С. 40.

6 Курушин В.Д., Минаев В.А. Компьютерные преступления и информационная безопасность. М., 1998, С. 165.

7 Global Agenda Council on Cybersecurity, World Economic Forum, April 2016, // http://www3.weforum.org/docs/GAC16_Cybersecurity_WhitePaper_.pdf, p.47

8 Warnes, K., Cybersecurity, Salem Press Encyclopedia. 2019 // https://ezproxy.nu.edu.kz/login?url=https://ezproxy.nu.edu.kz:2358/login.aspx?direct=true&db=ers&AN=89677538&site=eds-live&scope=site

9 Szakos J., Szadeczky T., Building a Cybersecurity Ecosystem in a Hungarian City – The Potential for Innovative Growth //The Choice-Architecture behind Policy Designs. – С. 195-202.//https://www.nispa.org/files/publications/PRACTIC-monograph-final.pdf

10 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.

11 Wihlborg E., Hedström 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.

12 Mishra A., Ghosh S., Mishra B. K. Cybersecurity: A Practical Strategy Against Cyber Threats, Risks with Real World Usages //Cyber Security in Parallel and Distributed Computing: Concepts, Techniques, Applications and Case Studies. – 2019. – С. 207-220.

13 М. Искаков «Оценка рисков системы информационной Безопасности в государственном аппарате». 2022 С-34. //
https://repository.apa.kz/handle/123456789/1037

14 Қазақстан Республикасы Үкіметінің «Цифрлық Қазақстан» мемлекеттік бағдарламасын бекіту туралы» 2017 жылғы 12 желтоқсандағы № 827 қаулысы // https://adilet.zan.kz/kaz/docs/P1700000827

15 «Казахстан – страна цифрового будущего»: https://kazakh-tv.kz/ru/view/tech/page_204771_kazahstan-strana-tsifrovogo-budushchego

16 Қазақстан Республикасы Үкіметінің «Киберқауіпсіздік тұжырымдамасын («Қазақстанның киберқалқаны») бекіту туралы» 2017 жылғы 30 маусымдағы № 407 қаулысы // https://adilet.zan.kz/kaz/docs/P1700000407

17 https://baigenews.kz/kazahstan-podnyalsya-na-28-mesto-v-reytinge-razvitiya-elektronnogo-pravitelstva-oon_139304/

18 Қазақстан Республикасы Үкіметінің «Цифрландыру, ғылым және инновациялар есебінен технологиялық серпіліс» ұлттық жобасын бекіту туралы» 2021 жылғы 12 қазандағы № 727 қаулысы //
https://adilet.zan.kz/kaz/docs/P2100000727

19 ҚР ЦДИАӨМ Ақпараттық қауіпсіздік комитетінің ресми сайты //
https://www.gov.kz/memleket/entities/infsecurity?lang=ru

20 Клименко П., Клименко И., Цифровая экономика современного Казахстана: новые вызовы //Черноморская конференция-2019. – 2019. – С. 98-99.

21 Мусабаев, Р., Касымжанов, Б., Калиева, Г., & Ибраева, В., Разработка Информационных технологий и систем для стимулирования устойчивого развития личности как одна из основ развития Цифрового Казахстана //
Проблемы оптимизации сложных систем. – 2018. – С. 39-46.

22 Киберқауіпсіздік деңгейі бойынша елдердің рейтингі //
https://nonews.co/directory/lists/countries/cybersecurity-index

23 Аудиторское заключение ГК «ЦК» //
https://www.gov.kz/memleket/entities/esep/documents/details/320509?lang=ru

24 Услуги по обеспечению кибербезопасности / пер. Е. Харитонова //
Борьбас преступностью за рубежом: по материалам иностр. печ. — 2019. — № 9. — С. 37–40.

25 Қазақстанның мемлекеттік құрылымдарының IT-ландшафтын зерттеу қорытындылары //
https://bluescreen.kz/news/10393/itoghi-obsliedovaniia-it-landshafta-ghosstruktur-kazakhstana

26 Ақпараттық қауіпсіздік инциденттері //
https://cert.gov.kz/press_club/infographics

27 Қазақстан Республикасының «Ақпараттандыру туралы» Заңы 2015 жылғы 24 қарашадағы № 418-V ҚРЗ // https://adilet.zan.kz/kaz/docs/Z1500000418

28 Қазақстан Республикасының «Дербес деректер және оларды қорғау туралы» 2013 жылғы 21 мамырдағы № 94-V Заңы //
https://adilet.zan.kz/kaz/docs/Z1300000094

29 Қазақстан Республикасы Үкіметінің «Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарды бекіту туралы» 2016 жылғы 20 желтоқсандағы № 832 қаулысы // https://adilet.zan.kz/kaz/docs/P1600000832

30 Реализация казахстанской концепции кибербезопасности https://www.gov.kz/memleket/entities/infsecurity/press/news/details/409917?lang=ru

31 Услуги по обеспечению кибербезопасности / пер. Е. Харитонова // Борьбас преступностью за рубежом: по материалам иностр. печ. — 2019. — № 9. — С. 37–40.

32 Новый центр по обеспечению кибербезопасности в Австралии / пер.С. Велев // Борьба с преступностью за рубежом: по материалам иностр. печ. — 2019. — № 10. — С. 9.

33 Вопросы кибербезопасности в Бразилии / пер. С. Велев // Борьба с преступностью за рубежом: по материалам иностр. печ. — 2019. — № 3. — С. 11–14.

34 Классификация киберпреступности в КНР на основе внесенных судебных решений / пер. Е. Харитонова // Борьба с преступностью за рубежом: по материалам иностр. печ. — 2019. — № 8. — С. 33–46.

35 Құқықтық статистика // https://qamqor.gov.kz/crimestat/statistics

36 Электрондық коммерциядағы ақпараттық қауіптер // Ахметов А.Н // https://kazconf.com/files/archive/5375709.pdf

37 Депутаттық сауал // https://www.inform.kz/ru/uvelichit-zatraty-na-informbezopasnost-prizyvayut-deputaty_a3986960

38 Интернетте қанша қазақстандық бар және олар немесе айналысады // https://digitalbusiness.kz/2022-12-27/skolko-kazahstanczev-v-internete-i-chto-oni-tam-delayut-czifry-iz-issledovaniya-digital-rynka/

39 Концепция Киберщит Казахстана https://www.gov.kz/memleket/entities/infsecurity/press/news/details/409929?lang=ru