# Киберқауіпсіздік тұжырымдамасын ("Қазақстанның киберқалқаны") бекіту туралы

Қазақстан Республикасы Үкіметінің 2017 жылғы 30 маусымдағы № 407 қаулысы.

"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 **ҚАУЛЫ ЕТЕДІ:**

1. Қоса беріліп отырған Киберқауіпсіздік тұжырымдамасы ("Қазақстанның киберқалқаны") (бұдан әрі – Тұжырымдама) бекітілсін.

2. Қазақстан Республикасының орталық мемлекеттік органдары:

1) Тұжырымдаманы іске асыру жөніндегі қажетті шараларды қабылдасын;

2) жарты жылда бір рет, есепті жартыжылдықтан кейінгі айдың 10-ы күнінен кешіктірмей, Қазақстан Республикасының Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігіне Тұжырымдаманың іске асырылу барысы туралы ақпарат беріп тұрсын.

Ескерту. 2-тармаққа өзгеріс енгізілді - ҚР Үкіметінің 17.03.2023 № 236 (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) қаулысымен.

3. Қазақстан Республикасының Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігі:

1) үш ай мерзімде Тұжырымдаманы іске асыру жөніндегі іс-шаралар жоспарын әзірлесін және заңнамада белгіленген тәртіппен Қазақстан Республикасы Үкіметінің қарауына енгізсін;

2) жылына екі рет, 25 шілдеге және 25 қаңтарға қарай Қазақстан Республикасы Үкіметінің Аппаратына Тұжырымдаманың іске асырылу барысы туралы жиынтық ақпарат беріп тұрсын.

Ескерту. 3-тармаққа өзгеріс енгізілді - ҚР Үкіметінің 17.03.2023 № 236 (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) қаулысымен.

4. Осы қаулының орындалуын бақылау Қазақстан Республикасының Цифрлық даму , инновациялар және аэроғарыш өнеркәсібі министрлігіне жүктелсін.

Ескерту. 4-тармақ жаңа редакцияда - ҚР Үкіметінің 17.03.2023 № 236 (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) қаулысымен.

5. Осы қаулы қол қойылған күнінен бастап қолданысқа енгізіледі.

*Қазақстан Республикасының*

*Премьер-Министрі* *Б. Сағынтаев*

Қазақстан Республикасы
Үкіметінің
2017 жылғы 30 маусымдағы
№ 407 қаулысымен
бекітілген

# Киберқауіпсіздік ТҰЖЫРЫМДАМАСЫ

# ("Қазақстанның киберқалқаны")

Мазмұны



## 1. Кіріспе

Киберқауіпсіздік тұжырымдамасы ("Қазақстанның киберқалқаны") (бұдан әрі – Тұжырымдама) Қазақстанның әлемнің ең дамыған 30 мемлекетінің қатарына енуі бойынша "Қазақстан-2050" Стратегиясының тәсілдерін ескере отырып, Қазақстан Республикасы Президентінің "Қазақстанның үшінші жаңғыруы: жаһандық бәсекеге қабілеттілік" атты Жолдауына сәйкес әзірленді.

Тұжырымдама мемлекеттік органдарды ақпараттандыру, мемлекеттік көрсетілетін қызметтерді автоматтандыру, "цифрлы" экономиканы дамыту және өнеркәсіптегі өндірістік процестерді технологиялық жаңғырту перспективалары, ақпараттық-коммуникациялық қызметтер көрсету аясын кеңейту саласындағы ағымдағы ахуалды бағалауға негізделген.

Тұжырымдама электрондық ақпараттық ресурстарды, ақпараттық жүйелер мен телекоммуникация желілерін қорғау, ақпараттық-коммуникациялық технологияларды ( бұдан әрі – АКТ) қауіпсіз пайдалануды қамтамасыз ету саласындағы мемлекеттік саясатты іске асырудың негізгі бағыттарын белгілейді.

Тұжырымдама мемлекеттік органдардың, жеке және заңды тұлғалардың ақпараттық қауіпсіздікті қамтамасыз ету мониторингіне, сондай-ақ ақпараттық қауіпсіздік инциденттерін, оның ішінде әлеуметтік, табиғи және техногендік сипаттағы төтенше жағдайлар, төтенше немесе соғыс жағдайларын енгізу жағдайларында алдын алу және жедел ден қою тетіктерін жасау тәсілдерінің бірлігін қамтамасыз етуге арналған.

Тұжырымдаманы әзірлеу кезінде ақпараттық-коммуникациялық технологияларды әзірлеу және пайдалану саласындағы көшбастаушы мемлекеттердің, сол сияқты

әлеуметтік-экономикалық даму мақсаттарына жету үшін оларды қолдану саласын кеңейтуге ұмтылған елдердің ұлттық ақпараттық-коммуникациялық инфрақұрылымын қорғау тәсілдерін қалыптастыру саласындағы халықаралық тәжірибе зерделенді.

Осы Тұжырымдаманың орындалуы қазақстандық қоғамды одан әрі жаңғыртуға қызмет етеді және Қазақстанның БҰҰ-ның Киберқауіпсіздіктің жаһандық бағдарламасын іске асыруға қосқан үлесі болады.

**Терминдер мен анықтамалар**

Осы Тұжырымдаманың мақсаттары үшін киберқауіпсіздік бұл электрондық нысандағы ақпараттың және оның өңдеу, сақтау, беру (электрондық ақпараттық ресурстарды, ақпараттық жүйелер мен ақпараттық-коммуникациялық инфрақұрылымды) ортасының сыртқы және ішкі қауіп-қатерлерден қорғалу жағдайы, яғни ақпараттандыру саласындағы ақпараттық қауіпсіздік деп түсіндіріледі.

Ақпаратты немесе электрондық ақпараттық ресурстарды және ақпараттық жүйелерді қорғау – ақпараттық қауіпсіздікті қамтамасыз етуге бағытталған физикалық, техникалық, бағдарламалық, криптографиялық және әкімшілік шаралар кешені.

Ақпараттық қауіпсіздіктің классикалық үлгісі ақпараттың қауіпсіздігі үшін маңызды үш белгіні қамтамасыз етуге негізделеді: құпиялық, тұтастық және қолжетімділік.

Ақпараттың құпиялығы онымен өзінің иесі белгілеген қатаң шектелген адамдар тобы ғана таныса алады дегенді білдіреді.

Егер ақпаратқа қолжетімділікті уәкілеттілігі жоқ адам алатын болса, рұқсат етілмеген қолжетімділікке немесе құпиялықтың бұзылуына жол беріледі.

Заң немесе иесі қорғайтын ақпараттың кейбір түрлері үшін құпиялық ең маңызды белгілерінің (қызметтік ақпарат, заңмен қорғалатын құпиялар түрлері, қолжетімділігі шектеулі жеке деректер, мысалы, банктің клиенттері, кредиторлары туралы мәліметтер, салықтық деректер, медицина мекемелерінің пациенттердің денсаулық жағдайы туралы мәліметтері және т.б.) бірі болып табылады.

Ақпараттың тұтастығы – ақпараттың (деректердің) бұрмаланбаған түрде сақталу қабілеті. Ақпараттың заңсыз және иесі көздемеген өзгеруі (оператор қатесінің немесе уәкілеттігі жоқ адамның қасақана іс-әрекетінің нәтижесінде) тұтастықтың бұзылуына алып келеді.

Әсіресе аса маңызды ақпараттық-коммуникациялық инфрақұрылым объектілерінің жұмыс істеуімен байланысты деректердің тұтастығы ерекше маңызды (мысалы, әуе қозғалысын, электрмен және энергиямен жабдықтауды басқарудың автоматтандырылған жүйелері және т.б.).

Ақпараттың қолжетімділігі ақпараттық жүйенің тиісті өкілеттіктері бар субъектілерге ақпаратқа дер кезінде бөгетсіз рұқсат беру қабілетімен анықталады. Ақпаратты жою немесе бұғаттау (қателіктің немесе қасақана іс-әрекеттің нәтижесінде) қолжетімділіктің жойылуына алып келеді.

Қолжетімділік – ақпараттық-коммуникациялық қызметтерді беру (теміржол және авиациялық билеттерді сатудың, банктік қызметтердің ақпараттық жүйелері, интернетте өнімдерді интернет-ресурстармен және электрондық БАҚ-пен тарату) жолымен клиенттерге қызмет көрсетуге бағытталған ақпараттық жүйелердің жұмыс істеуі үшін маңызды белгі. Уәкілетті пайдаланушы белгілі бір қызметтерге (көбінесе желілік) рұқсат ала алмайтын жағдайды қызмет көрсетуден бас тарту деп атайды.

Коммуникациялық (желілік) технологиялардың дамуына байланысты ақпараттық жүйені немесе басқарушы электрондық ақпараттық ресурсты алыстан пайдаланушы адамның жеке басына байланысты ақпараттық қауіпсіздіктің қосымша тағы екі ерекшелігін бөліп көрсетеді: аутенттілік және дәлелдегіштік.

Аутенттілігі – ақпараттық-коммуникациялық қызметтер көрсету саласында ақпаратқа немесе хабарға қатысты заңдық тұрғыдан маңызды іс-әрекеттің авторын дұрыс анықтау мүмкіндігі, мысалы, электрондық коммерцияда электрондық-цифрлық қолтаңба немесе түпнұсқаландырудың өзге тәсілі пайдаланылған кезде.

Дәлелдегіштік (бастартпаушылық) – авторлықтан бас тартқан кезде жасалған іс-әрекеттерді тіркеу жолымен ақпараттық жүйедегі немесе ресурстағы ақпаратқа қатысты іс-әрекет жасаған автор басқа ешкім емес, осы пайдаланушы болып табылатындығын дәлелдеу мүмкіндігі.

Түпнұсқаландыру (түпнұсқаға сәйкестігін анықтау) – қолжетімділік субъектісі көрсеткен сәйкестендіргіштің оған тиесілігін тексеру және оның түпнұсқаға сәйкестігін растау.

Сәйкестендіру – қолжетімділік субъектілеріне ақпараттық жүйеге рұқсат беру кезінде субъектінің сәйкестігін анықтауды және өкілеттіктерін белгілеуді қамтамасыз ететін жеке сәйкестендіргіштің ақпараттық жүйесіне немесе электрондық ресурсына қолжетімділік беру, жұмыс сеансы процесіндегі өкілеттіктерді бақылау және іс-әрекеттерді тіркеу.

Сәйкестендіру мен түпнұсқаландыру қазіргі заманғы бағдарламалық-техникалық құралдар қауіпсіздігінің негізі, өйткені кез келген АКТ-қызметтер мен сервистер, негізінен, пайдаланушы субъектілерге қызмет көрсетуге есептелген.

Ақпараттық қауіпсіздік қауіп-қатері – әбден болуы мүмкін оқиға, процесс немесе құбылыс, ол ақпаратқа немесе ақпараттық жүйенің немесе ресурстың компоненттеріне әсер ету арқылы иеленушілер мен пайдаланушылардың мүдделеріне тікелей немесе жанама зиян келтіруге әкеліп соқтыруы мүмкін.

Ақпараттық қауіпсіздіктің барынша көп таралған қауіп-қатерлері – бұл жабдықтың (кабельдік жүйенің, дискілік жүйелердің, серверлердің, жұмыс станцияларының және тағы басқалардың) іркілісі, архивтік деректердің дұрыс сақталмауы, деректерге қолжетімділік құқықтарының бұзылуы), пайдаланушылар мен қызмет көрсетуші

жұмыскерлер құрамының жөнсіз жұмысы, ақпараттың жоғалуы (рұқсат етілмеген қолжетімділіктен немесе зиян келтіретін бағдарламалармен – компьютерлік вирустармен бүлінуден).

Компьютерлік атака – ақпаратқа, электрондық ресурсқа, ақпараттық жүйеге рұқсатсыз әсер ету немесе оларға бағдарламалық немесе бағдарламалық-ақпараттық құралдарды (немесе желілік өзара іс-әрекеттердің хаттамаларын) қолдана отырып қолжетімділік алу арқылы қауіп-қатер төндіруді іске асырудың мақсатты әрекеті.

Барлық өзге терминдер Қазақстан Республикасының Конституциясында, Қазақстан Республикасының Қылмыстық кодексінде, "Әкімшілік құқық бұзушылық туралы" Қазақстан Республикасының кодексінде, "Қазақстан Республикасының ұлттық қауіпсіздігі туралы", "Мемлекеттік құпиялар туралы", "Терроризмге қарсы іс-қимыл туралы", "Электрондық құжат және электрондық цифрлық қолтаңба туралы", " Ақпараттандыру туралы", "Техникалық реттеу туралы", "Рұқсаттар мен хабарламалар туралы", "Бұқаралық ақпарат құралдары туралы", "Байланыс туралы", "Жеке деректер және оларды қорғау туралы", "Ақпаратқа қолжетімділік туралы" Қазақстан Республикасының заңдарында және ұлттық техникалық стандарттарда пайдаланылатын мағыналарда келтірілген.

## 2. Ағымдағы ахуалды талдау

Соңғы онжылдықтарға тән ақпараттық-коммуникациялық технологиялар жетістіктерін енгізудің жалпы әлемдік үрдісі "ақпараттық қоғам" үшін қоғамдық және өндірістік қарым-қатынастарды пайдаланудың және нығайтудың мәдениетін қалыптастыру қарқынынан елеулі басымдыққа ие болып, киберқауіпсіздікті қамтамасыз ету бірінші кезектегі мәселеге айналуына байланысты бұл Қазақстанда да қолдауға ие болып отыр.

Дегенмен "Ұлттық ақпараттық инфрақұрылымды, ақпараттандыру процестерін қалыптастыру мен дамыту және ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі жұмыстарды үйлестіру туралы" Қазақстан Республикасы Үкіметінің 1998 жылғы 31 желтоқсандағы № 1384 қаулысы қабылданған 1998 жылдан бері "Ақпараттандыру туралы" Қазақстан Республикасы заңдарының 3 жаңа редакциясы (2003, 2007, 2015 жылдары) және оларға ақпараттарды (деректерді) берудің электрондық форматтары мәселелері бойынша, оның ішінде ақпараттық-коммуникациялық желілер, " электрондық үкімет" мәселелері бойынша тиісті өзгерістер енгізу туралы Қазақстан Республикасының бірнеше мамандандырылған заңдары қабылданды.

Өткен кезеңде электрондық ақпараттық ресурстар және ақпараттық жүйелер мүліктік активтердің басқа түрлерімен бірге шаруашылық айналымға енгізілді, оларды нарықтық пайдалану саласы кеңейді.

Мемлекеттік көрсетілетін қызметтерді автоматтандыру саласы, электрондық коммерция мен электрондық төлемдер нарығы ақпараттық-коммуникациялық

технологияларды қолдану кезінде жеке адамның, қоғамның және мемлекеттің қауіпсіздігін қамтамасыз ету, сондай-ақ ақпараттандыру және байланыс объектілерінің сенімділігі мен басқарылуын қамтамасыз ететін бірыңғай стандарттар негізінде қызметті жүзеге асыру қағидаттарында дамуда.

Ақпараттық қауіпсіздік мәселелері қалыптасқан кезеңнен бастап бар ақпараттың сипатын ескере отырып, көпшілікке қолжетімді және құпия электрондық ақпараттық ресурстар мен жүйелердің құқықтық режимдері сараланды, меншік иелерінің, оларды қорғау жөніндегі иеленушілер мен пайдаланушылардың құқықтары мен міндеттері белгіленді.

Мемлекеттік органдар және ақпараттандыру мен байланыс саласындағы ақпараттық қауіпсіздікті қамтамасыз ету бойынша басқа да субъектілердің қызметі олардың салалық құзыретіне, сондай-ақ АКТ пайдаланумен байланысты нысаналы салалардағы (байланысты және ақпараттық технологияларды реттеу, жеке деректерді қорғау, мемлекеттік құпияларды қорғау, шетелдік техникалық барлау қызметіне қарсы іс-қимыл, байланыс желілеріндегі жедел-іздестіру қызметі, АКТ пайдалану арқылы жасалатын қылмыстарды тергеу және басқалары) мақсаттары мен міндеттеріне сәйкес жүзеге асырылады.

Тұтастай алғанда, Қазақстан Республикасында ақпараттандыру мен байланыс саласындағы ақпараттық қауіпсіздікті (киберқауіпсіздікті) қамтамасыз ету бойынша шаралар жүйесінің ұйымдастыру-құқықтық және техникалық негіздері "Ұлттық қауіпсіздік туралы" Қазақстан Республикасының Заңына сәйкес ақпараттық қауіпсіздіктің және ақпараттық кеңістік пен байланыс инфрақұрылымының қауіпсіздігін қамтамасыз етудің құрамдас бөліктері ретінде заңнамалық түрде бекітілді.

Соңғы жылдары ақпараттандыру мен байланыс саласындағы ақпараттық қауіпсіздікті қамтамасыз етудің түрлі өзара байланысты аспектілері Қазақстан Республикасының Қылмыстық кодексінде, "Әкімшілік құқық бұзушылық туралы" Қазақстан Республикасының Кодексінде, "Мемлекеттік құпиялар туралы", "Жеке деректер және оларды қорғау туралы", "Электрондық құжат және электрондық цифрлық қолтаңба туралы", "Байланыс туралы" Қазақстан Республикасының заңдарында және 2016 жылғы 1 қаңтардан бастап күшіне енген "Ақпараттандыру туралы" Қазақстан Республикасы Заңының жаңа редакциясын іске асыру үшін әзірленген заңға тәуелді бірқатар актілерде көрініс тапқан.

Соңғы кезде қабылданған заңға тәуелді бірқатар заңнамалық актілердің құқық қолдану тәжірибесі әлі өріс алған жоқ. Атап айтқанда, ұлттық және үйлестірілген стандарттардың құқықтық және техникалық нормаларын кодификациялауды білдіретін "Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарды бекіту туралы" (бұдан әрі – Бірыңғай талаптар) Қазақстан Республикасы Үкіметтің 2016 жылғы 20 желтоқсандағы қаулысы. Құжат заңмен қорғалатын ақпарат түрлерін өңдеу кезінде

ақпараттық-коммуникациялық технологияларды пайдалану бойынша рәсімдер мен қағидаларды егжей-тегжейлі сипаттайды, ақпараттық инфрақұрылымның, ақпараттық жүйелер мен ресурстардың, бағдарламалық жасақтаманың, техникалық құралдардың әрекет ету циклінің барлық кезеңдеріндегі технологиялық қауіпсіздігін қамтамасыз ету бойынша маңызды нормалардан тұрады.

Мемлекеттік, сонымен қатар мемлекеттік жүйелермен интеграцияланатын мемлекеттік емес ақпараттық жүйелерді қамтитын "электрондық үкіметтің" ақпараттандыру объектілерінің ақпараттық қауіпсіздігін қамтамасыз ету мониторингі жүйесінің жұмыс істеуі заңнамалық деңгейде реттелген.

Қазақстан Республикасы Инвестициялар және даму министрінің міндетін атқарушының 2016 жылғы 26 қаңтардағы № 66 бұйрығымен бекітілген Ақпараттық қауіпсіздікті, "электрондық үкіметтің" ақпараттандыру объектілерін қорғау және оның қауіпсіз жұмыс істеуін қамтамасыз ету мониторингін жүргізу қағидаларында технологиялық іркілістер немесе компьютерлік атакалар белгілері, сондай-ақ туындаған оқиғалар мен ақпараттық қауіпсіздік инциденттеріне ден қою алгоритмдері кезінде мүдделі тараптар арасындағы өзара іс-қимылдың негізгі қағидаттары көрсетілген.

"Электрондық үкіметтің" қауіпсіздік мониторингі орталығы күн сайын жойылмаған осалдықтарды анықтайды, шараларды қабылдау үшін бұл туралы оның компоненттері болып табылатын ақпараттық жүйелердің иелеріне хабарламалар жібереді. Анықталған осалдықтардың және оларға қатысты қабылданған шаралардың оң серпіні бар. Мысалы , 2014 жылы 1241 жойылмаған осалдық анықталды, 2015-те – 469, 2016-да – 355.

Сондай-ақ Қазақстан Республикасы Үкіметінің 2016 жылғы 8 қыркүйектегі № 529 қаулысымен ерекше маңызды мемлекеттік және стратегиялық объектілер, сондай-ақ стратегиялық маңызы бар экономика саласының объектілері қатарынан Ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілеріне жатқызу қағидалары мен өлшемшарттары бекітілді.

Ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілері тізбесіне кірген осындай объектілерге Бірыңғай талаптар қолданылады, сондай-ақ олар заңнамада көзделген ақпараттық қауіпсіздік инциденттері туралы хабарлау міндетін қоса алғанда, олардың ақпараттық қауіпсіздігі, қорғалуы және қауіпсіз жұмыс істеуі мониторингін қамтамасыз ету бойынша бірлескен шараларға қатысуы қажет.

Ақпараттық жүйелерді өнеркәсіптік пайдалануға кіргізу рәсімі жетілдірілуде. Осыған байланысты ақпараттық жүйелерге олардың белгілі бір сынаққа жататындығына қарай қауіпсіздік шаралары заңнамалық түрде сараланды, ақпараттық жүйенің тәжірибелік пайдалану режимінде болу мерзімі шектелді.

Ақпараттық қауіпсіздік талаптарына сәйкестік тұрғысынан мемлекеттік және мемлекеттік жүйемен интеграцияланатын мемлекеттік емес ақпараттық жүйелерде 500-ден астам аттестациялық зерттеулер жүргізілді, олардың нәтижелері бойынша

өндірістік пайдалануға енгізу үшін негіз болып табылатын 199 аттестат берілді. Ақпараттық жүйелердің қалған бөлігі "Ақпараттандыру туралы" Қазақстан Республикасының Заңына сәйкес 2018 жылдың соңына дейін аттестаттаудан өтуге міндетті.

2016 жылғы 1 қаңтардан бастап мемлекеттік органдардың ақпараттық жүйелері, мемлекеттік ақпараттық жүйелермен интеграцияланатын мемлекеттік емес ақпараттық жүйелер тәжірибелік пайдалану кезеңінде ақпараттық қауіпсіздік талаптарына сәйкестігі тұрғысынан сынақтан өтеді. Сынақ кезінде шығыс кодтар, қауіпсіздік функцияларының теңшеуі тексеріледі, желілік және серверлік жабдықтар зерттеледі және жүктеме тестілеу жүзеге асырылады.

Сынақты өткізу нәтижелері ақпараттық жүйелердің қорғалуының және істен шығудан беріктігінің артуы, ақпараттық жүйелердің бағдарламалық жасақтаманың қауіпсіздігі, ақпараттық жүйелердің ақпараттық қауіпсіздігінің бұзылу факторлары ықпалының төмендеуі, ақпараттық жүйелердің қауіпсіздігін бақылау және мониторинг тетіктерін енгізу арқылы көрінеді.

Техникалық реттеу жүйесі бағдарламалық жасақтама мен телекоммуникациялық жабдықтың, соның ішінде олардың мемлекеттік секторда пайдаланылуы кезінде міндетті түрде сертификатталу жағдайларын айқындаумен сәйкес келуін растауды көздейді. Осы мақсаттарда жыл сайын ақпараттық қауіпсіздік, ақпаратты қорғау, ақпараттық технологиялардың қауіпсіздігі саласындағы ұлттық және үйлесімді техникалық стандарттар жиынтығы өзектілендіріледі. Қазіргі уақытта 68 техникалық стандарт бар.

Мемлекеттік органдардың интернетке қолжетімділіктің бірыңғай шлюзі арқылы интернетке қосылуын орталықтандырудың арқасында рұқсатсыз қолжетімділік қаупі және мемлекеттік органдардың электрондық ақпараттық ресурстарына зиян келтіретін ықпалдар айтарлықтай төмендеді. Күн сайын әртүрлі деңгейдегі 180 миллионнан астам атака тіркеліп, оларға тойтарыс беріледі.

Есептеу техникасының құралдарын пайдалана отырып өңделетін мемлекеттік құпиялардың құқықтық, ұйымдық, техникалық және криптографиялық шараларының жүйесі құрылып, жетілдірілуде.

Мемлекеттің қауіпсіздігі үшін неғұрлым сезімтал электрондық нысандағы ақпарат интернеттен бөлектенген және ақпаратты қорғаудың криптографиялық құралдарын пайдаланатын арнайы мақсаттағы телекоммуникация желілері арқылы ғана жіберіледі.

Жалпы пайдаланатын байланыс және телекоммуникациялар желілері инфрақұрылымының қауіпсіздігін қамтамасыз ету тәсілдері шекаралық жабдықта " электрондық шекара" тұжырымдамасын іске асыратын магистральдық байланыс операторларының мүмкіндіктері арқылы телекоммуникациялар желілерін орталықтан басқару жүйесінің айналасына тізіледі.

Интернеттің ұлттық сегменті заңнамаға сәйкес Қазақстан Республикасының аумағында орналастырылатын .KZ және .ҚАЗ домендеріндегі 120 мыңнан астам интернет-ресурсты құрайды. Ақпараттық ресурстар мен жүйелердің иелері мен пайдаланушыларына АТК-ны қауіпсіз пайдалану мәселелері бойынша жәрдемдеу мақсатында 2010 жылдан бастап KZ-CERT Компьютерлік инциденттерге ықпал ету ұлттық қызметі жұмыс істейді. Қызмет бірқатар халықаралық ұйымдардың қатысушысы болып табылады, соның ішінде FIRST (Forum of Incident Responseand Security Teams), TI (Trusted Introducer for Security and Incident Response Teams), OIC-CERT (Компьютерлік инцидиенттерге ден қою қызметінің исламдық өзара іс-қимыл ұйымы).

Қызмет шет елдердің бейіндік құрылымдарымен өзара түсіністік және ынтымақтастық туралы 20 меморандум жасап, ақпараттық қауіпсіздік инциденттерінің 66000-нан астамын тіркеді және өңдеді.

Қазақстандық нарықта ақпараттық қауіпсіздік талаптарына сәйкестігі тұрғысынан қорғалуын бағалау бойынша (енуді тестілеу арқылы) аспаптық аудитпен айналысатын және ақпараттық қауіпсіздік инциденттерінің мән-жайын, себептері мен жағдайларын зерттеуге, сондай-ақ зиянды бағдарламалық жасақтаманы техникалық зерделеуге мамандандырылған алғашқы отандық компаниялар пайда болды. Вирусқа қарсы алғашқы отандық құралдар әзірленді.

Бірнеше ұлттық компанияда және жеке құрылымдарда техникалық оқиғалар мен технологиялық процестердің мониторингісін жүргізетін бөлімшелер бар, олар штаттан тыс жағдайларға шұғыл ден қою үшін тәулік бойы кезекшілік жүргізеді.

Азаматтардың дербес деректерін электрондық түрде жинау, өңдеу мақсаттары, сондай-ақ оларды қорғау тәртібі мен шаралары заңнамалық тұрғыдан айқындалды. Заңнамада оларды тек азаматтардың келісімімен ғана жинау, сондай-ақ операторлардың олардың талабы бойынша дербес деректерді жою рәсімдері, сондай-ақ дербес деректерді ел аумағында қауіпсіз сақтау және трансшекаралық беру жағдайлары регламенттеледі.

Банктік ақпараттық жүйелердің қауіпсіздігі бойынша талаптар ақпараттық жүйелердің қауіпсіздігін қамтамасыз ету жөніндегі салалық және халықаралық талаптарды ескере отырып, Қазақстан Республикасы Ұлттық Банкінің нормативтік-құқықтық актілерімен қамтамасыз етіледі.

2014 жылдан бері қолданыстағы Қазақстан Республикасы Қылмыстық кодексінің жаңа редакциясында ақпарат және байланыс саласында жасалатын қылмыстарға арналған жеке тарау көзделген. Саралау мән-жайларын ескере отырып, онда электрондық ақпараттық ресурстар мен жүйелерге немесе телекоммуникациялар желілеріне қарсы қылмыстардың 38 құрамы қамтылған.

"Әкімшілік құқық бұзушылық туралы" Қазақстан Республикасының Кодексінде жасалғаны үшін әкімшілік жауапкершілік шаралары көзделген, соның ішінде

электрондық ақпараттық ресурстарды қорғау құралдарын пайдалану жөніндегі талаптарды бұзу, Бірыңғай талаптарды орындамау, дербес деректерден тұратын ақпараттық жүйелердің меншік иесінің немесе иесінің оларды қорғау бойынша шараларды жүзеге асырмауы не тиісті жүзеге асырмауы түріндегі ақпараттық қауіпсіздікті қамтамасыз ету бойынша міндеттерді орындамайтын лауазымды адамдар үшін бірқатар әкімшілік құқық бұзушылықтар құрамдары қамтылған.

Бүгінде "Ақпараттық қауіпсіздік жүйелері" мамандығының оқу жоспарларына қолданбалы пәндерді оқудан басқа, қауіпсіздіктің интеграцияланған жүйелерінде пайдаланылатын микропроцессорлық жүйелер мен құрылғыларды қолданбалы бағдарламалау, радиоэлектрондық құрылғыларды автоматтандырылған түрде жобалау мен әзірлеу бойынша білімдер мен қабілеттерді қалыптастыратын пәндер қосылған.

Елдің жетекші техникалық жоғары оқу орындарында мынадай пәндер оқытылады: " Қолданбалы инженерлік бағдарламалар", "Микропроцессорлар мен микропроцессорлық жүйелер", "Бағдарламалау және құрамдас жүйелерді іске асыру".

Талдамалық зерттеулер, ғылыми-зерттеу және тәжірибелік-конструкторлық жұмыстар жүргізу, бейіндік конференциялар мен семинарларды ұйымдастыру тәжірибесі қалыптасуда, бұл қоғамның, ғылыми ортаның және ақпараттандыру субъектілерінің ақпараттық қауіпсіздік саласындағы түрлі аспектілерге деген қызығушылығының артқанын көрсетеді.

Халықаралық электр байланыс одағы өткізген 195 елдің құқықтық, техникалық, ұйымдастырушылық даярлығы мен әлеуетін бағалайтын "Киберқауіпсіздіктің жаһандық индексі" зерттеуі (бұдан әрі – Киберқауіпсіздіктің жаһандық индексі) Қазақстанның 29 ел ішінде 0,176 индексімен 23 топтық орнын белгіледі.

**Негізгі проблемалар**

1. Қазақстан Республикасында 2010 жылдан бастап 2016 жылға дейінгі кезеңде интернетті пайдаланушылар тығыздығы 36,1%-дан 75%-ға дейін өсті, ал мобильді интернетті пайдаланушылардың саны 3 миллион 694 мыңнан үш еселеніп 10 миллион 567 мыңға жетті. Интернет пайдаланушылар санының мұндай экспоненциалдық ұлғаюы маңыздылықты арттырып, істен шыққан немесе техникалық құралдарға зиян келтірілген жағдайларда олардың салдарын неғұрлым елеулі етеді.

Дербес компьютерлер мен ұялы құрылғылар үшін зиян келтіретін бағдарламалардың таратылуы оларды пайдаланушылардың санымен қатар өсуде. Бұл ретте пайдаланушылардың басым көпшілігі өздерінің дербес компьютерлерін, смартфондарын, планшеттерін қорғау үшін мамандандырылған бағдарламалық жасақтамаларды пайдаланбайды.

Аталған факторды "хакерлер" пайдалануда, бұл абоненттік құрылғыларды зиян келтіретін бағдарламалық жасақтамамен зақымдауға бағытталған атакалар санының күн сайын ұлғаюына әкеп соқтырады.

Интернетке қосылған абоненттік құрылғылар саны ұлғайған сайын және пайдаланушылардың көбі өзіне және өздеріне тиесілі құрылғыларға қатысты "цифрлық гигиена" шараларын елемеуді жалғастырған сайын, "Интернет заттары" тұжырымдамасы олардың қауіпсіз пайдалану проблемасын күшейте түседі.

Егер дербес компьютерлер мен ноутбуктер сияқты электрондық құрылғылардың вирусқа қарсы бағдарламалық жасақтаманы орнату және жаңарту бойынша мүмкіндігі болса, ал "Интернет заттарын" пайдаланушылар олардың жұмыс істеуін қалай қауіпсіз ету қажеттігін жиі біле бермейді.

Мұндай құрылғылар, әлі де болса, технологиялық тәуекелдер ескерілмей жасалады, бұл оларды ақпараттық желілерге қолжетімділіктен айырылуға бағытталған және адал пайдаланушыларға ақпараттық-коммуникациялық қызметтерді көрсету кезінде қызмет көрсетуден бас тартылуына әкеп соқтыратын әртүрлі желілік атакалар жүзеге асыру үшін пайдаланылатын зиян келтіргіш желілердің ("ботнеттердің") ықтимал элементтері етеді.

Интернет-ресурстар мен әлеуметтік желілерді пайдалану кезінде қауіпсіздік жағын елемеу жеке өмірдің қол сұғылмаушылығы үшін жоғары тәуекелге, көпшілікке қолжетімді дербес деректерді рұқсатсыз пайдалануға немесе модификациялауға, сондай-ақ қолжетімділігі шектеулі дербес деректердің жария болуына немесе олардың қылмыстық қоғамдастықтар немесе олар басқа мемлекеттердің аумағында сақталған кезде барлау құрылымдары үшін эксаумақтық қолжетімділігіне әкеледі.

Ақпараттық қауіпсіздік мәселелері бойынша құқықтық сауаттылықтың төмен болуы және тұрғындардың, АКТ саласы қызметкерлерінің және ұйымдар басшыларының арасында оны арттыруға қалыптасқан қажеттілігінің болмауы ақпараттық салада құқық бұзушылықтар мен қылмыстардың дамуы үшін жарамды негіз туғызады.

Құқықтық шектеулер туралы білімнің болмауы басқа азаматтардың құқықтары мен бостандықтарын, авторлық және сабақтас құқықтарды иеленушілердің ақпараттық жасақтамаға құқықтарын бұзатын және ақпараттық ресурстардың жұмыс істеуіне әсер ететін әрекеттерді жасауға болады деген иллюзия туғызады.

Осылайша, соңғы пайдаланушылардың зиян келтіретін компьютерлік бағдарламаларды және бағдарламалық өнімдерді (әсіресе жасанды интернет-дүкендер мен банктердің "фишинг" парақтарын, "бұзылған" сайттар арқылы вирустық және " трояндық" бағдарламаларды тарату, лицензиялық емес ("пираттық" бағдарламалық жасақтамамен) көшірудің жалпы әдістері бойынша негізгі білімдері болмаған кезде дербес деректерді қорғау мәселелерінде цифрлық сауаттылығының төменгі деңгейі Қазақстан Республикасы азаматтарының құрбан болған, ал оларға тиесілі техникалық құралдардың АКТ-ны заңсыз пайдалану құралына айналған мыңдаған жағдайларға әкеледі.

2. Ақпаратты қорғау әдістерінен жеткілікті хабардар болмау, шағын және орта бизнес кәсіпорындарының, оның ішінде көп жағдайда өздеріне тиесілі ақпараттық-коммуникациялық инфрақұрылымның жай-күйін бағалай алмайтын ақпараттық-коммуникациялық қызметтер көрсету саласында жұмыс істейтін кәсіпорындардың ақпараттық қауіпсіздігі жүйелерінің төмен қамтамасыз етілуі, ақпараттық қауіпсіздіктің талдауға келмейтін оқиғалары мен инциденттерінің көп болуына әкеледі, олар технологиялық осалдықтардың алдын алуды, сонымен қатар АКТ-ны қылмыстар жасау үшін құрал ретінде пайдаланатын қылмыскерлермен күресті қиындатады.

Бұдан басқа, мұндай шаруашылық субъектілері басқалары үшін, бірінші кезекте, әріптестер немесе мердігерлер ретінде жұмыс істейтін ірі кәсіпорындар немесе мемлекеттік органдар мен ұйымдар үшін қауіп төндіреді.

Бұл ретте ірі жеке меншік және қаржы секторы бірлескен күштер мен операциялық қызметтің шынайы қауіпсіз ортасын қалыптастыру жөніндегі салалық бастамалардың маңыздылығын бағаламай, тек өз күшіне сенуге бейім.

Сонымен қатар жұмыс берушілер мүдделілігінің төмендігі мен кәсіптік бәсекелестіктің болмауы ақпараттық қауіпсіздік саласында жұмыс істейтін мамандардың өздерінің бастамашылығын дамытуға ынталандырмайтын фактор болып табылады, сондай-ақ аталған адамдардың қызметтің заңсыз түрлерімен айналысуы үшін алғышарттар жасайды.

3. Ақпараттық қауіпсіздік саласындағы мамандануды қоса алғанда, АКТ саласындағы мектеп, орта арнайы, жоғары және жоғары оқу орнынан кейінгі білімнің қолданыстағы қазақстандық моделі, осы саланың серпінді дамуына байланысты қоғамның қазіргі заманғы талаптарына және ақпараттық технологиялардың қауіпсіз дамуын қамтамасыз ету үрдісіне сәйкестігі тұрғысынан барлық мүдделі тұлғалар ( Қазақстан Республикасының Білім және ғылым министрлігі, жоғары оқу орындары және өнеркәсіп) тарапынан үнемі және мұқият талдауды талап етеді.

Атап айтқанда, білім беру және кәсіптік стандарттар, мамандықтар сыныптауыштары, пәндер, олардың контенттік мазмұны мен оқыту нәтижелері мерзімді қайта қарауды талап етеді. АКТ саласындағы қазіргі заманғы сын-қатерлерге неғұрлым икемді ден қоюға мүмкіндік беретін тетікті әзірлеу қажеттілігі туындайды. Бұл саладағы білімнің тез ескіретініне байланысты мамандардың біліктілігін мерзімді растап отыру талап етіледі.

АКТ саласында мамандар дайындайтын 93 жоғары оқу орнының ішінен тек қана 7-еуі "Ақпараттық қауіпсіздік жүйелері" мамандығы бойынша мамандар даярлайды. 2015 – 2016 жылдары оқыған 32439 студенттің ішінде көрсетілген жоғары оқу орындарында тек 362-сі (1,1 %-ы) ғана "Ақпараттық қауіпсіздік жүйелері" мамандығы бойынша, олардың ішінде мемлекеттік тапсырыс бойынша 226 адам оқыды. 2016 жылы жоспарлы шығару 85 түлекті құрады.

2016 – 2017 оқу жылында "Ақпараттық қауіпсіздік жүйелері" мамандығы бойынша мамандар даярлауға мемлекеттік тапсырыс бойынша 40 орын, 2014 – 2015 оқу жылында – 60 орын, 2015 – 2016 оқу жылында – 60 орын бөлінді.

Осыған байланысты, "Ақпараттық қауіпсіздік жүйелері" мамандығы бойынша кәсіптік бағдарлау жұмысына аса көңіл бөлінеді, оның ішінде талапкерлердің назары осы мамандықтың өзектілігіне, осы бейіндегі мамандардың индустрияға қажеттілігіне аударылады.

Талапкерлерді "Ақпараттық қауіпсіздік жүйелері" мамандығына коммерциялық негізде оқуға қабылдау жеткілікті ілгерілемейді және жарнамаланбайды. Арнайы пәндер түлектердің оқуды аяқтағаннан кейін арнайы мемлекеттік органдарда қолдану үшін қажетті толықтырылмайды.

Оқу бағдарламаларында "Атамекен" ұлттық кәсіпкерлер палатасы бекіткен және біліктіліктің салалық шеңберіне негізделген "Ақпараттық қауіпсіздік жөніндегі маман" кәсіптік стандартының білімдеріне, қабілеттері мен дағдыларына қойылатын талаптар ескерілмеген.

Соның салдарынан мемлекеттік, сондай-ақ жеке меншік секторда АКТ саласында ақпараттық қауіпсіздік жөніндегі мамандардың жетіспеушілігі бар. Айталық, орталық мемлекеттік органдарда қамтамасыз етілу 25 %-ды, жергілікті органдарда – 6 %-ды құрайды.

4. IT-саланың отандық секторы ұлттық экономиканы әртараптандыру бағдарламасына айтарлықтай үлес қоспайды (мемлекеттік секторда пайдаланылатын өнімдердің 5 пайызынан кемі қазақстандық өнім), ал киберқауіпсіздік мәдениеті, соның ішінде өнімдерді әзірлеу мен пайдалану саласындағы өндірістік мәдениет үнемі анықтағыш бола бермейді.

Қорғаныс пен қауіпсіздікті қоса алғанда, мемлекеттік басқару саласындағы ақпараттандырудың қол жеткізілген жоғары деңгейіне қарамастан, жеке адам мен қоғам өмірінің әртүрлі салаларында АКТ-ны кеңінен пайдалануда Қазақстан, ел ретінде , әлі де болса тек IT-технологияларды ғана емес, ақпараттандыру және байланыс саласында ақпараттық қауіпсіздікті қамтамасыз ету өнімдерін қоса алғанда, дайын бағдарламалық өнімдерді де айтарлықтай шамада импорттайды (шеттен алады), бұл бір жағынан, IT-индустриясы алыптарының қысымын көрсетсе, ал екінші жағынан олардың әсерінен мемлекет қауіпсіздігін қамтамасыз ету байланысты болатын әзірленімдердің аса маңызды салаларында өз күштеріне сүйене отырып, олардың тиімді орналасуы бойынша қабылданатын күштер мен шаралардың жеткіліксіз екенін көрсетеді.

5. Мемлекеттік функцияларды автоматтандыруға және мемлекеттік қызметтерді электрондық нысанда көрсетуге байланысты шаралар, сондай-ақ мемлекеттік органдардың қызметі туралы ақпаратқа қолжетімділікті цифрландырудың одан әрі жалғасуы белгілі бір тәуекелді тудырады.

Азаматтар мен жеке ұйымдарға "электрондық үкімет" шеңберінде көрсетілетін сапасыз қызметтер мен қосымшалар, соның ішінде машинамен оқылатын ашық деректер азаматтардың құқықтары мен заңды мүдделерінің бұзылуына әкеп соқтыруы мүмкін.

Өндірістік және пайдалану мәдениеті деңгейінің төмендігінен туындаған техникалық стандарттардың белгіленген талаптарынан ауытқу, тапсырыс берушілер мен шешімдерді әзірлеушілердің тарапынан жасау деңгейінде жол берілген ұқыпсыздық пен немқұрайлылық, ақпараттық жүйелерді ақпаратты қорғау және қорғалуын бақылау жүйелерімен қамтамасыз етуді қалдықпен қаржыландыру қағидаты технологиялық іркілістердің жоғары тәуекелдеріне әкеледі.

Ақпараттық жүйелер иелерінің бағдарламалық жасақтамадағы осалдықтарды дер кезінде жоймағаны заңсыз қолжетімділік қаупін айтарлықтай ұлғайтады.

Мемлекеттік және жеке меншік секторларда өңделетін деректердің көлемі өсуде, бұл оларды сақтаудың жаңа нысандарын әзірлеу қажеттілігіне әкеп соғады. Сонымен бірге, деректерді сақтаудың бұлттық қойма немесе онлайн-сервистерді пайдалану сияқты нысандарын операторлар мен қызметтерді жеткізушілер айқын емес немесе стандартталмаған шешімдерге, оның ішінде деректер қауіпсіздігі тұрғысынан жиі негіздейді. Бұл ретте үйлесімді стандарттар аудару және бейімдеу сапасының төмендігінен түпдеректен айтарлықтай ерекшеленеді.

Жағдай бағдарламалық жасақтама мен телекоммуникациялық жабдыққа сертификаттау, пайдалану процесінде олқылықтарды жою кезеңінде үнемі айқындала бермейтін немесе вирусқа қарсы бағдарламалармен анықталмайтын функцияларды ( атап айтқанда "бэкдорларды") мақсатты енгізу мүмкіндігіне байланысты қиындайды, сондықтан ақпараттық жүйелер мен телекоммуникациялар желілерінің жұмысын бұзу үшін пайдаланылуы мүмкін.

6. АКТ-ның көптеген өнімдерінің трансұлттық және трансшекаралық сипатын және көпшілік пайдаланатын телекоммуникациялар желілерінің халықаралық байланыстылығын қылмыскерлер пайдаланушылар мен АКТ-қызметтерінің операторларына және ұлттық сегментте орналасқан интернет-ресурстарының иелеріне, сондай-ақ интернетпен өзара әрекет ететін ақпараттық жүйелерге қатысты заңға қайшы әрекеттерді жасау мақсатында пайдаланады.

Осындай қылмыстардың жоғары жасырындылығы және халықаралық сипаты олардың қоғамдық қауіпсіздігін арттырады. Жағдайды ақпараттық қауіпсіздіктің қылмыстық-құқықтық институттарының дамығанына қарамастан, "киберқылмыстың" жазаға тартылмауы, АКТ-ны қауіпсіз пайдалану саласын нығайту бойынша мемлекет қабылдайтын шаралардың керексіздігі туралы қоғамда тамырын тереңге жайған стереотип, жоғары технологиялық қылмыстар жасаған кінәлілерді жауапкершілікке тарту бойынша құқық қорғау органдары мүмкіндіктерінің шектеулігі әсерінен күшейте түседі.

7. Жекелеген елдердің АКТ саласын милитарландыруға айдап салуы, негізінен интернетті басқарудың қолданыстағы халықаралық жүйесінің стихиялық қалыптасқан сипаты тудырған мемлекеттердің АКТ-ны халықаралық құқық қағидаттарын бұза отырып пайдалануға қатыстылығын дәлелдеудің қиындығы, елдер арасында сақталып отырған цифрлық айырмашылық әлемдік қоғамдастықта ақпараттандыру және телекоммуникациялар саласында жетістіктерді соғыс мақсатында пайдалануды болғызбайтын сенімді халықаралық-құқықтық құралдарды қалыптастыруға кедергі келтіреді.

Бұл ретте әскери мақсаттарда пайдаланылатын арсенал сайып келгенде киберқылмыс пайдаланатын бағдарламалық-техникалық құралдар арсеналынан ерекшеленбейді, бұған АКТ-ны барлау, бұзу және халықаралық бейбітшілік пен қауіпсіздікті сақтауға қауіп төндіретін өзге де мақсаттарда пайдаланудың көптеген жағдайлары куә.

Осылайша, Қазақстанда киберқауіпсіздік саласында мынадай айтарлықтай қауіптер бар:

тұрғындардың, АКТ саласы қызметкерлерінің және ұйымдар басшыларының ақпараттық қауіпсіздік мәселелері жөніндегі құқықтық сауаттылығының төмендігі;

ақпараттандырудың мемлекеттік және мемлекеттік емес субъектілерінің және АКТ саласында көрсетілетін қызметтерді пайдаланушылардың белгіленген талаптарды, техникалық стандарттар мен ақпаратты электрондық түрде жинау, өңдеу, сақтау және беру регламенттерін бұзуы;

ақпараттық жүйелерге, бағдарламалық жасақтама және ақпараттық-коммуникациялық инфрақұрылымның басқа да элементтеріне теріс ықпал ететін персоналдың әдейі жасамаған қателері және технологиялық іркілістер;

халықаралық қылмыстық топтардың, қоғамдастықтардың және жеке тұлғалардың қаржы-банк саласындағы ұрлауды, өнеркәсіптің, энергетиканың, байланыс және ақпараттық-коммуникациялық қызметтер саласының технологиялық процестерін басқарудың автоматтандырылған жүйесінің жұмысын бұзу мақсатында зиянды ықпалды жүзеге асыру бойынша іс-қимылы;

ақпараттық-коммуникациялық инфрақұрылымға барлау және зиянкестік әрекет жасау арқылы Қазақстан Республикасы мүдделеріне қарсы бағытталған саяси, экономикалық, террористік құрылымдардың, шет мемлекеттердің барлау және арнайы қызметтерінің қызметі.

### 3. Халықаралық тәжірибе

"Киберқауіпсіздік" терминінің және одан туындайтын ұғымдардың (киберкеңістік, киберқорғау, кибератака, кибершабуыл және т.б.) халықаралық деңгейде көпшілік мойындаған бірыңғай заңды анықтамасы жоқ.

Дегенмен БҰҰ деңгейінде Халықаралық электр байланыс одағының (ХЭО) Ғаламдық киберқауіпсіздік бағдарламасы немесе "Киберқауіпсіздіктің ғаламдық мәдениетін қалыптастыру және аса маңызды ақпараттық инфрақұрылымдарды қорғау жөніндегі ұлттық күштерді бағалау" БҰҰ Бас ассамблеясының қарары секілді бірқатар құжаттар бар, оларда (1) жеке өмірге қол сұғылмаушылықты, (2) электрондық нысандағы ақпараттың құпиялылығын, тұтастығы мен қолжетімділігін, (3) интернетпен өзара іс-қимыл жасайтын аса маңызды ақпараттық-коммуникациялық инфрақұрылымды (оның ішінде ақпараттық жүйелерді, аппараттық-бағдарламалық кешендерді, телекоммуникациялық жүйелерді, телекоммуникация желілерін, ақпаратты қорғау, бағдарламалық жасақтама жүйелерін) зиян келтіретін ықпалдан бағдарламалық-техникалық әдістермен қорғауды қамтамасыз ету мәселелерінде ақпараттық-коммуникациялық технологияларды қауіпсіз пайдалану саласын қамтитын киберқауіпсіздікті түсіну тәсілдері қамтылған.

Бұл ретте көптеген елдер ақпаратты еркін тарату және оған қол жеткізу құқығын тым шектеуден қауіптенгендіктен, басшылыққа алатын құжаттарда АКТ пайдалана отырып таратылатын зиянды немесе заңсыз ақпараттан қорғау мәселелерін киберқауіпсіздік ұғымы контексінде қарастырмайды.

Жекелеген елдер киберқауіпсіздік призмасы арқылы тек телекоммуникациялар мен есептеуіш ресурстардың бүкіләлемдік жүйесі ретінде интернетте терроризмді, балалар порнографиясын насихаттайтын электрондық материалдарды және заңсыз ақпараттың кейбір түрлерінің бақылаусыз таралуын ғана қарастырады, бұл ең алдымен, мұндай ақпаратты тарату көзін анықтаудың техникалық күрделілігіне байланысты.

Бұл ретте кейбір елдер қауіп-қатерлерді және оларға қатысты қабылданатын қарсы іс-қимыл шараларын бағалауда құқықтық реттеу мен мемлекеттік басқару жүйесінің тиісті моделін қалыптастыра отырып, АКТ пайдаланудың барлық аспектілеріне қолданылатын ақпараттық қауіпсіздік ұғымын ұстанады.

Айталық, Норвегияның стратегиясында жаңа қызметтер мен құрылғылар қарапайым қолданушылардың құзыретіне өте жоғары талаптар қоятындығы аталған. Ақпараттың, жүйелер мен желілердің қауіпсіздігін қамтамасыз етуге басты жауапкершілік меншік иесіне немесе операторға жүктеледі. Мұндай жұмыстар күнделікті жұмыстың бір бөлігі болуы тиіс және ағымдағы операциялармен бірдей қаржыландырылуы керек. Ақпараттық қауіпсіздікке жәрдемдесу жөніндегі шаралардың құны басқарудың жекелеген салаларындағы тәуекелді бағалаумен мөлшерлес болуы тиіс (киберқауіпсіздіктің жаһандық индексі 0,735 құрайды).

Эстонияда ақпараттық жүйелердің қауіпсіздігіне басты назар аударылады. Ұсынылатын шаралар азаматтық сипатқа ие және құқықтық реттеуге, оқытуға және ынтымақтастыққа негізделеді (киберқауіпсіздіктің жаһандық индексі 0,706 құрайды).

Финляндия стратегиясы киберқауіпсіздікті финдік ақпараттық қоғамның дамуымен тығыз байланысты экономикалық сипаттағы проблема ретінде түсінуге негізделген ( киберқауіпсіздіктің жаһандық индексі 0,618 құрайды).

Словакия ақпараттық қауіпсіздікті қамтамасыз етуді қоғамның қалыпты жұмыс істеуі мен дамуының қажетті шарты ретінде қарастырады. Сондықтан стратегияның мақсаты – ақпаратты қорғау үшін берік іргетас ретінде қызмет ету. Стратегия қауіп-қатерлердің алдын алуға да, сонымен қатар олардың алдын алу құралдарының беріктігі мен дайындығын қамтамасыз етуге де бағытталған (киберқауіпсіздіктің жаһандық индексі 0,618 құрайды).

Чех Республикасының киберқауіпсіздік стратегиясының негізгі мақсаттары ақпараттық-коммуникациялық жүйелерді ұшырауы мүмкін осалдықтардан қорғауды және жүйелерге жасалатын атакалардан келетін ықтимал зиянды азайтуды қамтиды. Стратегияның негізгі нысанасы Чех Республикасында ақпараттық сервистерге еркін қол жеткізу, деректердің тұстастығы мен құпиялылығы проблемаларына бағдарланған ( киберқауіпсіздіктің жаһандық индексі 0,500 құрайды).

Франция ақпараттық жүйелердің ақпараттың қолжетімділігіне, тұтастығына және құпиялылығына әсер етуі мүмкін оқиғаларға қарсы тұруға қабілетті болуына бағдарланады, ақпаратты қорғаудың техникалық құралдарына, киберқылмыстылыққа қарсы күреске және киберқалқан орнатуға көңіл бөледі (киберқауіпсіздіктің жаһандық индексі 0,588 құрайды).

Германияның стратегиясы аса маңызды ақпараттық жүйелердің қауіпсіздігінің негізін қалайды. Германия кибератакалардың алдын алуға және оларды қылмыстық қудалауға, сондай-ақ кездейсоқ факторлардан туындайтын IT-жабдықтың істен шығуына жол бермеуге бағдарланған. Германияның киберқауіпсіздік стратегиясы киберкеңістіктегі деректердің тұтастығын, сенімділігі мен құпиялылығын, ақпараттар мен коммуникацияларды қорғау және оларға қол жеткізу үшін қабылданған барлық ұлттық және халықаралық шаралардың қол жеткізілген жиынтығымен, сондай-ақ негізгі стратегиялық IT-құзыреттіліктердің барлық диапазонында герман технологиялық егемендігі мен экономикалық әлеуетті нығайту арқылы киберқауіпсіздік деңгейін айқындайды (киберқауіпсіздіктің жаһандық индексі 0,706 құрайды).

Литваның электрондық ақпараттық қауіпсіздікті дамыту бағдарламасы электрондық ақпараттық қауіпсіздікті қамтамасыз етуге, электрондық ақпарат айналымын дамытуға, сондай-ақ киберкеңістіктегі оның құпиялылығын, қолжетімділігі мен тұтастығын қамтамасыз етуге бағытталған мақсаттар мен іс-шараларды айқындауға бағдарланады. Бұдан басқа Литва стратегиясы дербес деректерді, телекоммуникациялық желілерді, ақпараттық жүйелер мен аса маңызды инфрақұрылымдарды "электрондық периметр" шектерінің әсерінен қауіпсіздіктің бұзылушылығы мен кибератакалардан қорғауға бағытталған.

Нидерланды, бір жағынан, осы жүйелердегі ауыр бұзушылықтардан қауіптенгендіктен, қауіпсіз және сенімді ақпараттық-коммуникациялық жүйелерге ұмтылады, екінші жағынан, интернет-кеңістіктің еркін және ашық болу қажеттілігін мойындайды. Стратегияда киберқауіпсіздікке анықтама беріледі. "Киберқауіпсіздік – бұл ақпараттық-телекоммуникациялық жүйелерді дұрыс пайдаланбаудан және олардың істен шығуынан қорғалу. Істен шығу және дұрыс пайдаланбау ақпараттық-телекоммуникациялық жүйелердің қолжетімділігі мен сенімділігіне кері әсер етуі, жүйелерде сақталатын ақпараттың құпиялылығы мен тұтастығына қауіп төндіруі мүмкін" (киберқауіпсіздіктің жаһандық индексі 0,676 құрайды).

Аустрияның АКТ қауіпсіздігі стратегиясы Аустрия экономикасының ұзақ мерзімді өміршеңдігін қамтамасыз ету мақсатында "электрондық үкімет" жүйесінде іске асырылған қауіпсіздіктің интегралдық тәсілдерін трансұлттық деңгейде құрылуы тиіс салаларды қоса алғанда, басқа салаларға да таратуға негізделген (киберқауіпсіздіктің жаһандық индексі 0,676 құрайды).

Ұлыбританияның тәсілі киберқауіпсіздікті дамытуға бағытталған. Мақсаты: Біріккен Корольдікті ақпараттық-телекоммуникациялық технологиялар саласындағы инновациялар, инвестициялар және сервистердің сапасы бойынша бірінші орынға шығару және сол арқылы киберкеңістіктің барлық артықшылықтары мен игіліктерін толық көлемде пайдалану. Киберкеңістікті азаматтар мен экономика үшін қауіпсіз ету мақсатында қылмыскерлердің, террористердің және басқа мемлекеттердің кибератакалары түріндегі тәуекелдерді жою қажет (киберқауіпсіздіктің жаһандық индексі 0,706 құрайды).

Швейцарияның ұлттық стратегиясында интернет-индустрияға қатысушы бірнеше елдің басым мүдделерінің ықпалын азайту қажеттілігі аталады, онда сипатталатын шаралардың "бейбіт уақытта қолданылуын қарастыратындығы және осылайша соғыс ықтималдылығын жоятыны" көрсетілген.

Бұл ретте, істен шығуға төтеп бере алатын әскери инфрақұрылым кең ауқымды дағдарыс болған жағдайда басқа субъектілер үшін стратегиялық резервтің маңызды элементі ретінде қарастырылады. Түрлі салалардағы қолданыстағы заңнама мемлекеттік және жеке сектордың қолданыстағы міндеттерінің және міндеттерінің кибер-аспектілерін көрсететіндіктен, Швейцарияның бірыңғай арнайы киберзаңы шеңберінде киберқауіпсіздік мәселелерін шешу жарамсыз деп саналады, себебі " қолданыстағы заңнама өзгерістерге үздіксіз бейімделіп отыруы тиіс" ( киберқауіпсіздіктің жаһандық индексі 0,353 құрайды).

Осылайша, әрбір елде киберқауіпсіздік пен негізгі басымдықтардың ұлттық түсінігінде айтарлықтай айырмашылықтар бар.

Нәтижесінде киберқауіпсіздік стратегияларын жасау тәсілдері де түрлі болып келеді . Дегенмен киберқауіпсіздік мәселелерін қамтитын басшылыққа алынатын құжаттар, әдетте, мыналарды көздейді:

- киберқауіпсіздікті қамтамасыз ету саласындағы мемлекеттік басқару жүйесін құру ;

- жеке және мемлекеттік мүдделі тараптарға ұлттық ақпараттық инфрақұрылымдардың қауіпсіздігін қамтамасыз ету проблемаларын талқылауға мүмкіндік беретін тиісті тетікті айқындау (негізінен, қоғамдық-мемлекеттік әріптестік);

- қажетті қауіпсіздік саясатын және реттеуші тетіктерді айқындау, жеке және мемлекеттік сектор үшін рөлдерді, құқықтар мен жауапкершілікті айқын белгілеу ( мысалы, қауіпсіздік инциденттері туралы міндетті хабардар ету, қауіпсіздікті қамтамасыз етудің базалық шаралары және іс-қимыл нұсқаулығы, материалдық-техникалық қамтамасыз етудің жаңа нормалары).

Әлемдік тәжірибе көрсетіп отырғандай, бағдарламалық жасақтамадағы қателерден немесе ақпараттық қауіпсіздік инциденттерінен толық қорғалуға қол жеткізу мүмкін емес, бірақ өзін саналы, жауапты ұстау арқылы бүлдіруші салдарларға жол бермеу үшін олардың жиілігі мен ықтималдылығын төмендету, ақпараттық жүйелер мен ресурстардың жұмысқа қабілеттілігін қалпына келтірудің жоғары жылдамдығын қамтамасыз ету өте маңызды қажеттілік.

Бұл саланы үйлестіру көптеген елдерде айтарлықтай дәрежеде ақпараттық технологиялар және байланыс саласындағы азаматтық реттеуші (KISA ақпараттық қауіпсіздік агенттігі – Корея, Ақпараттық технологиялар министрлігінің Ақпараттық қауіпсіздік орталығы – Өзбекстан және т.б.) не ақпаратты қорғауға және ақпараттық қауіпсіздікке жауапты орган (Ақпараттық техника қауіпсіздігі бюросы – Германия, Қорғаныс министрлігі жанындағы Ақпараттық жүйелер қауіпсіздігі агенттігі – Франция , Чехия ұлттық қауіпсіздік агенттігі, Ресей Федерациясының Федералдық қауіпсіздік қызметі және Техникалық және экспорттық бақылау саласындағы федералдық қызмет, Беларусь Республикасының Президенті жанындағы Жедел-талдау орталығы, Украина Арнайы байланыс және ақпарат қорғау қызметі. Еуропалық одақта бұл саладағы реттеуші – Ақпараттық және желілік қауіпсіздік агенттігі болып табылады) айналасында құрылады.

## 4. Мақсаты, міндеттері, күтілетін нәтижелер және іске асыру мерзімі

Тұжырымдаманың мақсаты ғаламдық бәсекелестік жағдайларында Қазақстан Республикасының орнықты дамуын қамтамасыз ететін, электрондық ақпараттық ресурстардың, ақпараттық жүйелер мен ақпараттық-коммуникациялық инфрақұрылымның сыртқы және ішкі қауіп-қатерлерден қорғалу деңгейіне қол жеткізу және сол деңгейде ұстау болып табылады.

**Тұжырымдаманың міндеттері:**

1. Қауіп-қатерлер туралы хабардарлықты арттыру, адами капиталды және зиянды бағдарламалық-техникалық ықпалды және қорғалған телекоммуникациялық жабдықты бұғаттауға және жоюға бағытталған бағдарламалық өнімдер мен қорғалған

киберқауіпсіздік жүйелерін жасау бойынша отандық АКТ саласының әлеуетін дамыту үшін қажетті жағдай жасау.

2. Технологиялық процестерді басқарудың автоматтандырылған жүйелерінің қауіпсіздігін және ақпаратты қорғаудың ұлттық жүйесінде АКТ-ны қауіпсіз пайдалануды нормативтік-құқықтық және ұйымдастырушылық-техникалық қамтамасыз етуді, құқық қолдану практикасын, әдіснамалық базасын жетілдіру.

3. Барлық ұлттық ақпараттық-коммуникациялық инфрақұрылымға қатысты ақпараттандыру және байланыс саласындағы ақпараттық қауіпсіздікті мемлекеттік басқарудың жоғары бейімделген және интеграцияланған жүйесін құру.

**Күтілетін нәтижелер:**

1) Қазақстанның киберқауіпсіздігінің жаһандық индексі 2017 жылға қарай 0,200, 2018 жылға қарай – 0,300, 2019 жылға қарай – 0,400, 2020 жылға қарай – 0,500, 2021 жылға қарай – 0,550, 2022 жылға қарай – 0,600 құрайды;

2) ақпараттық қауіпсіздікке төнетін қауіп-қатерлер туралы хабардарлықты 2018 жылдың базалық кезеңіне қарағанда 2019 жылы 5%-ға, 2020 жылы – 10%-ға, 2021 жылы – 15%-ға, 2022 жылы – 20%-ға арттыру;

3) ақпараттық қауіпсіздік саласындағы қайта даярланған мамандардың саны 2018 жылы– 300, 2019 жылы – 500, 2020 жылы – 600, 2021 жылы – 700, 2022 жылы – 800 болады;

4) мемлекеттік және квазимемлекеттік секторларда пайдаланылатын ақпараттандыру және байланыс саласындағы отандық бағдарламалық өнімдердің үлесін 2017 жылдың базалық кезеңіне қарағанда 2018 жылы – 10%-ға, 2019 жылы – 20%-ға, 2020 жылы – 30%-ға, 2021 жылы – 40%-ға, 2022 жылы – 50%-ға арттыру;

5) KZ және .ҚАЗ домені бар интернет-ресурстарының шифрланған деректерді беру кезінде отандық қауіпсіздік сертификаттарын пайдалану 2018 жылы – 20%, 2019 жылы – 40%, 2020 жылы – 60%, 2021 жылы – 80%, 2022 жылы – 100% құрайды;

6) ақпараттық қауіпсіздік мониторингі орталықтарына қосылған мемлекеттік органдардың ақпараттық жүйелерінің, мемлекеттік жүйелермен интеграцияланған мемлекеттік емес ақпараттық жүйелердің, ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілерінің ақпараттық жүйелерінің үлесі 2018 жылы – 20%, 2019 жылы – 40%, 2020 жылы – 60%, 2021 жылы – 80%, 2022 жылға қарай – 100% болады.

**Тұжырымдаманы іске асыру мерзімі екі кезеңнен тұрады:**

1) бірінші кезең – 2017 – 2018 жылдар;

2) екінші кезең – 2019 – 2022 жылдар.

Бірінші кезеңде:

- ақпараттық қауіпсіздікті қамтамасыз ету саласындағы белгіленген талаптарды сақтаудың көлемді құқық қолдану практикасы жасалатын болады, оның нәтижелері бойынша қажет болған жағдайда заңнамаға тиісті өзгерістер енгізіледі;

- білім беру бағдарламалары мен кәсіптік стандарттарға ревизия жүргізіледі, ақпараттық қауіпсіздік саласында даярланатын мамандардың саны мен сапасы артады, осы салада жұмыс істейтін қызметкерлердің біліктілігін арттыру қамтамасыз етіледі;

- отандық зерттемелер жасауда өнеркәсіп пен ғылым арасындағы өзара іс-қимыл мен кооперацияның тиімді схемасы жасалады, бұл ұлттық және салалық ақпараттық қауіпсіздік шұғыл орталықтарын дамыту үшін негіз жасайды, бұл екінші кезеңде:

- қазақстандық IT-компаниялардың ұлттық ақпараттық-коммуникациялық инфрақұрылымды ақпараттық қауіпсіздік жүйелерімен қамтамасыз етуге негізді түрде қатысуын;

- отандық электрондық өнеркәсіп кәсіпорындарын мемлекеттік органдар мен квазимемлекеттік сектордың ел аумағындағы ақпараттық қауіпсіздік талаптарына сәйкестігі тұрғысынан сертификаттау рәсімінен өткен және өндірілген телекоммуникациялық жабдықты сатып алуына тапсырыстармен қамтамасыз етуге мүмкіндік береді.

## 5. Негізгі қағидаттар мен тәсілдер

**Негізгі қағидаттар:**

1) жеке тұлғалардың құқықтарын, бостандықтары мен заңды мүдделерін, сондай-ақ заңды тұлғалардың құқықтары мен заңды мүдделерін сақтау;

2) ақпараттық-коммуникациялық технологияларды қолданған кезде тұлғаның, қоғамның және мемлекеттің қауіпсіздігін қамтамасыз ету;

3) Қазақстан Республикасы аумағында ақпараттандыру объектілерінің сенімділігі мен басқарылуын қамтамасыз ететін бірыңғай стандарттар негізінде ақпараттандыру қызметін жүзеге асыру;

4) мемлекеттік органдардың өкілеттігін айқын ажырату;

5) ақпараттық-коммуникациялық инфрақұрылым объектілерінің ақпараттық қауіпсіздігінің үздіксіз мониторингі;

6) ұлттық қауіпсіздікті қамтамасыз ету жүйесінің халықаралық қауіпсіздік жүйелермен интеграциялануы.

Қауіп-қатерлер туралы хабардарлықты арттыру, адами капиталды және бағдарламалық өнімдерді, ақпараттық қауіпсіздік жүйелерін, зиянды бағдарламалық-техникалық ықпалға төзімді телекоммуникациялық жабдықты жасау бойынша отандық АКТ саласының әлеуетін дамыту үшін қажетті жағдай жасау міндетін іске асыру үшін мыналар ұсынылады:

Қоғамда "кибергигиена" туралы орнықты түсініктер қалыптастыруға және бағдарламалық өнімдердің, ақпараттық жүйелердің, бағдарламалық жасақтаманың, технологиялық тұғырнамалардың, ақпараттық және желілік инфрақұрылымның, жұмысты қамтамасыз ететін жабдықтың әрекет ету циклінің барлық кезеңдерінде АКТ жасау мен пайдаланудың жоғары өндірістік мәдениетін қалыптастыру.

Кәмелетке толмаған интернет пайдаланушылар мен олардың ата-аналары арасында дербес деректерді қорғау және жеке өмірге қолсұғылмаушылық бойынша тренингтер мен оқыту практикаларын пайдалану.

Мемлекеттік органдардағы ақпараттық қауіпсіздіктің жай-күйіне жауапты қызметкерлердің кәсібилігін арттыру және олар қабылдайтын шараларды тиісті түрде әмбебап ету, кәсіптік стандарттарды бейімдеу, сондай-ақ ақпараттық ресурстар мен жүйелердің қорғалуын бақылау параметрлері мен қорғау профильдерін жақсартатын тәжірибелік дағдылар мен техникалық білімдер бойынша талаптарды кеңейту.

Қазақстанның жоғары оқу орындарына ақпараттық қауіпсіздік саласында білім беру және зерттеу міндеттерін іске асыруда маңызды рөл беру, бұл мемлекет қауіпсіздігін қамтамасыз ету бойынша арнайы мемлекеттік органдардың техникалық мүмкіндігін кеңейтеді және Тұжырымдаманы іске асыру бойынша іс-шараларды талдамалық және ғылыми-зерттеумен сүйемелдеу деңгейін көтереді.

Құқық қорғау органдарының ғылыми-зерттеу ұйымдарын неғұрлым күрделі киберқылмыстарды тергеуге тарту арқылы киберқылмыстылыққа қарсы іс-қимылға техникалық дайындық және кәсіби құзыреттіліктің жоғары деңгейін қалыптастыру және қолдау бойынша міндеттерді шешу.

Ғылыми, ғылыми-техникалық және білім беру қызметі саласында қазақстандық әлеуетті ұлғайту үшін ғылыми-зерттеу және тәжірибелік-конструкторлық жұмыстарға назар аудару, оқу процесінің электрондық өнеркәсіп кәсіпорындарының өндірістік қызметімен тығыз байланысын қамтамасыз ету, оқу бағдарламаларын салалық кәсіптік стандарттарға және технологияларды дамытудың заманауи деңгейіне сәйкес келтіру қажет.

Зерттеулерге және қолданбалы математика, ақпаратты криптографиялық қорғау құралдарын әзірлеу, криптология, бағдарламаланатын логикалық интегралдық схемалар бойынша әзірлемелер, кванттық криптография мен ақпарат берудің, өңдеудің және сақтаудың қорғалған жүйелерін, сондай-ақ ақпараттық қауіпсіздік жүйелерін құру бойынша өз мектептерімізге басымдық беру.

Отандық әзірлемелердің сұранысқа аса ие болмауы проблемасын жою, өйткені киберқауіпсіздік түптен келгенде отандық IT-саласының және электронды өнеркәсібінің даму деңгейіне байланысты. Мұның себептерінің бірі мемлекеттік органдарда олардың өнімдерін басым түрде пайдалану міндеттілігінің болмауы.

Оларды қолдау шараларын белгілеу, оның ішінде мемлекеттік-жекешелік әріптестікті ынталандыру, бәсеке қабілеттілікті арттыру. Зерттемені оқшаулау және техникалық қолдау талаптарына сәйкестік, жеткізушіде бағдарламалық өнімдер мен телекоммуникациялық жабдықтардың конструкторлық және техникалық құжаттамасына айрықша зияткерлік меншік құқықтарының болуы, сондай-ақ өндірісті, кепілдік және кепілдіктен кейінгі қызмет көрсетуді ұйымдастыру үшін қажетті ғылыми өндірістік базаның болуы өлшемшарттар болуы тиіс.

Сала өкілдерімен бірлесіп ақпараттық қауіпсіздік талаптарына сәйкестікке міндетті сертификаттау рәсімінен өткен сенімді отандық немесе шетелдік үлгілермен оларды ауыстыру мақсатында мемлекеттік органдар мен квазимемлекеттік секторда сатып алынатын бағдарламалық жасақтама мен телекоммуникациялық жабдыққа ұдайы талдау жасауды өткізу.

Ақпараттық қауіпсіздік жөніндегі уәкілетті орган жанынан Киберқауіпсіздік жөніндегі кеңес құрылуы тиіс, оның негізгі міндеттерінің бірі киберқауіпсіздік бойынша өзекті мәселелерді қарау, басшылыққа алынатын құжаттарды, нормативтік құқықтық базаны өзекті күйінде ұстау, отандық электрондық және софтверлік өнеркәсіп өнімін басым түрде пайдалануға ықпал ету, қоғамдық маңызы бар IT-жобаларға жария бағалау жүргізу болуы тиіс.

Еліміздің жетекші компанияларымен және кәсіпорындарымен, білім беру және ғылыми зерттеу ұйымдарымен тұрақты тікелей диалог орнату, АКТ пайдаланудың аса маңызды салаларында интеграцияланған киберқауіпсіздікті қамтамасыз ету бойынша міндеттерді шешуде жүйелі және кешенді сипат беруге және күштерді біріктіруге мүмкіндік береді.

Мемлекеттік ақпараттық жүйелер мен ресурстардың қорғалуына мониторинг пен талдау жүргізумен, азаматтар мүддесі үшін АКТ-ны қауіпсіз пайдалану бойынша жәрдемдесумен қатар, "кибергигиена" шараларын дәріптеу KZ-CERT компьютерлік инциденттерге мемлекеттік ден қою қызметінің қосымша басымдығына айналуы тиіс.

Жеке ақпараттық жүйелердің иелері мен меншік иелері өздерінің экономикалық мүмкіндіктеріне қарай, ақпараттық жүйелерді әзірлеудің, жасаудың, сынаудың және пайдаланудың стандартталған процестеріне сүйенуге ұмтылып, олардың ақпараттық қауіпсіздігін қамтамасыз етуге қажетті шаралар қарастыруы тиіс. Бұл үшін қажетті бағдар ретінде қызмет ете алатын техникалық стандарттар мен басқа да нормативтік-техникалық құжаттар бар.

Технологиялық процестерді басқарудың автоматтандырылған жүйелерінің қауіпсіздігін және ақпаратты қорғаудың ұлттық жүйесінде АКТ-ны қауіпсіз пайдалануды нормативтік-құқықтық және ұйымдастырушылық-техникалық қамтамасыз етуді, құқық қолдану практикасын, әдіснамалық базасын жетілдіру бойынша міндеттерін іске асыру үшін ұсынылады:

Мемлекеттік секторда заңнамамен және техникалық стандарттармен белгіленген ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі талаптарды мүлтіксіз орындау, сондай-ақ киберқауіпсіздік үшін зиян келтірмей технологиялардың даму серпінін ескере отырып, оларға қажетті өзгерістерді жедел енгізу.

Белгіленген талаптарды сақтау пәрменді мемлекеттік бақылау шараларымен қамтамасыз етілуі тиіс.

Ақпараттық ресурстар мен жүйелердің иелерінің бейғамдық және салғырттық танытуына сенетін киберқылмыскерлер мен шетелдік техникалық компьютерлік

барлаушылар қызметінің сипатын есепке ала отырып, ақпараттандыру объектілерінің қорғалу жай-күйін толық бағалау үшін қорғалуды бақылаудың техникалық құралдарымен ақпараттық жүйелер мен ресурстардың жай-күйін тұрақты мониторингтеуге және ақпараттың таралу арналарын (осалдықтарды, вирустарды, троян бағдарламаларын, декларацияланбайтын функциялар мен белгілерді) анықтау бойынша жұмысты жүзеге асыруға ұмтылу қажет.

Осындай тәсіл ұлттық және қоғамдық қауіпсіздікке қауіп төндіретін ақпараттық қауіпсіздік инциденттерінен туындаған технологиялық, әлеуметтік сипаттағы төтенше жағдайлар орын алған жағдайда мемлекеттік функцияларды іске асыру мүмкіндігін, ал төтенше немесе соғыс жағдайы орын алған жағдайда ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілерінің қызмет ету мүдделері үшін ұлттық қауіпсіздікті қамтамасыз ету күштерінің тұрақты ақпараттық-коммуникациялық инфрақұрылымын пайдалану мүмкіндігін сақтауға мүмкіндік береді.

Стратегиялық және аса маңызды мемлекеттік объектілер, экономиканың стратегиялық салаларының объектілері қатарынан аса маңызды ақпараттық-коммуникациялық инфрақұрылым объектілерімен жұмысты жолға қоюмен қатар, халыққа ақпараттық-коммуникациялық қызметтер көрсетуге бағдарланған аса маңызды объектілерге жатқызу мүмкіндігімен ақпараттық-коммуникациялық инфрақұрылымының аса маңызды объектілеріне жатқызу тәсілдерін қайта қарау қажет.

Алдын алу және профилактикалық шараларды мемлекеттік органдарға және мемлекеттік жүйелермен интеграцияланатын жеке ақпараттық жүйелердің иелеріне ғана емес, сонымен қатар өнеркәсіптік кәсіпорындар, қаржылық ұйымдар иелеріне және бұзылуы еліміздің экономикалық дамуына кері әсер етуі мүмкін автоматтандырылған технологиялық процестері бар экономика объектілерінің өзге санаттарына да қолдану қажет.

Жалпы ұлттық ауқымдағы қауіп-қатерлерді тиімді оқшаулау және оларды іске асырудың алдын алу үшін Бірыңғай талаптар мен қолданыстағы "Электрондық үкіметтің" ақпараттандыру объектілерінің ақпараттық қауіпсіздігін, қорғалуын және қауіпсіз жұмыс істеуін қамтамасыз етудің мониторингін жүргізу қағидалары негізінде мемлекеттік сектор үшін ғана емес, сонымен қатар жеке меншіктегі объектілер үшін де бағдар ретінде қызмет ететін басшылыққа алынатын құжаттар әзірлеуді көздеу қажет.

Азаматтар мен бизнестің мемлекеттік органдар көрсететін қызметтерге жоғары сенімін қамтамасыз ету мақсатында заңнамалық деңгейде бағдарламалық өнімдер, байланыс қызметтерін және өзге де ақпараттық-коммуникациялық инфрақұрылым жеткізушілері үшін кемінде үш жыл ішінде сатып алынатын өнімдерге, сатып алынатын өнімдер мен көрсетілетін қызметтерді міндетті техникалық қолдау жөніндегі шешімдерге келісімдерде, конкурстық құжаттамада және техникалық ерекшеліктерде көрсету үшін ақпараттық қауіпсіздік жөніндегі шаралар әзірлеу қажет.

Технологиялық процестерді басқарудың автоматтандырылған жүйелерінің және жалпы пайдаланудағы телекоммуникациялар желілерінің телекоммуникациялық жабдығының қауіпсіздігін қамтамасыз ету саласында қажетті талаптарды көздеу қажет. Тұрғындардың тіршілігін қамтамасыз ету жүйелерінде, отын-энергетикалық секторда, байланыс инфрақұрылымында және басқа да жүйелерде инфрақұрылымға ерекше көңіл бөлінуі қажет.

Интернеттің ұлттық сегментінің және деректерді өңдеу орталықтарының ( дата-орталықтардың), көпшілікке қолжетімді электрондық ақпараттық ресурстардың ( интернет-ресурстардың) жұмыс істеуін қамтамасыз ететін ақпараттық бағдарламалық кешендердің аса маңызды инфрақұрылымы элементтерінің орнықтылығына қатысты ұғымды елеулі тереңдету қажет.

Қолданушылардың әрекеттерін сенімді сәйкестендіруді, түпнұсқаландыруды және тіркеуді олардың дербес деректерінің құпиялылығын қамтамасыз ету шараларымен бірге қамтамасыз ету, ақпараттық жүйелердің пайдаланушылары мен электрондық бұқаралық ақпарат құралдарының аппараттық бағдарламалық кешендерін қоса алғанда, көпшілікке қолжетімді электрондық ресурстардың сәйкестігіне байланысты неғұрлым кең таралған қауіптер тәуекелін төмендетеді. Бұл ұлттық сегментте электрондық коммерция, электрондық төлемдер, банк қызметі және интернет-ресурстар арқылы көрсетілетін басқа да ақпараттық-коммуникациялық қызметтер саласындағы жалған әрекеттерді болғызбауға мүмкіндік береді.

Барлық ұлттық ақпараттық-коммуникациялық инфрақұрылымға қатысты ақпараттандыру және байланыс саласындағы ақпараттық қауіпсіздікті мемлекеттік басқарудың жоғары бейімделген және интеграцияланған жүйесін құру үшін мынаны ұсынамыз:

Мемлекеттік органдар мен көрсетілетін қызметтерді жеткізушілер қалыпты және күтпеген режимдерде жасалатын ақпараттық жүйелер сенімділігінің және олардың қасақана істен шығаруға төтеп беруінің аса жоғары деңгейін қамтамасыз ететін күштерге бірінші кезекте көңіл бөле отырып, қауіпсіздік тәуекеліне бағдарланған тәсілді қолдануы қажет.

Ақпараттық ресурстар мен жүйелердің иелеріне жәрдемдесу және туындайтын қауіп-қатерлер туралы өзара хабардар ету үшін ақпараттық қауіпсіздік инциденттеріне ден қоюдың және оларды мониторингілеудің ведомстволық және салалық құрылымдары арасындағы өзара іс-қимылды кеңейту қажет. Олардың қатысушылары қауіпсіздік мәселесін салалық ақпараттық жүйелер мен желілерді жоспарлаудың, жобалаудың, әзірлеудің және пайдаланудың аса маңызды элементі ретінде қарастыруы тиіс және еліміздің барлық ақпараттық-коммуникациялық инфрақұрылымының орнықтылығын айқындайтын негізгі өзегіне айналуы тиіс.

Ақпараттық қауіпсіздік инциденттеріне ден қою қызметтерінің мамандануы тартылған ұйымдар мен сарапшылар тобын кеңейтуге мүмкіндік береді, бұл салалық

ерекшеліктерді ескере отырып ақпараттық қауіпсіздік саласында жұмыс істейтін қызметкерлердің кәсібилігін жоғарылатуға және көп жағдайда IT және ақпараттық қауіпсіздік саласындағы білікті мамандарды ұстауға мүмкіндігі бола бермейтін шағын бизнес үшін ақпараттық қауіпсіздік аудиті қызметі нарығын кеңейтуге жәрдемдесуге ықпал ететін болады.

Шетелдік кеңістіктен іске қосылған компьютерлік атакалар еліміздің виртуалдық периметрі – "электрондық шекарасында" барынша тоқтатылуы тиіс.

Телекоммуникация желілері мен ақпараттық-коммуникациялық желілерді конвергенциялау салдарынан оның артып келе жатқан осалдығын және зиянды трафик көлемдерін төмендету және байланыс операторларының нормадан ауытқыған желілік белсенділікті уақтылы бұғаттауы қажеттілігін ескере отырып, Қазақстан Республикасы Бірыңғай телекоммуникациялар желісінің басшылыққа алынатын құжаттарын өзектілендіру қажет.

Арнайы бөлімшелер жеке құрамының біліктілігін тұрақты арттыру, техникалық тіркеу құралдары арсеналын кеңейту мен "цифрлық" дәлелдемелерді криминалистік зерттеу арқылы киберқауіпсіздікке қарсы тиімді күрес үшін жағдай жасау.

Қызметі АКТ пайдаланумен байланысты барлық субъектілердің міндеті киберқауіпсіздікті қамтамасыз ету болып табылады, сондықтан ақпараттық қауіпсіздікті қамтамасыз ету мақсатындағы ынтымақтастық барлық мүдделі тараптардың мүдделерін қорғауға ықпал етеді.

Күштерді біріктіру үшін ғылыми қоғамдастықтың, жеке сектордың қатысуымен Ұлттық үйлестіруші жедел ақпараттық қауіпсіздік орталығын құру қажет, ол онлайн режимде "электрондық шекара", сондай-ақ ұлттық ақпараттық инфрақұрылымның аса маңызды компоненттерінің қорғалу жай-күйі туралы ақпаратты өңдейтін болады және ақпарат алмасуды қамтамасыз етеді, бұл:

азаматтар мен бизнеске ақпараттық қауіпсіздік саласындағы қауіп-қатерлерді білікті бағалауға және бағдарламалық жасақтама мен ақпараттық және телекоммуникациялық жүйелердегі осалдықтарды пайдалану қаупінің кері әсерін қалай азайту қажеттігі туралы қосымша білімдер алуға қолжетімділікті қамтамасыз етуге мүмкіндік береді;

Ішкі істер министрлігіне ақпараттық технологияларды пайдаланып жасалатын жасырын қылмыстардың санын азайтуға және оларды ашудың жоғары деңгейін қамтамасыз етуге;

мемлекеттік органдарға технологиялық істен шығудың туындауының алдын алуға және бұзылуға төзімділіктің жоғары деңгейін сақтауға, сондай-ақ "электрондық үкімет" және басқа мемлекеттік ақпараттық жүйелер мен ресурстардың құрамына кіретін инфрақұрылымдағы олардың салдарын уақтылы жоюға;

ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілері иелеріне өздеріне тиесілі технологиялық процестерді автоматтандырылған басқару жүйелерінің қауіпсіздігіне ықтимал әсер ету туралы уақтылы ақпарат алуға;

Ұлттық Банк пен екінші деңгейдегі банктерге қаржы-банк жүйесіндегі өзекті қауіптер туралы қосымша ақпарат алуға мүмкіндік береді.

Қорғаныс министрлігі елдің әскери ұйымын дамыту шеңберінде ведомстволық ақпараттық ресурстарды тиімді қорғау, компьютерлік атакаларды болжау және уақтылы анықтау бойынша жүйені құру, оларды бағалау және мемлекеттің әскери қауіпсіздігіне қауіп төндіруі тұрғысынан жіктеу бойынша ұсыныстар әзірлеуі қажет.

Халықаралық құқықтар нормалары мен қағидаттары, халықаралық ақпараттық қауіпсіздік жүйесі негізінде нығайту бойынша бастамаларды жүзеге асыруды басымдық ретінде белгілеу арқылы ақпараттық саладағы халықаралық қоғамдастық қатысушылары арасында "цифрлық" айырмашылықты жоюға бағытталған Қазақстан Республикасының ұлттық мүдделерін сыртқы саяси және сыртқы экономикалық деңгейде дәйекті түрде ілгерілету.

Екіжақты және көпжақты дипломатия шеңберінде технологиялық даму жолын таңдауда мемлекеттердің егемендік теңдігі сөзсіз сақталған жағдайда АКТ-ны соғыс мақсаттарына пайдалануға қарсы ниеттегі, халықаралық ақпараттық қауіпсіздік саласындағы сенім шараларын нығайту, ашықтық бағдарын ұстанатын, қуатты әрі дәйекті серіктес ретінде Қазақстанның рөлін нығайтуды жалғастыру маңызды. Халықаралық, өңірлік және субөңірлік ұйымдар (БҰҰ, ШЫҰ, ЕАЭО, ҰҚШҰ, ТМД және т.б.) түйінді диалог алаңдарына айналуы тиіс, олардың бастамаларын түрлі халықаралық форматтарда бұдан әрі ілгерілету қажет.

"Қазақстанның киберқалқаны" тұжырымдамасын үйлестірілген түрде іске асыру Қазақстанның Киберқауіпсіздіктің жаһандық индексінде орнын едәуір ілгерілетуге және 2022 жылға қарай 0,600 индексіне жетуге көмектеседі.

**Қажетті ресурстар**

2017 – 2022 жылдары Тұжырымдаманы іске асыруға мүдделі мемлекеттік органдардың ағымдағы бюджеттік бағдарламалары аясындағы және "Цифрлы Қазақстан" мемлекеттік бағдарламасын іске асыру жоспарында көзделген мемлекеттік бюджет қаражаты бағытталатын болады.

## 6. Тұжырымдаманы іске асыру көзделетін нормативтік құқықтық актілердің тізбесі

Осы Тұжырымдаманы іске асыру кезеңінде қойылған міндеттерге және мақсаттарға жету мынадай нормативтік құқықтық актілер арқылы жүзеге асыру болжамдалады:

1. 2014 жылғы 3 шілдедегі Қазақстан Республикасының Қылмыстық кодексі.

2. 2014 жылғы 5 шілдедегі "Әкімшілік құқық бұзушылық туралы" Қазақстан Республикасының Кодексі.

3. 2015 жылғы 29 қазандағы Қазақстан Республикасының Кәсіпкерлік Кодексі.

4. "Жедел-іздестіру қызметі туралы" 1994 жылғы 15 қыркүйектегі Қазақстан Республикасының Заңы.

5. "Қазақстан Республикасындағы банктер және банк қызметі туралы" 1995 жылғы 31 тамыздағы Қазақстан Республикасының Заңы.

6. "Электрондық құжат және электрондық цифрлық қолтаңба туралы" 2003 жылғы 7 қаңтардағы Қазақстан Республикасының Заңы.

7. "Байланыс туралы" 2004 жылғы 5 шілдедегі Қазақстан Республикасының Заңы.

8. "Білім туралы" 2007 жылғы 27 шілдедегі Қазақстан Республикасының Заңы.

9. "Ғылым туралы" 2011 жылғы 18 ақпандағы Қазақстан Республикасының Заңы.

10. "Қазақстан Республикасының ұлттық қауіпсіздігі туралы" 2012 жылғы 6 қаңтардағы Қазақстан Республикасының Заңы.

11. "Дербес деректер және оларды қорғау туралы" 2013 жылғы 21 мамырдағы Қазақстан Республикасының Заңы.

12. "Азаматтық қорғау туралы" 2014 жылғы 11 сәуірдегі Қазақстан Республикасының Заңы.

13. "Рұқсаттар және хабарламалар туралы" 2014 жылғы 16 мамырдағы Қазақстан Республикасының Заңы.

14. "Ақпараттандыру туралы" 2015 жылғы 24 қарашадағы Қазақстан Республикасының Заңы.

15. "Мемлекеттік сатып алу туралы" 2015 жылғы 4 желтоқсандағы Қазақстан Республикасының Заңы.

16. "Ақпаратты Қазақстан – 2020" мемлекеттік бағдарламасы және "Мемлекеттік бағдарламалар тізбесін бекіту туралы" Қазақстан Республикасы Президентінің 2010 жылғы 19 наурыздағы № 957 Жарлығына толықтыру енгізу туралы" Қазақстан Республикасы Президентінің 2013 жылғы 8 қаңтардағы № 464 Жарлығы.

17. "Білім берудің тиісті деңгейлерінің мемлекеттік жалпыға міндетті білім беру стандарттарын бекіту туралы" Қазақстан Республикасы Үкіметінің 2012 жылғы 23 тамыздағы № 1080 қаулысы.

18. "Ақпараттық жүйені, "электрондық үкіметтің" ақпараттық-коммуникациялық платформасын, мемлекеттік органның интернет-ресурсын ақпараттық қауіпсіздік талаптарына сәйкестікке аттестаттаудан өткізу қағидаларын бекіту туралы" Қазақстан Республикасы Үкіметінің 2016 жылғы 23 мамырдағы № 298 қаулысы.

19. "Ақпараттық-коммуникациялық инфрақұрылым объектілерін ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілеріне жатқызу қағидалары мен өлшемшарттарын бекіту туралы" Қазақстан Республикасы Үкіметінің 2016 жылғы 8 қыркүйектегі № 529 қаулысы.

20. "Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарды бекіту туралы" Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы № 832 қаулысы.

21. "Телекоммуникациялар желілерінің өзара іс-қимыл жасауы мен орталықтан басқарудың бірыңғай қағидаларын бекіту туралы" Қазақстан Республикасы Инвестициялар және даму министрінің 2015 жылғы 29 қаңтардағы № 66 бұйрығы.

22. "Қауіпсіздік сертификатын беру қағидаларын бекіту туралы" Қазақстан Республикасы Инвестициялар және даму министрінің 2015 жылғы 25 желтоқсандағы № 1240 бұйрығы.

23. "Қауіпсіздік сертификатын қолдану қағидаларын бекіту туралы" Қазақстан Республикасы Инвестициялар және даму министрінің 2015 жылғы 25 желтоқсандағы № 1241 бұйрығы.

24. "Телекоммуникациялар желілерінде Қазақстан Республикасы заңнамасының талаптарын сақтау мәселелері бойынша мемлекеттік органдардың өзара іс-қимыл жасасу қағидаларын бекіту туралы" Қазақстан Республикасы Инвестициялар және даму министрінің міндетін атқарушының 2016 жылғы 25 қаңтардағы № 60 бұйрығы.

25. "Электрондық үкіметтің" ақпараттандыру объектілерінің ақпараттық қауіпсіздігін, қорғалуын және қауіпсіз жұмыс істеуін қамтамасыз етудің мониторингін жүргізу қағидаларын бекіту туралы" Қазақстан Республикасы Инвестициялар және даму министрінің міндетін атқарушының 2016 жылғы 26 қаңтардағы № 66 бұйрығы.

26. "Сервистік бағдарламалық өнімге, "электрондық үкіметтің" ақпараттық-коммуникациялық платформасына, мемлекеттік органның интернет-ресурсына және ақпараттық жүйеге олардың ақпараттық қауіпсіздік талаптарына сәйкестігіне сынақтар жүргізу әдістемесі мен қағидаларын бекіту туралы" Қазақстан Республикасы Инвестициялар және даму министрінің міндетін атқарушының 2016 жылғы 26 қаңтардағы № 63 бұйрығы.

27. "Интернетке қоғамдық қол жеткізу пункттерінде Интернетке қол жеткізудің қызметтерін көрсету қағидаларын бекіту туралы" Қазақстан Республикасы Инвестициялар және даму министрінің міндетін атқарушының 2016 жылғы 26 қаңтардағы № 67 бұйрығы.

28. "Қалааралық және халықаралық байланыс операторларының желілерін интернет-трафик алмасу нүктесіне жалғау қағидаларын бекіту туралы" Қазақстан Республикасы Инвестициялар және даму министрінің міндетін атқарушының 2016 жылғы 26 қаңтардағы № 65 бұйрығы.

29. "Ақпараттық жүйені, "электрондық үкіметтің" ақпараттық-коммуникациялық платформасын, мемлекеттік органның интернет-ресурсын олардың ақпараттық қауіпсіздік талаптарына сәйкестігіне аттестаттық зерттеп-қарауды жүргізу әдістемесін бекіту туралы" Қазақстан Республикасы Инвестициялар және даму министрінің міндетін атқарушының 2016 жылғы 28 қаңтардағы № 108 бұйрығы.

30. "Интернеттің қазақстандық сегментінің кеңістігінде домендік аттарды тіркеу, пайдалану және бөлу қағидаларын бекіту туралы" Қазақстан Республикасы

Инвестициялар және даму министрінің міндетін атқарушының 2016 жылғы 28 қаңтардағы № 118 бұйрығы.