«ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ҚАРЖЫ НАРЫҒЫН РЕТТЕУ ЖӘНЕ ДАМЫТУ АГЕНТТІГІ»

РЕСПУБЛИКАЛЫҚ МЕМЛЕКЕТТІК МЕКЕМЕСІ

2020 жылғы 20 шілде
№ 69

Алматы қаласы

« ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ҰЛТТЫҚ БАНКІ»

РЕСПУБЛИКАЛЫҚ МЕМЛЕКЕТТІК МЕКЕМЕСІ

2020 жылғы 20 шілде
№ 89

Нұр-Сұлтан қаласы

БІРЛЕСКЕН ҚАУЛЫ

Қазақстан Республикасының қаржы секторы киберқауіпсіздігінің 2020-2022 жылдарға арналған стратегиясын бекіту туралы

Қазақстан Республикасы Үкіметінің 2017 жылғы 30 маусымдағы № 407 қаулысымен бекітілген Киберқауіпсіздік тұжырымдамасын («Қазақстанның киберқалқаны») іске асыру мақсатында Қазақстан Республикасының Қаржы нарығын реттеу және дамыту агенттігінің (бұдан әрі – Агенттік) Басқармасы және Қазақстан Республикасы Ұлттық Банкінің Басқармасы **ҚАУЛЫ ЕТЕДІ:**

1. Қоса беріліп отырған Қазақстан Республикасының қаржы секторы киберқауіпсіздігінің 2020-2022 жылдарға арналған стратегиясы бекітілсін.

2. Қазақстан Республикасы Ұлттық Банкінің Қауіпсіздік департаменті:

1) осы қаулыны Қазақстан Республикасы Ұлттық Банкінің ресми интернет-ресурсына орналастыруды қамтамасыз етсін;

2) осы қаулыны Қазақстан Республикасы Ұлттық Банкінің мүдделі бөлімшелеріне жіберсін.

3. Агенттіктің киберқауіпсіздік басқармасы:

1) осы қаулыны Агенттіктің ресми интернет-ресурсына орналастыруды қамтамасыз етсін;

2) осы қаулыны Агенттіктің мүдделі бөлімшелеріне жіберсін.

4. Осы бірлескен қаулының орындалуын бақылау Қазақстан Республикасы Ұлттық Банкінің Төрағасына және Агенттік Төрағасының бірінші орынбасарына жүктелсін.

5. Осы бірлескен қаулы қабылданған күнінен бастап күшіне енеді.

Қазақстан Республикасының Қаржы нарығын реттеу және дамыту агенттігінің Төрағасы	**Қазақстан Республикасы Ұлттық Банкінің Төрағасы**
_____М. Әбілқасымова	**_____ Е. Досаев**

Қазақстан Республикасының
Қаржы нарығын реттеу және
дамыту агенттігі Басқармасының
2020 жылғы 20 шілдедегі № 69
және Қазақстан Республикасы
Ұлттық Банкі Басқармасының
2020 жылғы 20 шілдедегі № 89
бірлескен қаулысымен
бекітілді

Қазақстан Республикасының қаржы секторы киберқауіпсіздігінің 2020-2022 жылдарға арналған стратегиясы

1-тарау. Кіріспе

Қазіргі заманғы қаржы ұйымы түрлі автоматтандырылған ақпараттық жүйелер, телекоммуникациялық желілер, стационарлық компьютерлер мен мобильдік қондырғылар кешенінен тұрады.

Қаржы нарығында ақпараттық-коммуникациялық технологияларды (бұдан әрі – АКТ) дамыту, сондай-ақ қаржылық қызметтерді қашықтан көрсетудің белсенді түрде өсуі киберкеңістіктегі ақпараттық жүйелердің ақпаратының конфиденциалдылығы, тұтастығы мен қолжетімділігі (банк құпиясы, коммерциялық ақпарат немесе заңмен қорғалатын өзге құпия, дербес деректер) бұзылуымен байланысты тәуекелдерді арттырады.

Мұндай жағдайларда кибершабуылдардан қорғауды қоса алғанда, киберқауіпсіздіктің тиісті деңгейін қамтамасыз ету қажет. Кибершабуылдар кез келген мемлекеттің заманауи қаржы жүйесінің қауіпсіздігіне қауіп төндіретін ең маңызды қауіп болып табылады, сондықтан да киберқауіпсіздік ұлттық қауіпсіздіктің маңызды және ажырамас бөлігі болып табылады.

Қаржылық қызметтерді тұтынушылар үшін қашықтан көрсетілетін қызметтердің қауіпсіздігіне, сапасына, құнына және тізбесіне қанағаттану маңызды болып табылады. Қаржы ұйымдарының алдында, өз кезегінде, қамтамасыз етуге кеткен тиісті шығындар кезінде киберқауіпсіздік тәуекелдер деңгейін тиімді басқару мақсаты тұр. Өзінің қаржы делдалы функциясын барынша тиімді әрі қауіпсіз жүзеге асыра алатын қаржы нарығын қалыптастыру қоғам мен мемлекет үшін де, қаржы ұйымдары үшін де ортақ мақсат болып табылады.

Бұл ретте киберқылмыс проблемасында жаһандық сипат бар. Қазіргі заманғы АКТ қылмыскерлердің жасырын күйінде қалуына мүмкіндік береді, ал киберкеңістіктегі айналыста жүрген қаржы қаражатының ұлғайып жатқан көлемі осы қылмыстық қызметке адамдарды барынша көп тартуда.

Кибершабуылдарды жүзеге асыру үшін «дайын» шешімдерді әзірлеу жекелеген сала болды, онда киберқару саласындағы мемлекеттік арнайы қызметтердің жетістіктері де пайдаланылады. Ұсынылып отырған шешімдер функционалы пайдаланушыдан арнайы техникалық білімді талап етпейді, бұл осы саладағы қылмыстық қоғамдастықтың мүмкіндіктерін айтарлықтай ұлғайтады. Банк клиентінің қаражатын иелену, дербес деректер мен коммерциялық ақпаратты ұрлау, компанияларға шығын келтіру мақсатында ақпараттық жүйелерді немесе коммуникация құралдарын қасақана бүлдіру мақсатында қаржылық қызметтерді тұтынушылардың деректерін ұрлау немесе қашықтан банктік қызмет көрсету жүйесіне рұқсатсыз қолжетімділікті алу – киберқылмыстың қарқынды дамуымен байланысты қауіптердің едәуір толық емес тізбесі.

Қаржы секторын қоса алғанда, экономиканың түрлі секторларында мемлекетаралық деңгейде ықпалдасу процестерін де ескеру қажет. Қазақстан Республикасы мен оның қаржы жүйесі әлемдік үрдістерден тыс қалып жатқан жоқ. Қазақстан Республикасының жаһандық процестерге ықпалдасуы, бір жағынан, көрсетілетін қаржылық қызметтердің сапасын арттырып, аясын кеңейтуге тиіс болса, екінші жағынан, елдің қаржы жүйесінің ішкі және сыртқы киберқауіптер алдында осалдық дәрежесін арттырады.

Мұндай жағдайларда киберқауіпсіздік тәуекелдерінің іске асу ықтималдығы мен салдарлары барынша азайтылған кезде киберқылмыскерлердің қызметін реттеу мен алдын алудың оңтайлы тетіктерін әзірлеу қажет, бірақ бұл ретте шектеулер шектен тыс болып табылмайды және елдің халықаралық қаржы нарығындағы дамуына кедергі келтірмейді.

2-тарау. Терминдер мен ұғымдар

Киберкеңістік – адамдардың, бағдарламалық қамтамасыз етудің және сервистердің технологиялық қондырғылар мен желілердің көмегімен Интернет желісінде өзара іс-қимылы нәтижесінде қалыптастырылған кешенді виртуалды орта.

Кибершабуыл – ақпараттық ресурстың қорғалу жай-күйін рұқсатсыз өзгерту мақсатында оны бақылау алуға (құқықтарды арттыруға) бағытталған іс-қимыл немесе олардың кешені: рұқсатсыз қолжетімділік пен оны басқарудан бастап, рұқсатсыз модификациялау мен жоюға дейін.

Киберқауіпсіздік – киберкеңістіктегі ақпараттық қауіпсіздік, электрондық нысандағы ақпаратты және оны өңдеу, сақтау, беру (электрондық ақпараттық ресурстарды, ақпараттық жүйелерді және ақпараттық-коммуникациялық инфрақұрылымды) ортасын ішкі және сыртқы қауіптерден қорғаудың жай-күйі.

Киберқару – киберкеңістікке зиян келтіруге арналған бағдарламалық қамтамасыз ету немесе жабдық.

Киберқылмыс – киберкеңістікте ақпараттық технологияларды пайдалана отырып жасалатын кінәлі қоғамдық қауіпті іс-қимыл (іс-әрекет немесе әрекетсіздік).

Тұжырымдама – Киберқауіпсіздік тұжырымдамасы («Қазақстанның киберқалқаны»).

Киберқауіпсіздікті қамтамасыз ету – киберкеңістікте ақпараттың конфиденциалығын, тұтастығын және қолжетімділігін сақтау.

Скимминг – арнайы оқу құрылғысының көмегімен банк картасының деректерін рұқсатсыз алу.

Фишинг – пайдаланушылардың конфиденциалды деректеріне қолжетімділікті алу мақсаты болып табылатын интернет-алаяқтық түрі.

3-тарау. Мақсаты мен сипаты

Қазақстан Республикасының қаржы секторы киберқауіпсіздігінің 2020-2022 жылдарға арналған стратегиясында (бұдан әрі – Стратегия) мақсаттар, міндеттер мен іс-шаралар кешені сипатталады, оларға қол жеткізу, шешу және іске асыру Қазақстан Республикасы қаржы нарығының киберқауіпсіздігін қамтамасыз етудің тиімді жұмыс істейтін жүйесін (бұдан әрі – киберқауіпсіздікті қамтамасыз ету жүйесі) құруды қамтамасыз етуге мүмкіндік беретін. Стратегияда Қазақстан Республикасының қаржы нарығының киберқауіпсіздігін қамтамасыз ету жүйесінің құрылымы, оның негізгі қатысушылары, қойылған міндеттерді іске асыру шеңберінде олардың рөлі мен жауапкершілігі айқындалады. Стратегия бірінші кезекте киберқауіпсіздікті қамтамасыз ету жүйесі шеңберінде қатысушылар арасында тиімді коммуникацияларды құруға бағытталған. Қазақстан Республикасының қаржы нарығының (бұдан әрі – қаржы нарығы) тұрақты жұмыс істеп тұруы мен дамуын қамтамасыз ету үшін қажетті қаржылық қызметтерді қауіпсіз ұсыну үшін жағдайлар жасау Стратегияның негізгі мақсаты болып табылады.

Стратегияда қаржы нарығының киберқауіпсіздігінің ағымдағы жай-күйіне, сондай-ақ киберортада туындайтын ілеспе тәуекелдерге шолу қамтылған және киберқауіпсіздікті қамтамасыз ету жүйесін ұйымдастыру тәсілі мен қойылған мақсаттарға жету үшін орындалуы қажетті міндеттер ұсынылады.

4-тарау. Ағымдағы жағдайға шолу

4.1. Қаржы нарығындағы кибертұрақтылық пен киберқауіпсіздіктің жай-күйіне шолу

Киберқауіпсіздіктің жаһандық индексінде (Global Cybersecurity Index) 2019 жылы Қазақстан Республикасы 40 орында тұр. Киберқауіпсіздікті

қамтамасыз ету жөніндегі халықаралық қызметтердің деректері бойынша жыл сайын әлемде 556 млн жуық киберқылмыс жасалады, оларды келтірілген зиян 100 млрд АҚШ долларынан астам болады.

Ақпараттық қауіпсіздікті қамтамасыз ету саласындағы уәкілетті органның деректері бойынша 2018 жылдан бастап Қазақстан Республикасының Ұлттық ақпараттық қауіпсіздігінің үйлестіру орталығы (бұдан әрі – ҚР ҰАҚҰО) отандық инфрақұрылымға (мемлекеттік органдардың, жеке ұйымдардың және басқа кәсіпорындардың инфрақұрылымына) 2 млрд-тан астам кибершабуылға төтеп берді.

Бұл ретте екінші деңгейдегі банктерге ғана киберқылмыскерлер ай сайын алаяқтық транзакциялардың 5000 астам әрекетін жүзеге асырады. Ақшаны жымқырудың негізгі арнасы қашықтан қызмет көрсету арналары (мобильдік банкинг, интернет-банкинг және банкоматтар) болып табылады.

2019 жылдың ішінде Қазақстан Республикасының Ұлттық Банкіне (бұдан әрі – Ұлттық Банк) Қазақстанның екінші деңгейдегі банктерінің орын алған кибер оқыс оқиға салдары бойынша 30 астам өтініштері тіркелді. Өз кезегінде Ұлттық Банк пен Қазақстан Республикасының Қаржы нарығын реттеу және дамыту агенттігі (бұдан әрі – Агенттік) қаржы нарығының субъектілеріне 200 астам ескерту мен ақпараттық хабар дайындап, жіберді. Кибер оқыс оқиға мен кибершабуыл ауқымында: DDoS шабуылдары, зиянды кодты және бағдарламалық қамтамасыз етуді жұқтыру әрекеттері, банктердің инфрақұрылымына рұқсатсыз кіру әрекеттері, банкоматтарда скиммингтік құрылғыларды қолдану, Қазақстан Республикасының жеке және заңды тұлғаларының дербес және банктік деректерін жымқыруға арналған фишингтік ресурстарға әлеуметтік желілер мен мессенджерлер арқылы сілтемелерді тарату қамтылады.

Жеке тұлғаларға кибершабуылдардың ішінде кеңінен таралғаны әлеуметтік инженерия болуда, азаматтар түрлі психологиялық тәсілдердің ықпалымен өздерінің дербес деректерін, конфиденциалды ақпаратын немесе ақшалай қаражатын қаскүнемдерге береді.

Интернет-сервистерді пайдаланушылардың көпшілігінің цифрлық сауаттылығы төмен кезінде қаскүнемдер деректер мен ақшаны жымқыру әдістерін жетілдіруді жалғастыруда және бір-бірімен тығыз ынтымақтаса отырып, өздерінің тәжірибелерін біріктіреді.

Қазіргі кезде жақсы дайындалған қылмыстық топтар жүргізетін нысаналы кибершабуылдар қаржы нарығы үшін ең жоғары қауіпті білдіреді. Мысалы, әлемдік қоғамдастықта Cobalt, Silence және басқалары сияқты топтар барынша белсенді.

Сотқа дейін қаржы нарығындағы киберқылмыстар бойынша істердің аздаған саны ғана жететінін атап өтеміз, бұл құқық қорғау органдарында цифрлық қылмыстарды тергеудің тәртіпке келтірілген процесі болмауымен байланысты.

4.2. Ұлттық Банк 2020 жылға дейін іске асырған бастамаларға шолу

2017 жылғы 30 маусымда Қазақстан Республикасы Үкіметінің қаулысымен Тұжырымдама қабылданды, ол мемлекеттің электрондық ақпараттық ресурстарды, ақпараттық жүйелерді және телекоммуникациялар желілерін қорғау және АКТ қауіпсіз пайдаланылуын қамтамасыз ету саласындағы мемлекеттік саясатты іске асырудың негізгі бағыттарын айқындайды. Тұжырымдамаға сәйкес банктік ақпараттық жүйелер қауіпсіздігі жөніндегі талаптар ақпараттық жүйелердің қауіпсіздігін қамтамасыз ету жөніндегі салалық және халықаралық талаптар ескеріле отырып, Қазақстан Республикасының нормативтік құқықтық актілерімен қамтамасыз етіледі.

2017 жылдан бастап Ұлттық Банк бірқатар заңнамалық бастамаларды жүзеге асырды, қаржы нарығындағы ақпараттық қауіпсіздікті қамтамасыз етуді реттейтін нормативтік құқықтық актілерді бекітті. Мәселен, «Ақпараттандыру туралы» 2015 жылғы 24 қарашадағы Қазақстан Республикасының Заңында қаржы нарығын қамтамасыз етуді үйлестіретін ақпараттық қауіпсіздіктің салалық орталығын құру пысықталған, Банктер мен банк операцияларының жекелеген түрлерін жүзеге асыратын ұйымдардың, кредиттік бюролардың, сақтандыру ұйымдарының ақпараттық қауіпсіздігін қамтамасыз етуге қойылатын талаптар, Микрокредиттерді электрондық тәсілмен ұсыну қағидалары, Ақпараттық технологиялар мен ақпараттық қауіпсіздік тәуекелдері бөлігінде екінші деңгейдегі банктер үшін тәуекелдерді басқару және ішкі бақылау жүйесін қалыптастыру қағидалары әзірленді және нормативтік құқықтық актілермен бекітілді.

2019 жылы тәуекелге бағдарланған тәсілді пайдалана отырып, 3 екінші деңгейдегі банктің, 3 сақтандыру ұйымының, 2 банк операцияларының жекелеген түрлерін жүзеге асыратын ұйымның қызметіне тексеру жүргізілді, бағалы қағаздар нарығында қызметті жүзеге асыру үшін рұқсат беру құжаттарын беру бөлігінде 3 құжаттамалық тексеру жүргізілді. Ақпараттық қауіпсіздіктің 5 оқыс оқиғасына тексеру жүргізуге (үшеуі - екінші деңгейдегі банктерде, сақтандыру компаниясында және кредиттік бюрода) қатысты.

ҚР БҚҰК-пен өзара іс-қимыл процесі шеңберінде оқыс оқиғалар бойынша ақпарат алмасудың автоматтандырылған жүйесіне - MISP (Malware information sharing platform) қосу жүзеге асырылды, 6 кибер оқыс оқиғаны өңдеуге қатысты, 8 алаяқтық сайттарды бұғаттау жүзеге асырылды.

2019 жылы Ресей Қаржы Банкімен (кредит-қаржы саласындағы компьютерлік шабуылдарға мониторинг жүргізу және ден қою орталығы, Ресей Орталық банкінің арнайы құрылымдық бөлімшесі) өзара іс-қимыл шеңберінде 4 оқыс оқиғаны өңдеуге қатысты, 5 алаяқтық сайтты бұғаттау жүзеге асырылды.

Халықаралық ынтымақтастық шеңберінде Еуразиялық экономикалық одақ туралы шартқа (бұдан әрі – ЕАЭО) мүше мемлекеттердің орталық (ұлттық) банктерінің кредит-қаржы саласындағы қаржы нарығының ақпараттық қауіпсіздігін қамтамасыз ету және компьютерлік шабуылдарға қарсы іс-қимыл

мәселелері бойынша жұмыс тобы құрылды. Алматы қаласында оның бірінші күндізгі отырысы өткізілді, онда 2021 жылға дейінгі жұмыс жоспары әзірленді және бекітілді.

2019 жылы Ұлттық Банк қаржы нарығының субъектілеріне 11 ақпараттық таратылым, 117 ақпараттық қауіпсіздікке тіркелген шабуылдар мен қауіп-қатерлер туралы ескертулерді дайындады және жіберді, екінші деңгейдегі банктерден алынған 47 ақпараттық оқыс оқиғалар картасын өңдеді.

2019 жылы екінші деңгейдегі банктердің ақпараттық-коммуникациялық инфрақұрылымын ақпараттық қауіпсіздікті қамтамасыз ету саласындағы уәкілетті орган ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілеріне жатқызған.

Бұл ретте 2020 жылғы 1 қаңтардан бастап «Қазақстан Республикасының Мемлекеттік басқару жүйесін одан әрі жетілдіру туралы» Қазақстан Республикасы Президентінің 2019 жылғы 11 қарашадағы № 203 Жарлығына сәйкес Агенттік құрылды.

Осылайша, қаржы нарығының субъектілері ақпараттық қауіпсіздікті қамтамасыз ету саласындағы уәкілетті органның, Агенттіктің және Ұлттық Банктің талаптары қолданылатын үш жақты реттеу жағдайында болды.

Қазіргі уақытта Агенттік қаржы нарығына қатысушылармен киберқауіпсіздік туралы ақпарат алмасудың базалық процесін жасады.

Агенттік қызметкерлерінің қаржы нарығындағы кибер оқыс оқиғаларды тексеру бөлігіндегі құзыреті артады. Екінші деңгейдегі қазақстандық банктерде ақша қаражатын ұрлау фактілерін тексеруде уәкілетті органдарға көмек көрсетіледі.

Қаржы нарығының ақпараттық қауіпсіздігінің бірыңғай жүйесін құру кезінде қаржылық реттеушінің Агенттік пен Ұлттық Банкке бөліну фактісін, сондай-ақ «Астана» халықаралық қаржы орталығының (бұдан әрі – АХҚО) қатысуын ескеру қажет.

Бірінші кезекте Агенттік пен Ұлттық Банктің ақпараттық-коммуникациялық құрылымы қаржы нарығының ақпараттық қауіпсіздігін қамтамасыз етуге қойылатын талаптарға сәйкес болуы тиіс.

Агенттіктің Ұлттық Банкпен төлем қызметтерін реттеу және қаржылық технологияларды дамыту сияқты, сондай-ақ АХҚО-мен қаржылық технологиялар бағытында оның қызметінің бағыттары бойынша тығыз ынтымақтастығы қажет.

5-тарау. Ағымдағы проблемалар мен даму бағыттары

5.1. Қаржы секторы субъектілерінің киберқауіпсіздігін қамтамасыз ету жүйелерін реттеуді жетілдіру

Қазақстан Республикасы қаржы секторының киберқауіпсіздік мәселелерінде нормативтік құқықтық қамтамасыз ету ағымдағы күннің қажеттілігінен айтарлықтай қалып отыр. Киберқауіпсіздікті қамтамасыз ету жүйелері жұмыс істеген кезде негіз ретінде тәуекелге бағдарланған тәсілді пайдалану үзінді түрде жүзеге асырылады. Қазіргі уақытта тәуекелге бағдарланған тәсілді пайдалану бойынша талаптар банктерге және банк операцияларының жекелеген түрлерін жүзеге асыратын ұйымдарға қолданылады. Қаржылық ақпараттың түрлерін, ақпараттық ресурстарды, өнімдерді, қызметтерді іздеуді, алуды және тұтынуды жүзеге асыру кезінде туындайтын ақпараттық құқықтық қатынастарды реттейтін құқықтық тетіктер жеткілікті түрде пысықталған жоқ.

Қаржы ұйымдарын міндетті бақылау мен қадағалау саласында олар ұсынатын киберқауіпсіздікті қамтамасыз етуге қатысты кемшіліктер бар. Мәселен «Қаржы нарығы мен қаржы ұйымдарын мемлекеттік реттеу, бақылау және қадағалау туралы» Қазақстан Республикасы Заңының талаптары қаржы ұйымдарындағы қадағалау және бақылау шараларын көздемейді. Киберқауіпсіздік бойынша талаптар сақталмаған жағдайда қаржы ұйымдарына ықпал ету шаралары мен тетіктері жоқ.

Киберқылмыстарға қарсы іс-әрекеттерді құқықтық қамтамасыз етудің қазіргі заманғы жай-күйі пайдаланылатын құқықтық тетіктерді келіспеушіліктің әлсіз болуымен, заңнамалық бастама субъектілерінің қызметінде оларды дамыту мен жетілдіру бойынша жүйеліктің болмауымен, құқықтық нормалардың жеткілікті түрде тиімді және қарама-қайшы болмауымен, құқықтық статистиканың мүлтіксіз болмауымен және мүдделі тараптар өзара әрекет еткен кездегі үйлестірудің әлсіз болуымен сипатталады.

Киберқауіпсіздік тәуекелдерін басқару процестерін реттеу, сондай-ақ киберқауіпсіздікті қамтамасыз ету жүйелерін салу қаржы ұйымдарының барлық әр түрлілігін есепке алмағанда, үзінді түрінде жүзеге асырылады.

Субъектілерді тексеру үшін таңдау кезінде тәуекел дәрежесін ағымдағы бағалау киберқауіпсіздік өлшемшарттары мен тәуекелдерін ескермейді. Қаржы ұйымдарының жалпы санын, қаржы нарығында ақпараттық технологиялардың қарқынды дамуын және соның салдарынан киберқауіпсіздік тәуекелдерін ескере отырып, сондай-ақ Агенттіктің қолда бар ресурстық шектеулерін ескере келе, барлық қадағалаудағы субъектілердің жоспарлы негізде тиісті бақылауды және сәйкестігін бағалауды жүзеге асыру мүмкін емес. Киберқауіпсіздіктің жай-күйін тексеру сапасын арттыру қажет.

Ақпараттық қауіпсіздіктің және ақпараттық тәуекелдерді басқарудың заңнамалық және нормативтік талаптарын нарықтың сақтауын бақылау тиімділігі төмен деңгейде қалып отыр. Ағымдағы жағдайды талдау қаржы ұйымдарына қойылатын талаптар қаржы ұйымдарындағы мәдениет тәуекелінің төмен деңгейіне, ақпараттық қауіпсіздік қатерлерінен объектілердің қорғалу деңгейі жеткіліксіз болған, қаржы ұйымдары басшылығының киберқауіпсіздікті басқару процесіне тартылу деңгейі төмен болған жағдайда маңызды ықпал ету

шараларын қолданудың болмауына байланысты тиісті көлемде орындалмайтынын көрсетеді, бұл киберқауіпсіздік тәуекелдерінің артуына, ұйымдардың киберқауіпсіздік қатерлеріне өз бетінше қарсы тұра алмауына әкеп соғады, қаржылық қызметтерді пайдалану кезінде жеке және заңды тұлғалардың киберқауіпсіздігі тиісті шамада қамтамасыз етілмейді.

Қаржы ұйымдарының киберқауіпсіздігін реттеуді жетілдіру, мүдделі тараптар арасында сапалы коммуникацияларды құру, тәуекелдер дәрежесін бағалау және ақпараттық және киберқауіпсіздік өлшемдері негізінде ранжирлеуді ескере отырып, тексерулерді дербес жүргізуге көшу, әкімшілік жаза түрінде ықпал ету шараларын қолдану қорғалу деңгейі төмен қаржы ұйымдарының, сондай-ақ тұтастай алғанда қаржы нарығының киберқауіпсіздігін бақылауды және қамтамасыз етуді күшейтуге мүмкіндік береді.

5.2. Қаржы нарығының ақпараттық қауіпсіздігінің салалық орталығын дамыту

Қаржы ұйымдарында киберқауіпсіздікті қамтамасыз ету жүйесінің жұмыс істеу тиімділігінің жеткіліксіздігі байқалады. Бұл жағдай бірнеше факторларға байланысты. Бірінші кезекте қаржы ұйымдары бедел тәуекелдеріне байланысты едәуір шығындардан қорқып, ақпараттық қауіпсіздік тәуекелдерін іске асырумен байланысты шығындарды жарияламауды қалайды. Осының салдарынан, әрбір қаржы ұйымында ақпараттық қауіпсіздікті қамтамасыз ету бағыты тұйықталады. Осының салдарынан қаржы ұйымдарының ақпараттық қауіпсіздік мамандарының дайындық деңгейі өзгермелі қауіп-қатерлермен бірге өспейді, киберқауіптер бойынша ақпаратпен алмасу шектеледі, реттеуші қаржы нарығындағы кибертәуекелдермен ахуал туралы жеткілікті хабардар емес.

Реттеуіштің жеткіліксіз хабардар болуы қаржы нарығында киберқауіпсіздікті қамтамасыз етуді жетілдіру және қаржы ұйымдары анықтаған кибер оқыс оқиғаларға ден қою бойынша барабар шараларды әзірлеуге мүмкіндік бермейді.

Қаржы нарығында кибер оқыс оқиғалар бойынша ақпарат алмасудың автоматтандырылған жүйесінің болмауы киберқылмыскерлерге қарсы іс-қимыл бойынша іс-шараларды жедел жүргізуге мүмкіндік бермейді.

Сонымен қатар, киберқауіпсіздікті қамтамасыз ету қолданыстағы ресурстарды тиімді пайдалануды және барлық мүдделі тараптарды тарта отырып, тиісті көп деңгейлі ұйымды білдіреді.

Киберқауіпсіздікті қамтамасыз ету жүйесінің негізгі қатысушылары тұтынушылар (жеке және заңды тұлғалар), қаржылық және төлем қызметтерін берушілер (банктер, банк операцияларының жекелеген түрлерін жүзеге асыратын ұйымдар, сақтандыру ұйымдары, бағалы қағаздар нарығының кәсіби қатысушылары, төлем ұйымдары және басқа (өзге) ұйымдар), Агенттік, Ұлттық Банк және АХҚО болып табылады.

Агенттікте қалыптасқан жағдайды түзету мақсатында ақпараттық қауіпсіздіктің салалық орталығы (бұдан әрі – салалық орталық) құрылды. Агенттік оның тұрақты жұмысы үшін қажетті жағдайларды қамтамасыз ететін болады. Салалық орталықтың міндеттеріне ҚР БҚҰК-пен, компьютерлік оқыс оқиғаларға ден қоюдың мемлекеттік және жеке орталықтарымен, сондай-ақ арнайы мемлекеттік және құқық қорғау органдарымен өзара іс-қимыл кіреді. Салалық орталық қаржы нарығының киберқауіпсіздігі бойынша халықаралық ынтымақтастық үшін бірыңғай байланыс орталығы болып табылады.

Қаржы нарығының киберқауіпсіздігін қамтамасыз ету үшін жедел деңгейде Агенттіктің салалық орталығы киберқауіпсіздік оқыс оқиғаларын басқаруға құрылымдық тәсілді енгізуге ықпал етеді.

Қаржы нарығының киберқауіпсіздігін қамтамасыз ету төрт негізгі элементтен тұрады:

1) киберқауіпті бақылау және анықтау;

2) кибер оқыс оқиғалардың алдын алу (болдырмау);

3) кибер оқыс оқиғаларға ден қою;

4) киберқауіпсіздік мәселелері бойынша хабардарлықты арттыру.

Қаржы ұйымдарының киберқауіпсіздігін қамтамасыз ету үшін Агенттіктің салалық орталығы қаржы нарығындағы оқыс оқиғалардан тікелей және жанама залалды азайту мақсатында киберқауіпсіздік оқыс оқиғаларының теріс әсерін болдырмауға немесе тежеуге жәрдемдеседі.Осы мақсаттар үшін салалық орталық шеңберінде қаржы нарығындағы киберқауіпсіздік оқыс оқиғаларына ден қою қызметін құру қажет, ол қаржы нарығындағы киберқауіпсіздіктерге жедел әрекет ете алады, киберқауіпсіздіктің ағымдағы және әлеуетті қатерлері туралы, оның ішінде қаржы нарығының ақпарат алмасу және талдау орталығының мүмкіндіктерін пайдалана отырып, жедел режимде бар өзекті ақпаратты ала алады және тиісті ұсыныстарды қаржы және төлем ұйымдарына жеткізу қажет.

Қаржы нарығын реттеу деңгейінде Агенттік төлем қызметтері нарығының жұмыс істеуін өзгертуге және инновациялық қаржы технологияларын олардың ақпараттық қауіпсіздік талаптарына сәйкестігі мәніне енгізуге байланысты бастамаларды Ұлттық Банкпен келісуді жалғастырады және осы бастамалар бойынша АХҚО-мен жұмысты бастайды.

Қаржылық және төлем қызметтерін тұтынушылар мен жеткізушілерден, үйлестіру орталықтарынан басқа, «Қазақстан қаржыгерлерінің қауымдастығы» заңды тұлғалардың бірлестігі, байланыс операторлары, қызмет провайдерлері, медиа-қоғамдастық, білім беру институттары, кәсіби қауымдастықтар мен киберқауіпсіздік саласындағы қауымдастықтар, сондай-ақ Агенттікке, Ұлттық Банкке және ақпарат, ақпараттандыру және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы уәкілетті органдарға қолдау көрсететін бағдарламалық және аппараттық қамтамасыз етуді жеткізушілер өз облыстарында өткізілетін іс-шаралар бойынша сараптамалық пікір бере отырып, сондай-ақ шараларды іске

асыруға және киберқауіпсіздікті бақылауға көмек көрсете отырып маңызды рөл атқаруы тиіс.

Қаржы ұйымдарына қызмет көрсету кезінде мемлекеттік ақпараттық ресурстарға (жеке және заңды тұлғалардың мемлекеттік деректер қорына), мемлекет қатысатын кредиттік бюроның деректер базасына қол жеткізуі жиі талап етіледі, ол үшін олар жүйеаралық өзара іс-қимылды жолға қою қажет. Бұл бір ұйымның ақпараттық ресурсындағы осалдық басқа ұйымның жұмысына әсер ететінін білдіреді.

Елде ақпараттық қауіпсіздіктің бірыңғай жүйесін құру үшін киберқауіпсіздік оқыс оқиғалары бойынша ақпаратты жинауды және талдауды қамтамасыз ететін, компьютерлік қауіпсіздік қатерлерін мониторингтеу және болдырмауда пайдаланушыларға консультациялық және техникалық қолдау көрсетуді жүзеге асыратын ҚР БҚҰК құрылды.

Сонымен қатар, қаржы нарығының киберқауіпсіздігін қамтамасыз етудің тиімді жүйесін әзірлеу үшін ақпараттық қауіпсіздікті қамтамасыз ету саласындағы уәкілетті орган, ҚР БҚҰК және ақпараттық қауіпсіздіктің салалық орталығы ретінде Агенттік өкілеттіктерінің нақты иерархиялық құрылымын құру жоспарында заңнаманы пысықтау талап етіледі.

Жүйе ақпараттық қауіпсіздікті қамтамасыз ету саласындағы уәкілетті орган әзірлеген тұжырымдамалар, стратегиялар, заңдар түріндегі тұжырымдамалық талаптар ретінде Агенттік және Ұлттық Банк өз өкілеттіктері шегінде өз деңгейінде қаржы нарығы субъектілерінің ақпараттық қауіпсіздігін басқару жүйелерін ұйымдастыруға, сондай-ақ олардың негізінде субъектілерді тексеру жүзеге асырылатын тосын оқиғаларды өңдеуге қойылатын жан-жақты және нақтыланған талаптарды әзірлейтін болады.

Осылайша есептілік жүйесі құрылатын болады – Агенттік сала бойынша есептілікті біріктіріп, оны ақпараттық қауіпсіздікті қамтамасыз ету саласындағы уәкілетті органға беретін болады.

Ақпараттық қауіпсіздік оқыс оқиғаларын өңдеу бөлігінде тәсіл ұқсас болады. Агенттіктің салалық орталығы өз деңгейінде оқыс оқиғаларды өңдеуді қабылдайды және үйлестіреді. Ресурстар жетіспеген немесе бүкіл елдің инфрақұрылымы үшін қауіп төнген жағдайда ҚР БҚҰК тартылады. Сонымен қатар, салалық орталық өз саласы бойынша құзыретті орталық болып табылады. Яғни, ҚР БҚҰК салада қауіп-қатер туралы ақпарат болған жағдайда, ҚР БҚҰК қауіп-қатер деңгейіне сараптамалық баға береді және қауіптерді өңдеу бойынша іс-шараларды ұсынады.

Ақпараттық қауіпсіздіктің салалық орталығының өз мемлекеттерінің қаржы нарығының киберқауіпсіздігін қамтамасыз ететін шетелдік орталықтармен өзара іс-қимылын қолдау және дамыту қажет. Мұндай ынтымақтастық Қазақстан Республикасынан тыс жерлердегі киберқауіптер көздерімен тиімді күресуге мүмкіндік береді.

5.3. Төлем жүйелерінің, көрсетілетін төлем қызметтері нарығының және көрсетілетін цифрлық қаржы қызметтерінің киберқауіпсіздігі

Төлем жүйелері қаржы нарығының маңызды инфрақұрылымы болып табылады және төлем жүйелері арқылы қор нарығының, бағалы қағаздар нарығының, мемлекеттік сектордың айтарлықтай қаржылық операциялары жүргізілетіндіктен, нарыққа қатысушылардың сеніміне ие болуға тиіс. 2019 жылы Ұлттық Банктің төлем жүйелері арқылы 762,0 трлн теңгеге 41,6 млн транзакция жүргізілді. 2019 жылы бір күн ішінде орташа алғанда 3108,9 млрд теңгеге 169,3 мың транзакция өңделді.

Төлем жүйелері қызметінің үздіксіздігін қамтамасыз ету Ұлттық Банктің бірінші кезектегі міндеттерінің бірі болып табылады. Осы міндетті орындау шеңберінде Ұлттық Банктің қызметі, негізінен, төлем жүйелерінің операциялық сенімділігін арттыруға, төлемдерді жүргізуге кепілдік беруге, төлем жүйелерінің жүйелік тәуекелін реттеуге бағытталған.

Заманауи электрондық төлем тәсілдерінің жылдамдығымен, сапасымен және ыңғайлылығымен қатар, технологиялық тәуекелі де бар. Қолда бар ақпараттық тәуекелдерге және төлем жүйелеріне кибершабуылдардың орын алуына жедел ден қоюына қарамастан, кибершабуылдар әлі де жеткілікті жоғары деңгейде қалып отыр. Киберқылмыс жасаудың әдістері мен тәсілдері үнемі жетілдіріліп отырады, бұл мемлекет тарапынан үздіксіз назар аударуды, икемділікті және жеделдікті талап етеді. Осыған байланысты, Ұлттық Банк тарапынан төлем жүйелерінің киберқауіпсіздігін дамытудың одан әрі бағыты Қазақстан Республикасының аумағында жұмыс істейтін төлем жүйелерінің (оның ішінде халықаралық) қауіпсіздігіне қойылатын ең төменгі талаптарды әзірлеуге бағдарланатын болады.

Қазақстан Республикасында, сондай-ақ бүкіл әлемдегі сияқты цифрлық қызметтердің жылдам дамуы, ұтқыр және Интернет технологиялардың жаппай енуі, қолмен қызмет көрсетуден цифрлық онлайн сервистерге өту байқалады. Бүгінгі күні Интернет және мобильді банкинг жүйесінде 9,5 млн-нан аса белсенді пайдаланушы тіркелген. 2019 жылы онлайн транзакциялардың көлемі 10 трлн теңгені құрап, 2018 жылмен салыстырғанда 3 есеге өсті. Бизнес субъектілерінің қаржылық транзакцияларының 75%-на қашықтықтан қызмет көрсету арқылы қызмет көрсетіледі.

Инновациялық қаржылық қызметтердің дамуы, нарықта цифрлық қызметтерді ұсынатын жаңа институттардың пайда болуы ақпараттық қауіпсіздіктің маңыздылығын қайта қарау және арттыру алғышарттарын жасайды. Алаяқтық операцияларды жинау бойынша деректерді талдау 2019 жылы төлем карточкаларымен 337,4 млн теңге сомасына 15 858 алаяқтық операциялар тіркелгенін көрсетеді. 2018 жылмен салыстырғанда алаяқтық операциялардың саны 2,5 есеге өскені байқалады, бұл ретте операциялардың саны 37%-ға азайды. Жасалған алаяқтық транзакциялардың жалпы санынан

98%-ы шетелдік банктер желісінде қолма-қол ақшасыз тәсілмен жүзеге асырылған.

Киберқауіпсіздіктің қажетті деңгейін қамтамасыз ету үшін заманауи сандық қатерлерді уақтылы анықтау және оған қарсы тұру құралдарын әзірлеу талап етіледі. Ұлттық Банктің рөлі мен қызметі қаржы және төлем нарығының барлық қатысушыларын қамтитын электрондық банктік қызметтерді ұсыну жөніндегі қолданыстағы нормативтік құқықтық базасын жаңартуға бағытталады. Ұрлықтың алдын алу және банктер, төлем ұйымдары, төлем жүйесі операторлары тарапынан ақпараттық қауіпсіздікке қатысты оқыс оқиғаларға жауап беру әдістерін әзірлеу, осы әдістердің тиімділігін мерзімді тестілеу төлем инфрақұрылымын дамытуда киберқауіпсіздікті қамтамасыз етудің маңызды бағыты болып табылады.

Кибертұрақтылықты арттырудың одан арғы шаралары, соның ішінде төлем ұйымдары ретіндегі төлем нарығының жаңа қатысушыларына әсері тиеді. Төлем ұйымдарына олардың қызметінің ерекшелігін ескере отырып, ақпараттық қауіпсіздік оқыс оқиғаларға мониторинг жүргізу және оларға әрекет ету қызметтерін қосу жоспарлануда.

Қаржылық технологиялардың дамуымен жеке тұлғаны қашықтан сәйкестендіру тетігіне, мезеттік төлем жүйесіне, қаржылық маркетплейстерге ақпараттық қауіпсіздік талаптары мен стандарттарын әзірлеу сандық қаржылық экожүйенің негізгі құрылымдық элементтерінің қауіпсіздігін қамтамасыз етудің шешуші факторы болып табылады. Ұлттық Банк тарапынан осы шараларды қабылдауы қаржы нарығының қатысушылары үшін киберқауіптерді, оның ішінде клиенттердің дербес деректерін әшкерелеу тәуекелін азайтуға және сандық қаржылық қызметтерді қауіпсіз және сенімді деңгейде ұсынуға мүмкіндік береді.

5.4. Ғаламдық ауқымда киберқылмыспен күресу саласындағы ынтымақтастық

Компьютерлік шабуылдарға қарсы әрекет ету үшін басқа халықаралық орталықтармен ақпарат жинау, алмасу және талдау бойынша ынтымақтастық өзінің дамуының бастапқы кезеңінде келеді. Қол жеткізілген келісімдер шеңберінде ЕАЭО туралы шарт мүшелері - мемлекеттердің орталық (ұлттық) банктерімен ақпарат алмасу жүріп жатыр. Сонымен қатар, ол тек жекелеген жағдайлар.

Қаржы нарығының ақпараттық қауіпсіздігін қамтамасыз ету және ЕАЭО туралы шартқа қатысушы мемлекеттердің орталық (ұлттық) банктерінің кредит-қаржылық саласындағы компьютерлік шабуылдарға қарсы тұру жөніндегі жұмыс тобының шеңберінде 2022 жылға дейін бірқатар маңызды мәселелерді шешу межеленген, оның ішінде:

Еуразиялық экономикалық комиссияда және/немесе ЕАЭО орталық (ұлттық) банктерінде сенімді үшінші тарап негізінде қаржы нарықтары саласында ақпарат алмасудың жалпы өзара тиімді ережелерін пысықтау;

ақпараттық және киберқауіпсіздік, кибертұрақтылық және тиісті тәуекелдерді қадағалау мәселелері бойынша глоссарий жасау;

ақпараттық және киберқауіпсіздікті, кибертұрақтылықты және олардың жетілуіне қойылатын негізгі талаптарды қамтамасыз ететін процестердің өзара тиімді тізбесін қалыптастыру;

ақпараттық қауіпсіздіктің халықаралық және жергілікті/ұлттық стандарттарын қолдануды қоса алғанда, қадағалаудағы қаржы ұйымдарының тәуекел бейінінің ақпараттық және киберқауіпсіздігін, кибертұрақтылығын бағалаудың өзара тиімді әдістемесін қалыптастыру;

қорғалу мен сыртқы аудиттің талдауын жүзеге асыратын ұйымдарға қойылатын біліктілік талаптары бойынша өзара тиімді көзқарастарды қалыптастыру;

ЕАЭО елдерінде ақпараттық қауіпсіздікті қамтамасыз ету саласындағы маңызды / елеулі өзгерістерге мониторинг жүргізу үшін ұсыныстар әзірлеу;

клиенттің келісімінсіз операциялар туралы ақпарат алмасу ережелерін және осындай оқыс оқиғаларға жауап беру тетіктерін әзірлеу.

Осы бағытты дамыту үшін киберқауіпсіздік бойынша әртүрлі халықаралық шараларға қатысу, екіжақты және көпжақты келісімдер жасасу, төтенше жағдайларға компьютерлік әрекет ету топтарымен өзара тиімді әрекет ету үшін (computer emergency response team, CERT) халықаралық FIRST (Forum of Incident Response and Security Teams) форумына қатысу қажет.

Бұдан басқа, халықаралық деңгейде ынтымақтастық орнату үшін нормативтік құқықтық өрісті бірыңғай тұжырымдамалар мен талаптарға келтіру қажет, ол халықаралық стандарттарға сәйкес реттеуге толықтай көшуге ықпал ететін болады.

5.5. Халықтың киберсауаттылығын арттыру

Қашықтан банктік және басқа қаржылық қызметтерді тұтынушылар қаржы секторының қауіпсіздік құрылымындағы әлсіз буын болып табылады. Көптеген тұтынушылар қажетті сақтықты танытпайды және қашықтан қызмет көрсету арналарына тән тәуекелдер туралы толық хабардар болмайды. Қаржылық ұйымдар тарапынан тұтынушыларға қызметтерді алу кезіндегі қорғаныс тетіктері мен қажетті қауіпсіздік шаралары туралы ақпараттандыру бойынша жұмыстар толығымен жүргізілмейді.

Осылайша, халықтың киберсауаттылығын екі бағытта арттыру қажет. Біріншіден, бұқаралық ақпарат құралдарында Интернетте қаржылық қызметтерді пайдалану кезінде туындайтын киберқауіптерге жауап қайтарудың көкейкесті әдістерін жариялау қажет. Сондай-ақ, халықтың қаржылық

сауаттылығын арттыру бағдарламасына қашықтықтан қаржылық қызметтерді қауіпсіз алу бөлімдерін енгізу қажет.

5.6. Ұлттық Банкте және Агенттікте ақпараттық қауіпсіздікті басқару жүйесін жетілдіру

Қаржы секторының қауіпсіздігін тиімді қамтамасыз ету және оны реттеу Ұлттық Банк пен Агенттіктің ақпараттық қауіпсіздігін қамтамасыз ету жүйесі жұмыс істемеген жағдайда мүмкін емес.

«Ақпараттандыру туралы» Қазақстан Республикасының 2015 жылғы 24 қарашадағы Заңы Қазақстан Республикасындағы ақпараттық ресурстарды, ақпараттық жүйелер мен телекоммуникация желілерін қорғаудың талаптары мен шараларын айқындайтын негізгі құжат болып табылады, оның талаптары Ұлттық Банкке және оның құрылымына кіретін ұйымдарға, сондай-ақ Агенттіктің Ұлттық Банкпен интеграцияланған ақпараттық жүйелерінің бөлігіне қолданылмайды. Мұндай жағдайда Ұлттық Банк, оның еншілес ұйымдарын қоса алғанда, және Агенттік киберқауіпсіздікті қамтамасыз ету үшін тәсілдер мен талаптарды өз бетінше қалыптастыруы қажет.

Қазіргі уақытта Ұлттық Банкте және Агенттікте ұйымдастырылған ақпараттық қауіпсіздікті басқару жүйесі (бұдан әрі - АҚБЖ) ақпараттық қауіпсіздікті қамтамасыз ету процестерін іске асыру, мониторингі, талдау және қолдау үшін қолданылады.

Ұлттық банктің және Агенттіктің қолданыстағы АҚБЖ-ны одан әрі жетілдіру, кибертәуекелдерді басқару, кибер оқыс оқиғаларға тұрақты әрекет ету қызметін құру, заңнамалық деңгейде бекітілген талаптарға сәйкес ақпараттық қауіпсіздікті үйлестіруді қамтамасыз ету, қажетті техникалық қорғау шараларын уақтылы жүргізу бизнес-процестерді іске асыруға қажетті қолдау көрсетуге мүмкіндік туғызады.

АҚБЖ-ға түзетулерді енгізу және іске асыру кезінде халықаралық стандарттар мен Қазақстан Республикасының ақпараттық қауіпсіздік саласындағы мемлекеттік стандарттарының талаптары, әсіресе төлем инфрақұрылымдарының элементтеріне және мемлекеттік органдардың бірыңғай көліктік желісіне байланысты инфрақұрылымға қатысты талаптар ескерілетін болады.

Қаржы секторының негізгі қатысушыларының киберқауіпсіздігін қамтамасыз ету деңгейін арттыру үшін Ұлттық Банктің еншілес ұйымдарының АҚБЖ-ға қойылатын бірыңғай талаптарды қалыптастыру қажет.

Кез келген басқа қызмет саласындағы сияқты ақпараттық қауіпсіздікті қамтамасыз етуде бөлінген адам ресурстары мен олардың біліктілігінің маңызы зор. Бөлінген ресурстардың қазіргі деңгейі ақпараттық қауіпсіздікті қамтамасыз ету кезінде Ұлттық Банктің және Агенттіктің барлық бизнес-процестерін қамтуға және қаржылық реттеу процестеріне уақытылы қолдау көрсетуге

мүмкіндігі жеткіліксіз. Ақпараттық қауіпсіздікті және оның құзыретінің сапасын қамтамасыз етуге жауапты қызметкерлер санын одан әрі арттыру қажет.

6-тарау. Стратегияны іске асыру мақсаттары мен міндеттері

6.1. Қаржы нарығы субъектілерінің киберқауіпсіздігін қамтамасыз ету жүйелерін реттеуді жетілдіру	
Мақсаттары	Міндеттері
- реттеудің барлық кезеңдерінде тәуекелге бағдарланған тәсілді ендіру;	- қаржы секторын тәуекелге бағдарланған тәсілді қолдануға бағытталған ақпараттық қауіпсіздік саласындағы өзекті нормативтік құқықтық базамен қамтамасыз ету; - киберқауіпсіздік бойынша талаптарды орындау бөлігінде қары ұйымдарын тәуекелге бағдарланған бақылауды қамтамасыз ету;
- киберқауіпсіздік саласында талаптар бұзылған жағдайда ықпал ету шаралары жүйесін енгізу арқылы ұйым басшысын тарта отырып, қаржы ұйымдарындағы ақпараттық қауіпсіздікті қамтамасыз ету процестерінің сапасын арттыру;	- киберқауіпсіздік саласында талаптар бұзылған жағдайда қаржы ұйымдарына ықпал ету тетіктерін регламенттеу;
- халықаралық стандарттарды есепке ала отырып, ақпараттық қауіпсіздікті реттеудің бірыңғай мемлекеттік жүйесі шеңберінде қаржы нарығына заңнамалық және нормативтік талаптарды үйлесімді қалыптастыру.	- тәсілдерді үйлестіру және екі жақты реттеуді болдырмау мақсатында қаржы нарығына ықпал ететін елдегі ақпараттық (кибер) қауіпсіздікті реттеу жөніндегі заңнамалық және нормативтік құқықтық актілерді өзгерту және толықтыру бойынша ұсыныстар енгізу; - қаржы нарығында киберқауіпсіздікті қамтамасыз ету саласындағы қатынастарды реттейтін нормативтік құқықтық актілер мен нормативтік-әдістемелік құжаттарды халықаралық стандарттарға сәйкес келтіру.
6.2. Қаржы нарығы ақпараттық қауіпсіздігінің	

салалық орталығын дамыту	
Мақсаттары	Міндеттері
- қаржы нарығының субъектілеріндегі ақпараттық қауіпсіздік жағдайлары мен оқиғалары туралы ақпаратты талдау жүйесін құру;	- қаржы нарығының субъектілерінен келіп түсетін ақпараттық қауіпсіздік оқиғалары бойынша ақпаратты өңдеу процесін автоматтандыру; - қаржы нарығының субъектілерінен келіп түсетін ақпараттық қауіпсіздік жағдайлары мен оқиғалары бойынша ақпарат ағындарын біріктіру.
- киберқатерлер ландшафты және олармен күрес құралдары туралы қаржы нарығы субъектілерінің хабардарлық деңгейін арттыру процесін ұйымдастыру;	- қаржы нарығында ақпараттық қауіпсіздік қатерлерінің мониторинг жүйесін құру; - қаржы нарығында анықталған ақпараттық қауіпсіздік қатерлері және оларға қарсы іс-қимыл құралдары туралы хабарландыру жүйесін құру;
- ақпараттық қауіпсіздік саласындағы мамандардың біліктілігін арттыру;	- қызметкерлердің ақпараттық қауіпсіздік саласында біліктілік деңгейін арттыру бойынша курстар мен тренингтерге қатысуы; - сертификаттаудан өтуі; - қаржы секторында кибероқудан өтуі;
- Қаржы нарығы ақпаратымен алмасу және талдау орталығын құру.	- қаржы нарығындағы киберқауіпсіздік оқиғалары туралы жалпы/бірыңғай деректер базасын жинау және құру үшін технологиялық платформа құру; - төлем жүйелерінің киберқауіпсіздігін қамтамасыз ету бөлігінде Ұлттық Банктің ақпараттық жүйелерімен ықпалдасу; - киберқауіпсіздік оқиғалары туралы ақпаратпен алмасу тетігін жасау; - Қаржы нарығының ақпаратымен алмасу және талдау орталығының шеңберінде қаржы нарығының қатысушыларымен өзара әрекет ету және ынтымақтасу мәселелерін

	талқылау бойынша тұрақты кездесулер форматын әзірлеу.
6.3. Төлем жүйелерінің, төлем қызметтері нарығының және цифрлық қаржылық қызметтердің киберқауіпсіздігі	
Мақсаттары	Міндеттері
Төлем жүйелері мен төлем нарығының киберқауіпсіздігін дамыту.	Қазақстан аумағында жұмыс істейтін төлем (оның ішінде халықаралық) жүйелерінің қауіпсіздігіне қойылатын ең төменгі талаптарды әзірлеу; қаржы және төлем нарығының барлық қатысушыларын қамти отырып, электрондық банктік қызметтерді ұсыну бойынша қолданыстағы нормативтік құқықтық базаны жаңарту; төлем ұйымдарын, төлем жүйелерінің операторларын киберқауіпсіздікті қамтамасыз ету жөніндегі салалық орталыққа қосу; цифрлық қаржылық экожүйелердің инфрақұрылымдарына ақпараттық қауіпсіздік талаптарын және стандарттарын әзірлеу.
6.4. Жаһандық ауқымда киберқылмыспен күрес саласындағы ынтымақтастық	
Мақсаттары	Міндеттері
Мемлекетаралық деңгейде киберқауіпсіздік мәселелері бойынша өзара іс-қимылды ұйымдастыру.	Қаржы нарығының ақпараттық қауіпсіздігін қамтамасыз ету және ЕАЭО туралы шартқа мүше мемлекеттердің орталық (ұлттық) банктерінің кредиттік-қаржылық саласындағы компьютерлік шабуылдарға қарсы іс-қимыл мәселелері бойынша Жұмыс тобының шеңберінде қаржы нарығын реттеу тәсілдерін үйлестіру; басқа елдердің қаржылық реттеушілерімен киберқауіпсіздік мәселелері бойынша екіжақты және көпжақты ынтымақтастықты регламенттеу;

	төтенше жағдайларға ден қоюшы топтарды біріктіретін халықаралық ұйымдарға (computer emergency response team, CERT) кіру.
6.5. Халықтың киберсауаттылық деңгейін арттыру	
Мақсаты	Міндеттері
Халықтың қаржылық қызметтерді қауіпсіз алу бөлігінде хабардарлығын арттыру барысын ұйымдастыру.	халықтың қаржылық сауаттылығын көтеру бойынша білім беру бағдарламаларына киберсауаттылықты арттыру жөніндегі іс-шараларды енгізу; Қаржылық қызметтерді алу кезіндегі киберқауіпсіздік саласында халықта туындайтын мәселелер мен проблемалар жөнінде бұқаралық ақпарат құралдарында жариялау.
6.6. Ұлттық Банкте және Агенттікте ақпараттық қауіпсіздікті басқару жүйесін жетілдіру	
Мақсаты	Міндеттері
Ұлттық Банкте және оның еншілес ұйымдарында ақпараттық қауіпсіздікті қамтамасыз етудің бірыңғай тәсілін қалыптастыру;	Ұлттық Банктің еншілес ұйымдары үшін ақпараттық қауіпсіздікті басқару жүйесіне бірыңғай талаптарды қалыптастыру; әзірленген талаптарды Ұлттық Банктің процестерімен ықпалдасуды және үйлестіруді қамтамасыз ету.
Ақпараттық қауіпсіздік саласындағы мамандардың кадрлық әлеуетін арттыру;	қызметкерлердің ақпараттық қауіпсіздік саласындағы біліктілік деңгейін арттыру бойынша курстар мен тренингтерден өтуі; ақпараттық қауіпсіздік бойынша құзыреттілік орталықтары болып табылатын ұйымдарда тағылымдамадан өтуі; Агенттікте туындаған кибероқиғаларға уақтылы әрекет ету үшін ден қою қызметін ұйымдастыру.
Ұлттық Банкте ақпараттық қауіпсіздікті басқару жүйесін енгізу;	ақпараттық қауіпсіздікті басқару процестерінің жетілу деңгейін бағалау; ақпараттық қауіпсіздік саласында жаңартылған ішкі нормативтік құжаттаманы қамтамасыз ету.

Ақпараттық қауіпсіздікті қамтамасыз ету процестеріне құрылымдық бөлімшелер басшыларының қатысуын арттыру.	ақпараттық қауіпсіздікті қамтамасыз етуді тұрақты негізде бақылауды қамтамасыз ететін алқалы органды ұйымдастыру.

7-тарау. Стратегияны іске асыру тәуекелдері

Стратегияны іске асырудың негізгі тәуекелдері:

1) ресурстардың жетіспеушілігі – Стратегияны іске асыруға қажетті ресурстарды дұрыс жоспарламау және жеткіліксіз бөлу (ақпараттық қауіпсіздік саласындағы мамандар, оның ішінде еңбекақы төлеу, жабдық, бағдарламалық қамтамасыз ету), сондай-ақ Агенттіктің және Ұлттық Банктің қажетті ресурстарының қолжетімділігіне ықпал ететін сыртқы факторлар;

2) ұйымдардың бірінші басшыларын әлсіз тарту – Стратегия алға қойған міндеттерді іске асырған кезде жоғары басшылықтан қажетті қолдаудың болмауы;

3) киберқауіпсіздікті реттеу мәселелерінде консенсустың болмауы – мемлекеттік және салалық деңгейде киберқауіпсіздікті қамтамасыз етудің қажетті шаралары мен құралдарын анықтауға тәсілдердің айырмасы;

4) киберқауіпсіздік саласында ұлттық деңгейдегі нормативтік құқықтық базаның болмауы – бар заманауи технологияларға және оларды пайдалана отырып жасалатын қылмыстарға бейімделмеген ескі нормативтік құқықтық база.

8-тарау. Стратегияны жаңарту мониторингі

Қажеттіліктің туындауына қарай, оның ішінде тікелей Агенттіктің және Ұлттық Банктің стратегиялық жоспарларына өзгерістер енгізілгеннен кейін Стратегия жаңартылады.

Стратегияны іске асыру мақсатында алдағы міндеттер көрсетілген іс-шаралар жоспары әзірленуде, қажеттілігіне қарай оларға өзгерістер және (немесе) толықтырулар енгізіледі.

Агенттіктің және Ұлттық Банктің киберқауіпсіздігіне жауап беретін бөлімшелер Стратегияны әзірлеуші – жауапты бөлімшелер болып табылады.

8.1. Стратегияны іске асыру үшін мүмкіндіктер мен қауіптердің күшті және әлсіз жақтарын талдау

Күшті тараптар	Әлсіз тараптар
– ақпараттық және киберқауіпсіздікті қамтамасыз етудің операциялық деңгейі белгіленді; – операциялық деңгейдегі кадр ресурстарының сапасы; – осы уақытқа дейін іске асырылған алдын алу шараларының жақсы нәтижелері бар.	– ресурстардың (қаржылық, кадрлық, материалдық және техникалық) болмауы; – мемлекеттік және қаржы нарығының негізгі мүдделі тараптары арасында ынтымақтастықтың жеткіліксіз болуы; – қаржы нарығының киберқауіпсіздікті қамтамасыз ету саласындағы нормативтік құқықтық базаның жеткіліксіз болуы.
Мүмкіндіктер	Қауіптер
– пайдаланушылардың (жеке тұлғалар, қаржы ұйымдары, банктік холдингтер және банктік конгломерат қатысушылары, «Қазақстанның Даму Банкі» АҚ, қызметін бағалы қағаздар нарығында жүзеге асыратын заңды тұлғалар, бағалы қағаздардың эмитенттері, кредиттік бюролар, сақтандыру қызметінің субъектілері, сақтандыру брокерлері, сақтандыру холдингтері, сақтандыру топтары, ақша аударымы бойынша қызметтер көрсететін пошта операторы («Қазпочта» АҚ), арнайы қаржы компаниялары, исламдық арнайы қаржы компаниялары, инвестициялық қорлар және басқа да тұлғалар) Интернетті пайдалануға асқан сенімі, оны пайдалануды ұлғайтады (B2C, B2B, B2G, G2C), пайдалану шығыстарын төмендетеді, сәйкесінше цифрлық өсуді және қаржылық тұрақтылықты жүзеге асыруға мүмкіндік береді; – қатысушылардың бар мүмкіндіктері мен синергизмді пайдалануды ынталандыру.	– жалпы төмен киберқауіпсіздік мәдениетіне, ұлттық деңгейде осы саладағы жүйелі реттеуге қатысты консенсустың болмауына тығыз байланысты киберқауіпсіздікті қамтамасыз етудің маңыздылығы туралы жеткілікті түрде хабардар болмау.

9-тарау. Қорытынды

Стратегияны іске асыру нәтижесінде қаржы нарығындағы киберқауіпке жедел ден қою тетігі қалыптасатын болады, ол қаржы секторының субъектілерімен де, сол сияқты мемлекеттік органдармен, оның ішінде құқық қорғау және арнайы органдармен қауіп деңгейіне байланысты өзара іс-қимылды болжайды.

Агенттік пен Ұлттық Банк Стратегияның мақсатқа қол жеткізу үшін айқындалған іс-шараларының орындалуын бақылауды заңмен белгіленген өкілеттік шегінде жүзеге асыратын болады.