Банктердің, Қазақстан Республикасының бейрезидент-банктері филиалдарының және банк операцияларының жекелеген түрлерін жүзеге асыратын ұйымдардың ақпараттық қауіпсіздігін қамтамасыз етуге қойылатын талаптарды, Ақпараттық жүйелердегі бұзушылықтар, іркілістер туралы мәліметтерді қоса алғанда, ақпараттық қауіпсіздіктің оқыс оқиғалары туралы ақпаратты беру қағидалары мен мерзімдерін бекіту туралы

Қазақстан Республикасы Ұлттық Банкі Басқармасының 2018 жылғы 27 наурыздағы № 48 қаулысы. Қазақстан Республикасының Әділет министрлігінде 2018 жылғы 18 сәуірде № 16772 болып тіркелді.

Ескерту. Тақырыбы жаңа редакцияда – ҚР Қаржы нарығын реттеу және дамыту агенттігі Басқармасының 17.02.2021 № 34 (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) қаулысымен.

"Қазақстан Республикасындағы банктер және банк қызметі туралы" 1995 жылғы 31 тамыздағы Қазақстан Республикасының Заңы 61-5-бабының 7-тармағына сәйкес Қазақстан Республикасы Ұлттық Банкінің Басқармасы **ҚАУЛЫ ЕТЕДІ:**

Ескерту. Кіріспе жаңа редакцияда – ҚР Ұлттық Банкі Басқармасының 19.11.2019 № 203 (01.01.2020 бастап қолданысқа енгізіледі) қаулысымен.

1. Мыналар:

1) осы қаулыға 1-қосымшаға сәйкес Банктердің, Қазақстан Республикасының бейрезидент-банктері филиалдарының және банк операцияларының жекелеген түрлерін жүзеге асыратын ұйымдардың ақпараттық қауіпсіздігін қамтамасыз етуге қойылатын талаптар;

2) осы қаулыға 2-қосымшаға сәйкес Ақпараттық жүйелердегі бұзушылықтар, іркілістер туралы мәліметтерді қоса алғанда, ақпараттық қауіпсіздіктің оқыс оқиғалары туралы ақпаратты беру қағидалары мен мерзімдері бекітілсін.

Ескерту. 1-тармаққа өзгеріс енгізілді – ҚР Қаржы нарығын реттеу және дамыту агенттігі Басқармасының 17.02.2021 № 34 (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) қаулысымен.

2. "Екінші деңгейдегі банктердің және банк операцияларының жекелеген түрлерін жүзеге асыратын ұйымдардың ақпарат жүйелерінің қауіпсіздігін қамтамасыз ету жөніндегі ережені бекіту туралы" Қазақстан Республикасының Ұлттық Банкі Басқармасының 2001 жылғы 31 наурыздағы № 80 қаулысының (Нормативтік құқықтық актілерді мемлекеттік тіркеу тізілімінде № 1517 болып тіркелген) күші жойылды деп танылсын.

3. Ақпараттық қауіп және киберқорғау басқармасы (Перминов Р.В.) Қазақстан Республикасының заңнамасында белгіленген тәртіппен:

1) Заң департаментімен (Сәрсенова Н.В.) бірлесіп осы қаулыны Қазақстан Республикасының Әділет министрлігінде мемлекеттік тіркеуді;

2) осы қаулы мемлекеттік тіркелген күннен бастап күнтізбелік он күн ішінде оның қазақ және орыс тілдеріндегі қағаз және электрондық түрдегі көшірмесін " Республикалық құқықтық ақпарат орталығы" шаруашылық жүргізу құқығындағы республикалық мемлекеттік кәсіпорнына Қазақстан Республикасы нормативтік құқықтық актілерінің эталондық бақылау банкінде ресми жариялау және енгізу үшін жіберуді;

3) осы қаулыны ресми жарияланғаннан кейін Қазақстан Республикасы Ұлттық Банкінің ресми интернет-ресурсына орналастыруды;

4) осы қаулы мемлекеттік тіркелгеннен кейін он жұмыс күні ішінде Заң департаментіне осы қаулының осы тармағының 2), 3) тармақшаларында және 4-тармағында көзделген іс-шаралардың орындалуы туралы мәліметтерді ұсынуды қамтамасыз етсін.

4. Қаржылық қызметтерді тұтынушылардың құқықтарын қорғау және сыртқы коммуникациялар басқармасы (Терентьев А.Л.) осы қаулы мемлекеттік тіркелгеннен кейін күнтізбелік он күн ішінде оның көшірмесін мерзімді баспасөз басылымдарында ресми жариялауға жіберуді қамтамасыз етсін.

5. Осы қаулының орындалуын бақылау Қазақстан Республикасының Ұлттық Банкі Төрағасының орынбасары О.А. Смоляковқа жүктелсін.

6. Осы қаулы, 2018 жылғы 1 желтоқсаннан бастап қолданысқа енгізілетін осы қаулының 1-тармағының 1) тармақшасын және 2-тармағын қоспағанда, алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі.

Ұлттық Банк
Төрағасы *Д. Ақышев*

Қазақстан Республикасының
Ұлттық Банкі Басқармасының
2018 жылғы 27 наурыздағы
№ 48 қаулысына
1-қосымша

Банктердің, Қазақстан Республикасының бейрезидент-банктері филиалдарының және банк операцияларының жекелеген түрлерін жүзеге асыратын ұйымдардың ақпараттық қауіпсіздігін қамтамасыз етуге қойылатын талаптар

Ескерту. Талаптар жаңа редакцияда - ҚР Қаржы нарығын реттеу және дамыту агенттігі Басқармасының 29.04.2022 № 30 (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) қаулысымен.

1-тарау. Жалпы ережелер

1. Осы Банктердің, Қазақстан Республикасының бейрезидент-банктері филиалдарының және банк операцияларының жекелеген түрлерін жүзеге асыратын ұйымдардың ақпараттық қауіпсіздігін қамтамасыз етуге қойылатын талаптар (бұдан әрі – Талаптар) "Қазақстан Республикасындағы банктер және банк қызметі туралы" Қазақстан Республикасының Заңы 61-5-бабының 7-тармағына сәйкес әзірленді және банктердің, Қазақстан Республикасының бейрезидент-банктері филиалдарының (бұдан әрі – банк) және банк операцияларының жекелеген түрлерін жүзеге асыратын ұйымдардың (бұдан әрі – ұйым) ақпараттық қауіпсіздігін қамтамасыз етуге қойылатын талаптарды белгілейді.

2. Талаптарда "Ақпараттандыру туралы" Қазақстан Республикасының Заңында көзделген ұғымдар, сондай-ақ мынадай ұғымдар пайдаланылады:

1) ақпараттандыру саласындағы ақпараттық қауіпсіздік (бұдан әрі – ақпараттық қауіпсіздік) – электрондық ақпараттық ресурстардың, ақпараттық жүйелердің және ақпараттық-коммуникациялық инфрақұрылымның сыртқы және ішкі қатерлерден қорғалуының жай-күйі;

2) ақпаратты штаттық тасымалдаушы – ақпараттық-коммуникациялық инфрақұрылым объектісінің құрамдас бөлігі болып табылатын және оған тұрақты қосылған ақпарат тасымалдаушы;

3) ақпараттық актив – ақпараттың және оны сақтауға және (немесе) өңдеуге пайдаланылатын ақпараттық-коммуникациялық инфрақұрылым объектісінің жиынтығы;

4) ақпараттық жүйенің/активтің АТ-менеджері – банктің, ұйымның ақпараттық жүйені/активті ақпараттық жүйенің/активтің бизнес-иесінің талаптарына сәйкес келетін күйде ұстап тұруға жауапты қызметкері немесе бөлімшесі (қызметкерлері немесе бөлімшелері);

5) ақпараттық жүйенің немесе шағын жүйесінің бизнес-иесі – банктің, ұйымның ақпараттық жүйе немесе шағын жүйе автоматтандыратын негізгі бизнес-процестің иесі болып табылатын бөлімшесі (қызметкері);

6) ақпараттық-коммуникациялық инфрақұрылым (бұдан әрі – ақпараттық инфрақұрылым) – электрондық ақпараттық ресурстарды қалыптастыру және оларға қолжетімділік беру мақсатында технологиялық ортаның жұмыс істеуін қамтамасыз етуге арналған ақпараттық-коммуникациялық инфрақұрылым объектілерінің жиынтығы;

7) ақпараттық-коммуникациялық инфрақұрылымды қорғау шегі – банктің, ұйымның ақпараттық-коммуникациялық инфрақұрылымын сыртқы ақпараттық желілерден оқшаулайтын және ақпараттық қауіпсіздік қауіпінен қорғауды іске асыратын бағдарламалық-аппараттық құралдардың жиынтығы;

8) ақпараттық қауіпсіздік қатері – ақпараттық қауіпсіздіктің оқыс оқиғаларының пайда болуының алғышарттарын туындататын жағдайлардың және факторлардың жиынтығы;

9) ақпараттық қауіпсіздік тәуекелі – банктің, ұйымның ақпараттық активтері конфиденциалдылығының бұзылуы, тұтастығының немесе қолжетімділігінің қасақана бұзылуы салдарынан залалдың ықтимал пайда болуы;

10) ақпараттық қауіпсіздікті қамтамасыз ету – банктің, ұйымның ақпараттық активтерінің конфиденциалдылық, тұтастық және қолжетімділік күйін ұстап тұруға бағытталған процесс

11) ақпараттық қауіпсіздіктің оқыс оқиғалары туралы ақпарат – ақпараттық-коммуникациялық инфрақұрылымның немесе оның жекелеген объектілерінің жұмысында жеке немесе сериялық туындайтын, олардың тиісінше жұмыс істеуіне қауіп келтіретін іркілістер туралы ақпарат және (немесе) электрондық ақпараттық ресурстарды заңсыз алуға, көшіруге, таратуға, модификациялауға, жою немесе бұғаттауға арналған талаптар;

12) ақпараттық қауіпсіздіктің оқыс оқиғасы – ақпараттық-коммуникациялық инфрақұрылымның немесе оның жекелеген объектілерінің жұмысында жеке немесе сериялық туындайтын, олардың тиісінше жұмыс істеуіне қауіп келтіретін іркілістер және (немесе) электрондық ақпараттық ресурстарды заңсыз алуға, көшіруге, таратуға, модификациялауға, жоюға немесе бұғаттауға арналған талаптар;

13) алдын ала орнатылған есептік жазбалар – ақпараттық жүйелерді өндірушілер орнатқан есептік жазбалар;

14) артықшылықты есептік жазба – ақпараттық жүйедегі жасалу, жойылу және есептік жазбаларға кіру құқықтарын өзгерту артықшылықтары бар есептік жазба;

15) әкімшілендіру және мониторинг консолі – ақпараттық жүйені қашықтан басқаруды жүзеге асыруға мүмкіндік беретін жұмыс станциясы;

16) бизнес-процесс – сыртқы немесе ішкі тұтынушы үшін белгілі өнімді немесе қызметті жасауға бағытталған өзара байланысты іс-шаралар немесе міндеттер жиынтығы;

17) бизнес-процестің иесі – банктің, ұйымның бизнес-процестің жұмыс істеу цикліне және банктің, ұйымның бизнес-процеске тартылған бөлімшелерінің қызметін үйлестіруге жауап беретін бөлімшесі (қызметкері);

18) виртуалды орта – аппараттық іске асырудан абстракцияланған және бұл ретте бір нақты ресурста орындалатын есептеуіш процестердің бір-бірінен қисынды оқшауланuын қамтамасыз ететін есептеу ресурстары немесе олардың қисынды бірігуі;

19) гипервизор – бірнеше операциялық жүйені бір серверде немесе компьютерде құруға және іске қосуға мүмкіндік беретін бағдарламалық немесе аппараттық-бағдарламалық қамтамасыз ету;

20) деректер беру хаттамасы – желіге қосылған екі және одан көп құрылғы арасында қосу мен айырбастауды жүзеге асыруға мүмкіндік беретін қағидалар мен іс-қимыл жиынтығы;

21) деректерді өңдеу орталығы – банктің, ұйымның ақпараттық жүйелерінің жұмысын қамтамасыз ететін серверлер орналастырылған, арнайы бөлінген үй-жай;

22) желіаралық экран – ақпараттық инфрақұрылымның берілген қағидаларға сәйкес ол арқылы өтетін желілік трафикке бақылау мен сүзгіден өткізуді жүзеге асыратын элементі;

23) жұмыс станциясы – банктің, ұйымның ақпараттық активін пайдаланушының стационарлық дербес компьютері;

24) кіру – банктің, ұйымның ақпараттық активтерін пайдалану мүмкіндігі;

25) қауіпсіздіктің топтық саясаттары – ақпараттық жүйелердің құралдары арқылы іске асырылған ақпараттық қауіпсіздік қағидаларының үлгі жиынтықтары;

26) қосымша – ақпараттық жүйе пайдаланушысының қолданбалы бағдарламалық қамтамасыз етуі;

27) резервтік көшірме – деректер зақымдалған немесе бұзылған жағдайда оларды түпнұсқада немесе жаңадан орналастырылған орнында қалпына келтіруге арналған ақпарат тасымалдағыштағы деректер көшірмесі;

28) сигнатуралар – бағдарламалық кодты сәйкестендіретін деректер жиынтығы;

29) техникалық қауіпсіздікті қамтамасыз ету – техникалық құралдарды (күзет және өрт сигнализациясы, кіруді бақылау және басқару, бейнебақылау, өрт сөндіру, деректерді өңдеу орталығында температуралық режим мен ылғалдылықты бақылау жүйелерін) пайдалана отырып банктің, ұйымның қауіпсіздігін қамтамасыз ету процесі;

30) технологиялық есептік жазба – ақпарат жүйесіндегі ақпараттық жүйелердің өзара іс-әрекет жасау кезінде аутентификаттауға арналған есептік жазба;

31) түзету шарасы – ақпараттық қауіпсіздікті қамтамасыз ету барысында болған проблеманы не оның бұзылу салдарын түзетуге бағытталған ұйымдастыру және техникалық іс-шараларының жиынтығы;

32) уәкілетті орган – қаржы нарығын және қаржы ұйымдарын реттеу, бақылау мен қадағалау жөніндегі уәкілетті орган.

3. Банктердің, ұйымдардың ақпараттық қауіпсіздігін қамтамасыз етуге мынадай талаптар қойылады:

1) ақпараттық қауіпсіздікті басқару жүйесін ұйымдастыруға қойылатын талаптар;

2) банктің, ұйымның ақпараттық активтерін санаттарға бөлуге қойылатын талаптар;

3) банктің, ұйымның ақпараттық активтеріне қол жеткізуді ұйымдастыруға қойылатын талаптар;

4) ақпараттық инфрақұрылымның қауіпсіздігін қамтамасыз етуге қойылатын талаптар;

5) ақпаратты криптографиялық қорғау құралдарына қойылатын талаптар;

6) үшінші тұлғалардың банктің, ұйымның ақпараттық активтеріне қол жеткізуі кезінде ақпараттық қауіпсіздікті қамтамасыз етуге қойылатын талаптар;

7) ақпараттық қауіпсіздік жай-күйін ішкі тексеруге қойылатын талаптар;

8) ақпараттық қауіпсіздікті басқару жүйесінің процестеріне қойылатын талаптар.

2-тарау. Ақпараттық қауіпсіздікті басқару жүйесін ұйымдастыруға қойылатын талаптар

4. Банктің, ұйымның бірінші басшысы ақпараттық қауіпсіздікті қамтамасыз ету процесін басқаруға арналған банкті, ұйымды басқарудың жалпы жүйесінің бір бөлігі болып табылатын ақпараттық қауіпсіздікті басқару жүйесін құруды, оның жұмыс істеуін және жақсаруын қамтамасыз етеді.

5. Ақпараттық қауіпсіздікті басқару жүйесі банктің, ұйымның бизнес-процестері үшін ықтимал залалдың ең аз деңгейін көздейтін банктің, ұйымның ақпараттық активтерін қорғауды қамтамасыз етеді.

6. Банк, ұйым ақпараттық қауіпсіздікті басқару жүйесінің тиісті деңгейін, оның дамуы мен жақсартылуын қамтамасыз етеді.

7. Банктің, ұйымның ақпараттық қауіпсіздігін басқару жүйесінің қатысушылары:

1) басқару органы;

2) атқарушы органы;

3) ақпараттық қауіпсіздікті қамтамасыз ету міндеттері бойынша шешімдер қабылдауға уәкілетті алқалы орган (бұдан әрі – алқалы орган);

4) ақпараттық қауіпсіздік бөлімшесі; 5) ақпараттық технологиялар бөлімшесі;

6) қауіпсіздік бөлімшесі;

7) қызметкерлермен жұмыс жүргізу бөлімшесі;

8) заң бөлімшесі;

9) комплаенс-бақылау бөлімшесі;

10) ішкі аудит бөлімшесі;

11) ақпараттық қауіпсіздік тәуекелдерін басқару бөлімшесі.

Бөлімшелердің осы тармақтың бірінші бөлігінің 4), 5), 6), 7), 8), 9), 10) және 11) тармақшаларында көрсетілген функцияларын ұйымда осы тармақтың бірінші бөлігінде көрсетілген бөлімшелер не ұйымның жауапты қызметкерлері жүзеге асырады.

8. Банк, ұйым ақпараттық қауіпсіздікті басқару жүйесін құру және оның жұмыс істеуі кезінде ақпараттық қауіпсіздік бөлімшесінің және ақпараттық технологиялар бөлімшесінің тәуелсіздігін оларды банктің, ұйымның атқарушы органының әртүрлі мүшелеріне немесе банктің, ұйымның атқарушы органының тікелей басшысына қарату арқылы қамтамасыз етеді.

9. Банктің, ұйымның басқару органы ақпараттық қауіпсіздік саясатын бекітеді, онда мыналар:

1) ақпараттық қауіпсіздікті басқару жүйесін құрудың мақсаттары, міндеттері және негізгі қағидаттары;

2) ақпараттық қауіпсіздікті басқару жүйесінің қолданылу аясы;

3) банктің, ұйымның ақпараттық активтерінде жасалатын, сақталатын және өңделетін ақпаратқа қолжетімділікті басқаруға қойылатын талаптар;

4) ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі қызметке және ақпараттық қауіпсіздік қатерлерін анықтау мен талдау, шабуылдарға қарсы іс-қимыл және оқыс оқиғаларды тексеру жөніндегі іс-шараларды мониторингтеуді жүзеге асыруға қойылатын талаптар;

5) ақпараттық қауіпсіздіктің оқыс оқиғалары туралы ақпаратты жинауды, шоғырландыруды және сақтауды жүзеге асыруға қойылатын талаптар;

6) ақпараттық қауіпсіздіктің оқыс оқиғалары туралы ақпаратқа талдау жүргізуге қойылатын талаптар;

7) банк, ұйым қызметкерлерінің өздеріне жүктелген функционалдық міндеттерді атқару кезінде ақпараттық қауіпсіздікті қамтамасыз етуге жауапкершілігі айқындалады.

10. Банктің, ұйымның басқару органы бюджетті қалыптастыру кезінде банктің, ұйымның ақпараттық қауіпсіздігін қамтамасыз ету үшін ресурстарға қажеттілікті ескереді.

11. Банктің, ұйымның басқару органы қорғалатын ақпараттың тізбесін, оның ішінде қызметтік, коммерциялық немесе өзге де заңмен қорғалатын құпия болып табылатын мәліметтер туралы ақпаратты (бұдан әрі – қорғалатын ақпарат) қамтитын тізбені және қорғалатын ақпаратпен жұмыс тәртібін бекітеді.

12. Банктің, ұйымның атқарушы органы ақпараттық қауіпсіздікті басқару процесін регламенттейтін ішкі құжаттарды, қарау банктің, ұйымның ішкі құжаттарында айқындалатын тәртібі мен кезеңділігін бекітеді.

13. Банк, ұйым алқалы органды құрады, оның құрамына ақпараттық қауіпсіздік бөлімшесінің, ақпараттық қауіпсіздіктің тәуекелдерін басқару бөлімшесінің, ақпараттық технологиялар бөлімшесінің өкілдері, сондай-ақ банктің, ұйымның алқалы органы басшысының шешімі бойынша банктің, ұйымның басқа бөлімшелерінің өкілдері кіреді немесе атқарушы орган осы тармақта көрсетілген алқалы органның құрамына қойылатын талаптарға сәйкес келген кезде атқарушы органға алқалы органның функцияларын жүктейді.

Банкте, ұйымда алқалы орган құрылған жағдайда банктің, ұйымның алқалы органының басшысы болып банктің, ұйымның атқарушы органының басшысы немесе ақпараттық қауіпсіздік бөлімшесінің қызметіне жетекшілік ететін банктің, ұйымның атқарушы органының мүшесі тағайындалады.

14. Ақпараттық қауіпсіздік бөлімшесі банк, ұйым ақпаратының конфиденциалдылығын, тұтастығын және қолжетімділігін қамтамасыз ету мақсатында мынадай функцияларды жүзеге асырады:

1) ақпараттық қауіпсіздікті басқару жүйесін құрады, банк, ұйым бөлімшелерінің ақпараттық қауіпсіздікті және қауіптерді анықтау және талдау, шабуылдарға қарсы

іс-қимыл жасау және ақпараттық қауіпсіздіктің оқыс оқиғаларын тергеу жөніндегі іс-шараларды қамтамасыз ету бойынша қызметін үйлестіруді және бақылауды жүзеге асырады;

2) банктің, ұйымның ақпараттық қауіпсіздік саясатын әзірлейді;

3) банктің, ұйымның ақпараттық қауіпсіздікті қамтамасыз ету процесін әдіснамалық қолдауды қамтамасыз етеді;

4) өз өкілеттіктері шеңберінде банктің, ұйымның ақпараттық қауіпсіздігін басқару, қамтамасыз ету және бақылау әдістерін, құралдары мен тетіктерін таңдауды, енгізуді және қолдануды жүзеге асырады;

5) ақпараттық қауіпсіздіктің оқыс оқиғалары туралы ақпаратты жинауды, шоғырландыруды, сақтауды және өңдеуді жүзеге асырады;

6) ақпараттық қауіпсіздіктің оқыс оқиғалары туралы ақпаратты талдауды жүзеге асырады;

7) алқалы органның ақпараттық қауіпсіздік жөніндегі мәселелер бойынша шешім қабылдауы үшін ұсыныстар дайындайды;

8) банктің, ұйымның ақпараттық қауіпсіздігін қамтамасыз ету процесін автоматтандыратын бағдарламалық-техникалық құралдарын енгізуді және олардың тиісінше жұмыс істеуін, сондай-ақ оларға кіруді қамтамасыз етеді;

9) артықшылық берілген есептік жазбаларды пайдалану бойынша ақпараттық қауіпсіздікті талаптарын айқындайды;

10) банк, ұйым қызметкерлерінің ақпараттық қауіпсіздік мәселелері жөнінде хабардар болуын қамтамасыз ету бойынша іс-шараларды ұйымдастырады және жүргізеді;

11) банктің, ұйымның ақпараттық қауіпсіздікті басқару жүйесінің жай-күйін мониторингтеуді жүзеге асырады;

12) банктің, ұйымның ақпараттық қауіпсіздікті басқару жүйесінің жай-күйі туралы банктің, ұйымның басшылығын хабардар етуді жүзеге асырады.

15. Банк, ұйым ақпараттық қауіпсіздік бөлімшесіне техникалық қауіпсіздікті қамтамасыз ету бойынша функцияларды жүктеу мүмкіндігін айқындайды. Ақпараттық қауіпсіздік бөлімшесі олардың негізгі функцияларымен мүдделер қайшылықтарына апаратын функцияларды жүзеге асырмайды.

16. Ақпараттық технологиялар бөлімшесі мынадай функцияларды жүзеге асырады:

1) банктің, ұйымның ақпараттық инфрақұрылымы схемасының өзектілігін әзірлейді және қолдау жасайды;

2) кіруге ақпараттық технологиялар жөніндегі бөлімшеге жатпайтын ақпараттық жүйелердің АТ-менеджерлері рұқсат беретін мамандандырылған ақпараттық активтерді қоспағанда, банктің, ұйымның ақпараттық активтеріне банктің, ұйымның ақпараттық активтерін пайдаланатын банктің, ұйымның қызметкері (бұдан әрі-пайдаланушы) қол жеткізуді қамтамасыз етеді;

3) ақпараттық қауіпсіздік талаптарын ескере отырып, банктің, ұйымның жүйелік және қолданбалы бағдарламалық қамтылымының үлгі баптауларын қалыптастыруды және конфигурациялауды қамтамасыз етеді;

4) банктің, ұйымның ішкі құжаттарына сәйкес ақпараттық инфрақұрылымның үзіліссіз жұмыс істеуі, банктің ақпараттық жүйелері деректерінің конфиденциалдылығы, тұтастығы және қолжетімділігі (ақпаратты резервтеуді және (немесе) архивтеуді және резервтік көшіруді қоса алғанда) бойынша белгіленген талаптардың орындалуын қамтамасыз етеді;

5) ақпараттық жүйелерді таңдау, ендіру, әзірлеу және тестілеуден өткізу кезінде ақпараттық қауіпсіздік талаптарының сақталуын қамтамасыз етеді.

17. Банк, ұйым Талаптардың 14 және 16-тармақтарында көрсетілген жекелеген функцияларды банктің бөлімшелеріне беру, ұйымдастыру мүмкіндігін айқындайды.

18. Қауіпсіздік бөлімшесі мынадай функцияларды жүзеге асырады:

1) банкте, ұйымда физикалық және техникалық қауіпсіздік шараларын іске асырады , оның ішінде өткізу және объектішілік режимді ұйымдастырады;

2) банк, ұйым қызметкерлерін жұмысқа қабылдау және жұмыстан босату кезінде ақпараттық қауіпсіздік қатерлерінің туындау тәуекелдерін барынша азайтуға бағытталған профилактикалық іс-шараларды жүргізеді.

19. Қызметкерлермен жұмыс жүргізу бөлімшесі мынадай функцияларды жүзеге асырады:

1) банк, ұйым қызметкерлерінің, сондай-ақ қызмет көрсету туралы шарт бойынша жұмысқа тартылған адамдардың, стажерлардың, практиканттардың конфиденциалды ақпаратты жария етпеу туралы міндеттемелерге қол қоюын қамтамасыз етеді;

2) банк, ұйым қызметкерлерінің ақпараттық қауіпсіздік саласында хабардар болуын арттыру процесін ұйымдастыруға қатысады;

3) уәкілетті органды ақпараттық қауіпсіздік бөлімшесінің қызметкерлерін тағайындау және жұмыстан босату туралы хабардар етеді.

20. Заң бөлімшесі банктің, ұйымның ақпараттық қауіпсіздікті қамтамасыз ету мәселелері бойынша ішкі құжаттарының құқықтық сараптамасын жүргізеді.

21. Комплаенс-бақылау бөлімшесі банктің, ұйымның заң бөлімшесімен бірлесе отырып Талаптардың 11-тармағында көзделген қорғалатын ақпараттың тізбесіне енгізуге жататын ақпараттың барлық түрін айқындайды.

22. Ішкі аудит бөлімшесі банктің, ұйымның ішкі аудит жүйесін ұйымдастыруды реттейтін банктің, ұйымның ішкі құжаттарына сәйкес банктің, ұйымның ақпараттық қауіпсіздікті басқару жүйесінің жай-күйін бағалауды жүргізеді.

23. Банктің ақпараттық қауіпсіздік тәуекелдерін басқару бөлімшесі Нормативтік құқықтық актілерді мемлекеттік тіркеу тізілімінде № 19632 болып тіркелген, Қазақстан Республикасы Ұлттық Банкі Басқармасының 2019 жылғы 12 қарашадағы № 188 қаулысымен бекітілген Екінші деңгейдегі банктерге, Қазақстан Республикасының

бейрезидент-банктері филиалдарына арналған тәуекелдерді басқару және ішкі бақылау жүйесін қалыптастыру қағидаларында көзделген функцияларды жүзеге асырады.

Ұйымның ақпараттық қауіпсіздік тәуекелдерін басқару бөлімшесі ұйымның ішкі құжаттарына сәйкес функцияларды жүзеге асырады.

24. Банктің, ұйымның құрылымдық бөлімшелерінің басшылары:

1) қызметкерлердің банктің, ұйымның ақпараттық қауіпсіздікке қойылатын талаптарды (бұдан әрі - ақпараттық қауіпсіздікке қойылатын талаптары) қамтитын ішкі құжаттарымен танысуын қамтамасыз етеді;

2) олар басқаратын бөлімшелерде ақпараттық қауіпсіздікті қамтамасыз ету үшін дербес жауапкершілік атқарады;

3) конфиденциалды ақпаратты жария етпеу туралы келісімдер жасасуды және банктің, ұйымның бөлімшесі мұндай келісімдерді, шарттарды жасасуға бастамашы болған жағдайларда, ақпараттық қауіпсіздікті қамтамасыз ету туралы талаптарды келісімдерге, қызметтер көрсету/жұмыстарды орындау шарттарына енгізуді қамтамасыз етеді.

25. Ақпараттық жүйелердің немесе шағын жүйелердің бизнес-иелері:

1) ақпараттық жүйелерді құру, енгізу, түрлендіру, пайдалану және банктің, ұйымның клиенттері мен бөлімшелеріне өнімдер мен қызметтерді ұсыну кезінде, сондай-ақ мемлекеттік органдардың ақпараттық жүйелерін қоса алғанда, ақпараттық жүйелерді сыртқы ақпараттық жүйелермен біріктіру кезінде ақпараттық қауіпсіздікке қойылатын талаптардың сақталуына жауап береді;

2) ақпараттық жүйелерге кіру матрицаларының жаңартылуын қалыптастырады және қолдайды.

26. Банктің, ұйымның құрылымдық бөлімшелерінің қызметкерлері:

1) банкте, ұйымда қабылданған ақпараттық қауіпсіздік талаптарының орындалуы үшін жауап береді;

2) өздерінің функционалдық міндеттері шеңберінде олар өзара іс-әрекет жасайтын үшінші тұлғалардың ақпараттық қауіпсіздік талаптарын орындауын, оның ішінде аталған талаптарды үшінші тұлғалармен жасалған шарттарға енгізу арқылы бақылайды ;

3) өзінің тікелей басшысына және ақпараттық қауіпсіздік бөлімшесіне банктің, ұйымның ақпараттық активтерімен жұмыс істеу кезіндегі барлық күдікті жағдайлар мен бұзушылықтар туралы хабарлайды.

27. Егер банктің, ұйымның ақпараттық қауіпсіздігін қамтамасыз ету функциялары тысқары ұйымдарға берілсе, атқарушы органының ақпараттық қауіпсіздік мәселелеріне жетекшілік ететін мүшесі ақпараттық қауіпсіздікті қамтамасыз етуге жауапты болып табылады.

28. Банк, ұйым жыл сайын есепті жылдан кейінгі жылдың 10 қаңтарынан кешіктірмей уәкілетті органға ақпараттық қауіпсіздікті басқару жүйесінің жай-күйі

және оның Талаптарға сәйкестігі туралы ақпарат (бұдан әрі – АҚБЖ туралы ақпарат) береді.

29. АҚБЖ туралы ақпарат еркін нысанда жасалады және ұсынылатын деректердің құпиялылығы мен түзетілмеуін қамтамасыз ететін криптографиялық қорғау құралдарымен ақпаратты кепілді жеткізудің тасымалдау жүйесін пайдалана отырып, уәкілетті органға ұсынылады.

30. АҚБЖ туралы ақпаратта мыналар:

1) банктің, ұйымның ақпараттық қауіпсіздікті басқару жүйесінің қолданылу аясы және олардың функционалының Талаптарға сәйкестігін көрсете отырып, оның қатысушылары;

2) ақпараттық қауіпсіздікті басқару жүйесін құруды және оның жұмыс істеуін реттейтін құжаттардың болуы;

3) ақпараттық қауіпсіздікті қамтамасыз ету үшін пайдаланылатын бағдарламалық-техникалық құралдарының болуы және сандық құрамы;

4) операторлармен жасалған қызметтер көрсету туралы шарттарда ақпараттық қауіпсіздікті қамтамасыз ету бойынша талаптардың және міндеттемелердің болуы;

5) деректер өңдеудің резервтік орталықтарының болуы, материалдық-техникалық жабдықталуы және дайындығы;

6) банктің, ұйымның ақпараттық қауіпсіздікті басқару жүйесін және ақпараттық активтерін Талаптарға сәйкестендіру бойынша жүргізілген іс-шаралар туралы мәліметтер қамтылады.

31. Уәкілетті орган банктің, ұйымның Талаптарға сәйкестігін бағалауды 3 (үш) жылда кемінде бір рет жүзеге асырады.

3-тарау. Ақпараттық активтерді санатқа жатқызуға қойылатын талаптар

32. Банк, ұйым ақпараттық активтерді санатқа жатқызуды олардың конфиденциалдығын, тұтастығын, қолжетімділігін бұзудан болған зияндар деңгейі негізінде оларды маңызды және маңызды емеске бөлу арқылы жүзеге асырады.

33. Банк, ұйым олардың иелерін көрсете отырып, маңызды ақпараттық активтердің тізбесін қалыптастырады.

34. Банк, ұйым Талаптарға сәйкес маңызды санатына жатқызылған ақпараттық активтердің, сондай-ақ осы активтер кіретін ақпараттық жүйелердің ақпараттық қауіпсіздігін қамтамасыз етеді.

35. Маңызды емес санатына жатқызылған ақпараттық активтерді, сондай-ақ тұтастай осы активтерден тұратын ақпараттық жүйелерді қорғау әдістері мен құралдарын банк, ұйым дербес айқындайды.

4-тарау. Ақпараттық активтерге кіруді ұйымдастыруға қойылатын талаптар

36. Банктің, ұйымның қызметкерлеріне ақпаратқа кіру олардың функционалдық міндеттерін айқындайтын көлемде беріледі.

37. Банктің, ұйымның ақпараттық жүйелеріне кіруіне рұқсат беру ақпараттық жүйелерді пайдаланушылардың кіру құқықтарының олардың функционалдық міндеттеріне сәйкестігін қамтамасыз ету үшін рөлдерді қалыптастыру және енгізу жолымен жүргізіледі. Мұндай рөлдердің жиынтығы банк, ұйым электрондық нысанда немесе қағаз тасымалдағышта қалыптастыратын ақпараттық жүйеге кіру матрицасы болып табылады.

38. Банктің, ұйымның ақпараттық жүйелеріне кіру матрицаларын құру және пайдалану процесі Талаптардың 9-тарауына сәйкес банктің, ұйымның ішкі құжатында айқындалады.

39. Банктің, ұйымның ақпараттық жүйелеріне кіру ақпараттық жүйелерді пайдаланушыларды сәйкестендіру және бірегейлендіру арқылы жүзеге асырылады.

Банктің, ұйымның ақпараттық жүйелерін пайдаланушыларды сәйкестендіру және бірегейлендіру мынадай тәсілдердің бірі арқылы:

1) "есептік жазба (сәйкестендіруші) – пароль" деген жұпты енгізу немесе екі факторлық бірегейлендіру тәсілдерін қолдану арқылы (үш фактордың ішінен екеуін қолданумен: білім, иелік ету, ажырамастық);

2) биометриялық және (немесе) криптографиялық және (немесе) аппараттық бірегейлендіру тәсілдерін пайдалану арқылы жүргізіледі.

40. Банктің, ұйымның ақпараттық жүйелерінде пайдаланушылардың дербестендірілген есептік жазбалары ғана пайдаланылады.

41. Технологиялық есептік жазбалар ақпараттық қауіпсіздік бөлімшесі басшысының келісімі бойынша ақпараттық технологиялар бөлімшесінің басшысы бекітетін, оларды пайдалануға және өзектілігі үшін дербес жауапты адамдарды көрсете отырып, әрбір ақпараттық жүйе үшін осындай есептік жазбалардың тізбесіне сәйкес пайдаланылады.

42. Банктің, ұйымның ақпараттық жүйелерінде Талаптардың 9-тарауына сәйкес банк, ұйым айқындайтын есептік жазбаларды және парольдерді басқару, сондай-ақ пайдаланушылардың есептік жазбаларын оқшаулау бойынша функциялар пайдаланылады.

5-тарау. Ақпараттық инфрақұрылымның қауіпсіздігін қамтамасыз етуге қойылатын талаптар

43. Банктің, ұйымның ақпараттық технологиялар бөлімшесі мыналарды:

1) элементтерінің нақты орналасқан жерін көрсете отырып, ақпараттық инфрақұрылымның жалпы схемасын қалыптастыру және бекіту процесін;

2) ақпараттық активті немесе ақпараттық активтер тобын конфигурациялау құқығы берілген банктің, ұйымның жауапты қызметкерлерін (бұдан әрі – әкімшілер) тағайындау процесін;

3) мынадай:

операциялық жүйелердің;

дерекқорын басқару жүйелерін;

телекоммуникациялық құрылғыларды;

ақпараттық жүйелерді;

ақпараттық инфрақұрылымның тораптары мен соңғы нүктелерін, жұмыс станцияларын, оның ішінде қорғау периметрінің шегінен тыс тасымалдау және пайдалану үшін ыңғайлы нысанда жасалған дербес компьютерлерді (бұдан әрі – ноутбук) және операциялық жүйенің мобильді нұсқасы негізінде жұмыс істейтін жеке пайдаланылатын электрондық құрылғыларды (бұдан әрі-мобильді құрылғы) құжаттамалау және типтік теңшеулерін бекіту процесін әзірлейді және оларды іске асыруды қамтамасыз етеді.

44. Ақпараттық қауіпсіздік бөлімшесі банктің, ұйымның ақпараттық активтеріндегі жүйелік және конфигурациялық файлдардың, сондай-ақ аудиторлық із журналдарының қауіпсіздік теңшеулерінің және тұтастығының өзгеруін бақылау жүйесін ұйымдастыруды қамтамасыз етеді.

45. Банк, ұйым авторизацияланбаған құрылғылардың не теңшеулері банктің, ұйымның ішкі құжатында белгіленген ақпараттық қауіпсіздікті қамтамасыз ету тәртібіне қайшы келетін құрылғылардың ақпараттық инфрақұрылымына кіру тәуекелін төмендететін ұйымдастыру іс-шараларын жүргізеді және (немесе) бағдарламалық-техникалық құралдарды орнатады.

46. Банктің, ұйымның әрбір ақпараттық активі үшін ақпараттық жүйенің немесе шағын жүйенің кем дегенде бизнес-иесі, сондай-ақ АТ-менеджері және (немесе) әкімшісі анықталады.

47. Ақпараттық инфрақұрылым объектілерін құруға (жаңғыртуға) техникалық тапсырмаларды әзірлеу кезінде ақпараттық жүйенің немесе шағын жүйенің бизнес-иесі ақпараттық қауіпсіздік талаптарын ескереді.

48. Банк, ұйым ақпараттық жүйенің жұмыс істеуге қабілетті көшірмесін қалпына келтіруді қамтамасыз ететін ақпараттық жүйелер деректерінің, олардың файлдарының және теңшеулерінің резервтік сақталуын қамтамасыз етеді.

Ақпаратты резервтік көшіру, сақтау, қалпына келтіру тәртібі мен кезеңділігін, резервтік көшірмелерден маңызды ақпараттық жүйелердің жұмыс істеу қабілетін қалпына келтіруді тестілеуден өткізу кезеңділігін банк, ұйым айқындайды.

49. Банк, ұйым ақпараттық инфрақұрылымды вирусқа қарсы қорғауды Талаптардың 9-тарауына сәйкес банк, ұйым айқындаған тәртіппен қамтамасыз етеді.

50. Банктің, ұйымның деректерді өңдеу орталықтарының нақты қауіпсіздігін қамтамасыз ету тәртібін Талаптардың 9-тарауына сәйкес банк, ұйым айқындайды.

51. Банк, ұйым қызметкерлерінің жұмыс станцияларына, ноутбуктеріне және корпоративтік мобильді құрылғыларына олардың функционалды міндеттеріне сәйкес бағдарламалық қамтамасыз ету орнатылады.

52. Ақпараттық технологиялар бөлімшесі банкте, ұйымда пайдалануға рұқсат етілетін бағдарламалық қамтамасыз етудің тізбесін қалыптастырады және өзектендіреді . Бағдарламалық қамтамасыз ету ақпараттық қауіпсіздік бөлімшесі тексеру жүргізгеннен кейін тізбеге енгізіледі.

53. Банк, ұйым Талаптардың 9-тарауына сәйкес банктің, ұйымның жұмыс станцияларын, ноутбуктар мен мобильді құрылғыларын, сондай-ақ ақпарат тасымалдағыштарының және желілік ресурстарын қорғауды қамтамасыз ететін ұйымдық және техникалық шараларды айқындайды.

6-тарау. Ақпаратты криптографиялық қорғау құралдарына қойылатын талаптар

54. Ақпараттық жүйенің бизнес-иесі ақпаратты криптографиялық қолдау құралдарын енгізу және қолдау процесін ақпараттық қауіпсіздік бөлімшесімен келіседі.

55. Банк, ұйым Талаптардың 9-тарауына сәйкес ақпаратты криптографиялық қорғау құралдарын пайдалану тәртібін айқындайды. Банк, ұйым олардың мақсатын, оларда іске асырылатын криптографиялық алгоритмдерді, ақпараттық жүйенің атауын, ақпаратты криптографиялық қорғау құралдарын пайдаланатын ақпараттық жүйенің иесін көрсете отырып, қолданылатын ақпаратты криптографиялық қорғау құралдарының тізбесін бекітеді.

7-тарау. Үшінші тұлғалардың банктің, ұйымның ақпараттық активтеріне кіруі кезінде ақпараттық қауіпсіздікті қамтамасыз етуге қойылатын талаптар

56. Банк, ұйым банктің, ұйымның қызметкерлері немесе клиенттері болып табылмайтын үшінші тұлғалардың (бұдан әрі – үшінші тұлғалар) банктің, ұйымның ақпараттық активтеріне кіру кезінде ақпараттық қауіпсіздікті қамтамасыз етеді.

57. Үшінші тұлғалардың банктің, ұйымның ақпараттық активтеріне кіру рұқсаты Қазақстан Республикасының заңнамасында көзделген жағдайларды қоспағанда, ақпараттық қауіпсіздік талаптарын сақтау туралы талаптарды қамтитын келісім, шарт негізінде жүргізілетін жұмыстарда айқындалатын кезеңге және көлемде беріледі. Үшінші тұлғалармен жасалатын ақпараттық қауіпсіздік талаптарын сақтау туралы келісімдерде, шарттарда конфиденциалдылық туралы ережелер, ақпараттық қауіпсіздіктің бұзылуы салдарынан туындаған шығынды қайтару туралы, сондай-ақ үшінші тұлғалардың араласуы салдарынан болған ақпараттық жүйелердің жұмысындағы іркілістер және үшінші тұлғалардың әрекетінен немесе әрекетсіздігінен болған олардың қауіпсіздігін бұзуы салдарынан туындаған зиянды өтеу туралы талаптар қамтылады.

58. Банктің, ұйымның қызметіне тексеруді жүзеге асырған не тиісті кіру рұқсаты немесе ақпарат ұсынғанға дейін уәкілетті орган ақпарат сұратқан кезде уәкілетті орган өкілдерінің өкілеттіктері тексеріледі.

59. Үшінші тұлғалардың қызметін бақылауды қамтамасыз ету мақсатында мынадай ұйымдастыру және (немесе) бағдарламалық-техникалық шаралар көзделеді:

1) үшінші тұлғалар қызметінің нәтижесін тексеру;

2) үшінші тұлғалардың қызметін банк, ұйым қызметкерлерінің қатысуымен ғана жүзеге асыру;

3) үшінші тұлғалардың іс-қимылдары бойынша аудиторлық ізді жүргізу;

4) банктің, ұйымның ақпараттық активтеріне кіру сессиясын жазу.

60. Үшінші тұлғаларға банктің, ұйымның ақпараттық активтерінің бір бөлігін беру (серверлік қуаттарды тысқары деректерді өңдеу орталықтарына орналастыру, деректерді өңдеу және/немесе сақтаудың сыртқы сервистерін пайдалану) жағдайында ақпараттық қауіпсіздікті қамтамасыз етудің мынадай шаралары қабылданады:

1) үшінші тұлғамен жасалған тиісті келісімде, шартта банктің, ұйымның ақпараттық активтерін қорғау жөніндегі талаптарды және банктің, ұйымның осындай талаптардың орындалуын тексеру құқығын, сондай-ақ қауіпсіздікті және ақпараттық жүйелердің жұмыс істеу қабілетінің бұзылуы салдарынан туындаған шығынды қайтару туралы талаптарды көрсету;

2) Қазақстан Республикасының азаматтық, банк заңнамасына, Қазақстан Республикасының дербес деректер және оларды қорғау туралы заңнамасына сәйкес үшінші тұлғаларға беруге жол берілмейтін ақпаратқа үшінші тұлғалардың қол жеткізу мүмкіндігін болдырмау. Бұлттық сервистерді пайдалану кезінде осы мақсаттар үшін банк, ұйым тарапынан ақпаратты жариялаумен, ақпаратты шифрланған түрде сақтау әдісі қолданылады. Бұл ретте шифрлау кілті банкте, ұйымда сақталады.

8-тарау. Ақпараттық қауіпсіздіктің жай-күйіне ішкі тексерулер жүргізуге қойылатын талаптар

61. Ақпараттық қауіпсіздіктің жай-күйі мынадай тексеру жүргізу арқылы бағаланады:

1) ақпараттық қауіпсіздік бөлімшесі – атқарушы органның ақпараттық қауіпсіздік бөлімшесіне жетекшілік ететін мүшесі бекітетін жоспарға сәйкес, сондай-ақ банктің, ұйымның басқару органы басшысының жеке өкімі бойынша;

2) ішкі аудит бөлімшесі – банктің, ұйымның ішкі аудит жүйесін ұйымдастыруды реттейтін банктің, ұйымның ішкі құжаттарына сәйкес аудиторлық тексерулердің жылдық жоспары шеңберінде.

62. Ақпараттық қауіпсіздік бөлімшесі тексерудің нәтижесі бойынша тексеру материалдарын тіркей отырып, есеп жасайды, оны банктің, ұйымның тексерілетін бөлімшесіне мәлімет үшін жібереді.

9-тарау Ақпараттық қауіпсіздікті басқару жүйесінің процестеріне қойылатын талаптар

1-параграф. Ақпараттық жүйелерге кіруді ұйымдастыру процесіне қойылатын талаптар

63. Ақпараттық жүйеге кіру матрицасын құру процесін банк, ұйым белгіленген тәртіппен жүзеге асырады және мынадай кезеңдерден тұрады:

1) ақпараттық жүйенің бизнес-иесі банктің, ұйымның ақпараттық жүйесіне кіру матрицасын құруға және белсенділігін қамтамасыз етеді;

2) бизнес-процестің иесі ақпараттық жүйенің АТ-менеджерімен бірлесе отырып, қызметкерлердің функционалдық міндеттерінде айқындалатын көлемде ақпараттық жүйеде рөлдердің қалыптасуын және өзектілігін қамтамасыз етеді;

3) қалыптастырылған рөлдер ақпараттық жүйенің бизнес-иесімен келісіледі;

4) банк, ұйым қолданыстағы автоматтандырылған бақылауларды айналып өтуге мүмкіндік беретін кірудің қайшылықты құқықтарын рөлдерде алып тастауды қамтамасыз етеді;

5) ақпараттық жүйенің АТ-менеджері ақпараттық жүйеде рөлдерді іске асырады;

6) ақпараттық жүйенің немесе шағын жүйенің бизнес-иесі және бизнес-процестің иесі құрылған рөлдерді тестілеуден өткізеді;

7) ақпараттық жүйенің АТ-менеджері ақпараттық жүйеге рөлдерді енгізеді.

64. Ақпараттық жүйеге кіру матрицасына өзгерістер мен толықтыруларды енгізу Талаптардың 63-тармағында белгіленген тәртіппен жүзеге асырылады.

65. Банктің, ұйымның ақпараттық жүйесіне кіруді басқарудың тетігі мыналарды:

1) жаңа пайдаланушыны қосымша деңгейінде тіркеу мүмкіндігін;

2) пайдаланушыларға ақпараттық жүйелерге рольдер арқылы ғана кіру құқықтарын тағайындауды;

3) пайдаланушыларға ақпараттық жүйенің немесе шағын жүйенің бизнес-иесімен келісе отырып және ақпараттық қауіпсіздік бөлімшесіне хабарлай отырып, ақпараттық жүйеде бар рөлге қосымша жекелеген құқықтар беруді;

4) пайдаланушылардың рольдеріне ілеспе қызмет көрсетуді (құру, өзгерту, жою);

5) транзакциялық жүйелер үшін бірдей есептік деректер арқылы әртүрлі аппараттық құралдардан (компьютерлерден) бірмезгілде кіруді оқшаулау мүмкіндігін;

6) аудиторлық із жүргізуді қамтамасыз етеді.

66. Банктің, ұйымның ақпараттық жүйесінің деректеріне кіруді басқару тетігі мыналарды қамтиды:

1) пайдаланушыларға ақпараттық жүйенің деректеріне қосымша арқылы ғана кіруді қамтамасыз ету;

2) ақпараттық жүйенің деректеріне қосымшаны айналып өтіп, кіруді ұсыну ақпараттық қауіпсіздік бөлімшесімен келісу бойынша жүзеге асырылады;

3) ақпараттық технологиялар бөлімшесінің қосымшаны айналып өтіп, деректерге тікелей кіруге рұқсат берілген пайдаланушылар тізбесін қалыптастыруы және өзектендіруі.

67. Қызметкердің функционалдық міндеттері өзгерген кезде қолда бар кіру құқықтары ажыратылады және оның жаңа функционалдық міндеттеріне сәйкес жаңа кіру құқықтары тағайындалады. Қызметкер жұмыстан босатылған кезде жұмыстан босатылған күннен бастап бір тәуліктен асырмай оның барлық есептік жазбалары ажыратылады.

68. Ақпараттық қауіпсіздік бөлімшесі кіру матрицаларына сәйкес ақпараттық жүйелерге кіру құқықтарының дұрыстығына тексеру, сондай-ақ жұмыстан босатылған қызметкерлердің кіру құқықтарының ажыратылуына бақылау жүргізеді.

69. Ақпараттық жүйелердің және шағын жүйелердің бизнес-иелері ақпараттық жүйелерге кіру рөлдері мен құқықтарын қайта қарауды банктің, ұйымның мүдделі бөлімшелерін тарта отырып, жылына кемінде бір рет жүргізеді.

70. Банкте, ұйымдарда осы параграфтың бір немесе бірнеше талабын іске асыруға техникалық мүмкіндіктер болмаған кезде, ақпараттық қауіпсіздік тәуекелдерінің әсерін ішінара немесе толық болдырмау бойынша қосымша техникалық және ұйымдастыру шаралары түріндегі өтеу шараларын қолданады.

2-параграф. Пайдаланушылардың ақпараттық жүйелердегі парольдерін және есептік жазбаларын оқшаулауды басқару процесіне қойылатын талаптар

71. Банктің, ұйымның ақпараттық жүйелерінде пайдаланушылардың парольдерін және есептік жазбаларын оқшаулауды басқару жөніндегі функцияның мынадай өлшемдері қолданылады:

1) парольдің ең қысқа ұзындығы – осы өлшемнің мәні 8 символдан тұрады. Парольді осы өлшемге сәйкестігін тексеру пароль ауысқан сайын жүргізіледі, сәйкес келмеген жағдайда – пайдаланушыға хабарлама жіберіледі;

2) парольдің күрделілігі – парольде кемінде символдардың үш тобының: кішкентай әріптер, бас әріптерінің, цифрлық мәндердің, арнайы символдардың болуын тексеру мүмкіндігі. Парольдің осы өлшемге сәйкестігін тексеру пароль ауысқан сайын жүргізіледі, сәйкес келмеген жағдайда – пайдаланушыға хабарлама жіберіледі;

3) парольдің тарихы – жаңа пароль кемінде алдыңғы жеті парольді қайталамайды. Парольдің осы өлшемге сәйкестігін тексеру пароль ауысқан сайын жүргізіледі, сәйкес келмеген жағдайда – пайдаланушыға хабарлама жіберіледі;

4) парольдің ең қысқа пайдалану мерзімі – 1 (бір) жұмыс күні;

5) парольдің ең ұзақ пайдалану мерзімі – күнтізбелік 60 (алпыс) күннен аспайды. Парольдің осы өлшемге сәйкестігін тексеру ақпараттық жүйеге кірген сайын және пароль ауысқан кезде жүргізіледі. Парольдің ең ұзақ пайдалану мерзімі аяқталғанға дейін күнтізбелік 7 (жеті) күн және одан аз күн қалған жағдайда пайдаланушыға тиісті

хабарлама жіберіледі. Парольдің ең ұзақ қолданылу мерзімі аяқталғаннан кейін ақпараттық жүйе кіруді оқшаулайды және парольді міндетті түрде ауыстыруды талап етеді;

6) ақпараттық жүйеге бірінші рет кіру кезінде, не әкімші парольді ауыстырғаннан кейін ақпараттық жүйе пайдаланушыдан бұл рәсімді орындамау мүмкіндігінсіз парольді ауыстыруды сұратуға тиіс. Осы қағида парольдің қолданылу мерзімі туралы қағидадан басым болады;

7) ақпараттық жүйеде пайдаланушының белсенділігі күнтізбелік 30 (отыз) күннен аса болмаған жағдайда, оның есептік жазбасы автоматты түрде оқшауланады;

8) дұрыс емес парольді қатарынан бес рет енгізген кезде пайдаланушының есептік жазбасы уақытша оқшауланады;

9) пайдаланушы 30 (отыз) минуттан аса белсенді болмаған кезде ақпараттық жүйе пайдаланушының жұмыс істеу сеансын автоматты түрде аяқтайды, не пайдаланушының аутентификациялық деректерін енгізген кезде ғана оқшалаусыздандыру мүмкіндігімен жұмыс станциясын оқшаулайды.

72. Талаптардың 71-тармағының талаптары мынадай:

1) ақпараттық жүйе Талаптардың 71-тармағының талаптарына сәйкес келетін ақпараттық жүйемен аутентификациялау бөлігінде ықпалдастырылған;

2) бір ақпараттық жүйенің функциялары басқа ақпараттық жүйеде авторизацияланбаған кіру тәуекелін барынша азайтқан жағдайларда қолданылмайды.

73. Банк, ұйым парольдерді және есептік жазбаларды басқару процесін айқындайды және мыналарды қамтиды:

1) ақпараттық жүйелер әкімшілерінің ақпараттық жүйелерді пайдаланушылардың есептік жазбаларын басқару және олардың парольдерін ауыстыру;

2) есептік жазбаларды құруға өтінімдерді беру және қарау, сондай-ақ штаттан тыс оқиға туындаған кезде парольді өзгерту;

3) есептік жазбаларды өзгертуге немесе жоюға өтінімдер беру;

4) есептік жазбаларды құруға, өзгертуге немесе жоюға өтінім беретін тұлғаларды сәйкестендіру, сондай-ақ парольді өзгерту;

5) парольдерді үшінші тұлғаларға, ақпараттық жүйелерді басқарушыларға және банктің, ұйымның өзге де қызметкерлеріне заңсыз беруге тыйым салу;

6) пайдаланушыны дәлме-дәл идентификаттауды қамтамасыз ету кезінде көрсетілген уақыт аралығында ақпараттық қауіпсіздік бөлімшесімен келісім бойынша қызметтің үздіксіздігін қамтамасыз ету мақсатында бөтен есептік жазбаға қол жеткізуді ұсынуды қоспағанда, ақпараттық жүйелерде бөтен есептік жазбалармен жұмыс істеуге жол бермеу болып табылады.

3-параграф. Ақпарат қауіпсіздігін қамтамасыз ету процесіне қойылатын талаптар

74. Интернетті және электрондық поштаны пайдаланған кезде ақпаратты қорғау процесін банк, ұйым мынадай әдістердің кез келгенін пайдалана отырып, бірақ олармен шектелмей айқындайды:

1) ұйымдастырушылық: банк, ұйым айқындайтын шектеулер, қызметкерлердің хабардар болуын қамтамасыз ету, Интернет желісіне, жедел хабарламалар қызметіне, бұлттық сервистерге, IP-телефонияға және сыртқы электрондық почтаға кіру рұқсаты бар қызметкерлердің санын шектеу;

2) бағдарламалық-техникалық: пайдаланушылар санын және олардың интернет-ресурстарына кіруін шектеу, Интернетке, оның ішінде жедел хабарламалар қызметі, IP-телефония және сыртқы электрондық почта арқылы берілетін ақпаратты бақылау, Интернетке кіруді терминалдық сервер арқылы беру, желі сегменттерін бөлу, сыртқы электрондық почтаның мұрағатын жүргізу (сақтау мерзімін банк, ұйым айқындайды, осы мұрағаттағы ақпаратты өзгертуге немесе жоюға кіруді шектеу), банктің, ұйымның ақпараттық инфрақұрылымының қорғау периметріне бағытталған шабуылдарға қарсы іс-қимыл жасау жүйелерін пайдалану, жіберілетін ақпаратты шифрлау.

75. Сыртқы электрондық ақпаратты тасымалдағыштарды пайдаланған кезде ақпаратты қорғау үшін мынадай әдістердің кез келгені қолданылады, бірақ олармен шектелмейді:

1) ұйымдастырушылық: банк, ұйым айқындайтын шектеулер, қызметкерлердің хабардар болуын қамтамасыз ету, сыртқы ақпарат тасымалдағыштарға жазба жасауға кіру рұқсаты бар қызметкерлердің санын шектеу;

2) бағдарламалық-техникалық: ақпаратты сыртқы тасымалдағыштарға жазуды шектеуді, бақылауды және шифрлауды қамтамасыз ететін бағдарламалық-техникалық құралдарды пайдалану; банк, ұйым қызметкерлерінің жұмыс станцияларында немесе серверлерде пайдаланылмайтын енгізу-шығару порттарын және сыртқы тасымалдағышта жазба жасау құрылғыларын ажырату.

76. Қағаз тасымалдағыштарды пайдалану кезінде ақпаратты қорғау үшін мынадай әдістердің кез келгені пайдаланылады, бірақ олармен шектелмейді:

1) ұйымдастырушылық: банк, ұйым айқындайтын шектеулер, қызметкерлердің хабардар болуын қамтамасыз ету, қорғалатын ақпарат қамтылған құжаттармен жұмыс жасауға кіру рұқсаты бар қызметкерлердің санын шектеу;

2) бағдарламалық-техникалық: ақпаратты қағаз тасымалдағыштарына шығаруды бақылауды қамтамасыз ететін бағдарламалық-техникалық құралдарды пайдалану.

77. Штаттық ақпарат тасымалдағыштар жоғалған жағдайда, ақпаратты қорғау үшін мынадай әдістердің кез келгені пайдаланылады, бірақ олармен шектелмейді:

1) ұйымдастырушылық: банк, ұйым айқындайтын шектеулер, банктің, ұйымның периметрінің нақты қауіпсіздігін қамтамасыз ету, қызметкерлердің хабардар болуын қамтамасыз ету, ақпарат тасымалдағыштарын жарамсыз ету нормалары;

2) бағдарламалық-техникалық: жүйелік блоктарды ашуды бақылайтын құралдарды пайдалану, жұмыс станцияларында, серверлерде ақпаратты шифрлау, дерекқорын басқару жүйелерінде ақпаратты шифрлау немесе токенизациялау (түпнұсқа деректерді кездейсоқ деректер (токен) жинағын пайдалана отырып қандай да бір суррогатпен ауыстыру).

78. Қорғалатын ақпаратты жою оны қалпына келтіруді болдырмайтын әдістермен, тасымалдағыштың түріне байланысты аталған ақпарат жоюдың мына әдістерінің кез келгенін пайдалана отырып, жүргізіледі:

1) ақпарат тасымалдағышты нақты жою;

2) ақпарат тасымалдағышқа электромагниттік әсер ету (магниттік тасымалдағыштар үшін);

3) электрондық ақпаратты мамандандырылған бағдарламалық құралдармен бағдарламалық жою.

4-параграф. Ақпараттық инфрақұрылымның қорғау периметрінің қауіпсіздігін қамтамасыз ету процесіне қойылатын талаптар

79. Банк, ұйым ақпараттық-коммуникациялық инфрақұрылымының қорғау периметрін (бұдан әрі – қорғау периметрі) айқындайды. Ақпараттық технологиялар бөлімшесі қорғау периметрінің схемасын және қорғау периметрінің қауіпсіздігін қамтамасыз ету құралдары басқарушыларының тізбесін бекітеді және жұмыс істейтін жағдайда қолдайды.

80. Банктің, ұйымның қорғау периметрінен шығатын қалалық телефон желісімен қосылғыштарды қоспағанда, телекоммуникациялық қосылғыштар.

81. Телекоммуникациялық қосылғыштарды шифрлау ақпараттық қауіпсіздік жөніндегі бөлімшемен келісілген әдістермен жүргізіледі.

82. Талаптардың 80 және 81-тармақтарында көрсетілген телекоммуникациялық қосылғыштарды шифрлаумен бірге берілетін ақпаратты шифрлау қолданылады.

83. Қорғау периметрінде ақпараттық инфрақұрылымға кіруді шектеу үшін желіаралық экрандар орнатылады.

84. Желіаралық экрандар орнатылған кіру қағидалары банктің, ұйымның ақпараттық активтерінің жұмыс істеп тұру үшін пайдаланылмаған қосылғыштарды оқшаулауға теңшеледі. Көрсетілген қағидалар ақпараттық қауіпсіздік бөлімшесімен келісіледі. Қорғау периметріне жасалған шабуылдарды анықтау және көрсету үшін басып кіруді анықтау және алдын алу құралдары пайдаланылады.

85. Банк, ұйым "қызмет көрсетуден бас тарту" сияқты шабуылдарды болдырмау шараларын қолдануды қамтамасыз етеді. Аталған шараларды іске асыру кезінде қорғау периметрін қамтамасыз ету жүйесінің штаттық тетіктері және (немесе) қорғау

периметрінің қауіпсіздігін қамтамасыз етудің қосымша әдісі (телекоммуникациялық қызметтердің провайдерлерімен шарттар, осы тектес шабуылдан қорғау бойынша тиісті функционалы бар арнайы жүйелерді орнату және басқа тәсілдер) пайдаланылады.

86. Банктің, ұйымның ақпараттық активтеріне қорғау периметрінен тыс жерден кіруді пайдаланушыны аутентификациялай отырып қорғау периметрінде шифрленген арна бойынша ғана ұсынылады. Қорғау периметрінен тыс жерден ақпараттық жүйелерге кіру екі факторлық аутентификациялау әдісін пайдалана отырып қана ұсынылады (үш фактордың ішінен екеуін пайдалану арқылы: "мен нені білем", "менде не бар", "мен кіммін").

87. Пайдаланушыларға Интернет желісінің ресурстарына кірудің, сондай-ақ сыртқы электрондық поштаны пайдаланудың қауіпсіздігін қамтамасыз ету үшін тиісті шлюздер орнатылады, олар мыналарды:

1) трафикті зиянды кодтан тазалауды;

2) деструктивті функциялары бар Интернет ресурсты бұғаттауды;

3) пошта трафигін спамнан тазалауды қамтамасыз етеді;

4) кіріс электрондық поштаны жөнелтушінің домендік атауын аутентификациялауды және криптографиялық алгоритмдерді пайдалана отырып, шығыс электрондық поштаның домендік атауын аутентификациялау мүмкіндігін қамтиды.

88. Қорғау периметрінің қауіпсіздігін қамтамасыз ету құралының конфигурациясы өндірушілердің ұсынымдарын ескере отырып орындалады және банк, ұйым айқындаған кезеңділікпен қайта қаралады. Алдын ала белгіленген есептік жазбаларға парольдер міндетті тәртіпте өзгертіледі. Пайдаланылмаған, алдын ала белгіленген есептік жазбалар бұғатталады немесе жойылады.

89. Осы саладағы тәуелсіз сыртқы сарапшылар банк, ұйым айқындаған кезеңділікпен ақпараттық инфрақұрылымға рұқсатсыз кіруге тестілеу жүргізеді. Осы тестілеудің шегінде, жүйелік және қолданбалы бағдарламалық қамтылымның осал жерлерін іздестіру және пайдалану мүмкіндіктерінен басқа "қызмет көрсетуден бас тарту" шабуылына ұқсатып жүктеме тестілер, сондай-ақ әлеуметтік инженерия бойынша тестілер жүргізіледі.

5-параграф. Ақпараттық инфрақұрылымды қорғауды қамтамасыз ету процесіне қойылатын талаптар

90. Ақпараттық жүйенің АТ-менеджері ақпараттық активтің жүйелік уақытын эталондық уақыттың орталықтандырылған дереккөзімен үйлестіруді қамтамасыз етеді.

91. Ақпараттық технологиялар бөлімшесі ішкі желілік инфрақұрылымды кемінде мынадай сегменттерге:

1) клиенттік (пайдаланушылық);

2) серверлік (инфрақұрылымдық);

3) әзірлемелер (бар болса);

4) тестілік бөлуді қамтамасыз етеді.

92. Желілік инфрақұрылым сегменттері арасында ақпараттық активтердің жұмыс істеуі үшін пайдаланылмаған қосылғыштарды оқшаулауға рұқсат беру қағидалары теңшеледі.

93. Банк, ұйым ақпараттық инфрақұрылымды қорғау мақсатында банктің, ұйымның ақпараттық инфрақұрылымындағы болжанбаған (аномальді) белсенділікті анықтауға мүмкіндік беретін әдістерді немесе жүйелерді қолданады.

94. Банк, ұйым ақпараттық инфрақұрылымның түпкілікті құрылғыларына қауіпсіздіктің қажетті теңшеуін орнатуға мүмкіндік беретін операциялық жүйелердің, желілік архитектуралардың немесе бағдарламалық қамтылымның мүмкіндіктерін пайдалана отырып қауіпсіздіктің топтық саясаттарын құру және қолдану жөніндегі ұйымдық және (немесе) техникалық шараларды қолданады.

Қауіпсіздіктің топтық саясатынан ақпараттық инфрақұрылымның түпкілікті құрылғыларын алып тастау ақпараттық технологиялар бөлімшесімен келісіледі.

95. Банктің, ұйымның бірнеше ақпараттық активтерін бір серверде немесе гипервизорда орналастырған кезде осы серверде немесе гипервизорда орналастырылған барынша күрделі ақпараттық активке сәйкес келетін деңгейде қорғау қамтамасыз етіледі.

6-параграф. Ақпараттық жүйелерді қорғауды қамтамасыз ету процесіне қойылатын талаптар

96. Ақпараттық жүйелерді өнеркәсіптік пайдалану ортасында әзірлеу және пысықтау жүзеге асырылмайды.

97. Әзірлеу, тестілеу және өнеркәсіптік пайдалану орталары осы орталардың кез келгеніне енгізілген өзгерістер басқа ортада орналасқан ақпараттық жүйеге әсер етпейтіндей етіп бір бірінен бөлінеді.

98. Қорғалатын ақпаратты әзірлеу және тестілеу ортасында пайдаланған жағдайда оларды қорғау бойынша тиісті шаралар қолданылады.

99. Банктің, ұйымның және әзірлеуді жүзеге асыратын тысқары ұйымдардың ақпараттық технологиялар бөлімшесі қызметкерлерінің ақпараттық жүйенің өзгерістерін өнеркәсіптік ортаға ауыстыру өкілеттіктері, сондай-ақ өнеркәсіптік ортадағы ақпараттық жүйелерге әкімшілік кіру рұқсаты жоқ.

100. Ақпараттық жүйені өнеркәсіптік пайдалануға енгізудің алдында онда қалыпты жағдай бойынша орнатылған қауіпсіздік теңшеулері банкте, ұйымда белгіленген ақпараттық қауіпсіздікке қойылатын талаптарына сәйкес келетін теңшеулерге өзгертіледі. Көрсетілген теңшеулер тестілеу кезінде пайдаланылатын парольдерге ауыстыруды, сондай-ақ барлық тестілік есептік жазбаларды алып тастауды қамтуға тиіс

.

101. Артықшылық берілген есептік жазбалардың пайдаланылуын бақылау:

1) ақпараттық жүйелер әкімшілерінің тізбесін жасау және бекіту (операциялық жүйе, дерекқорды басқару жүйесі, қосымша);

2) ақпараттық жүйелерді әкімшілендіру функцияларын орындау кезінде қосарланған бақылауды енгізу және (немесе) артықшылық берілген есептік жазбалардың пайдаланылуын бақылаудың арнайы кешендерін енгізу арқылы қамтамасыз етіледі.

102. Банктің, ұйымның ақпараттық жүйелері техникалық қолдаумен қамтамасыз етіледі, оның құрамына тиісті ақпараттық жүйенің жаңартуларын, оның ішінде қауіпсіздік жаңартуларын ұсыну қызметтері кіреді.

7-параграф. Қызметкерлермен жұмыс жүргізу процесіне қойылатын талаптар

103. Жұмысқа қабылдау кезінде банктің, ұйымның жаңа қызметкері қорғалатын ақпаратты жария етпеу туралы міндеттемеге қол қояды. Міндеттеме қызметкердің жеке ісіне тігіледі.

104. Жаңа қызметкер жұмысқа қабылданған кезде ол жұмысқа қабылданған сәттен бастап 5 (бес) жұмыс күнінен кешіктірмей ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі негізгі талаптармен (кіріспе нұсқаулық) қолын қоя отырып танысады. Танысу нәтижелері тиісті нұсқаулық журналында немесе нұсқаулықтан өткенін растайтын жеке құжатта тіркеледі. Нұсқаулықтан өткенін растайтын жеке құжат қызметкердің жеке ісіне тігіледі.

105. Қызметкерді ақпараттық қауіпсіздікке қойылатын талаптармен танысқанға дейін оған маңызды емес ақпараттық активтерге ғана кіруге рұқсат етіледі.

106. Банктің, ұйымның қызметкерімен жасасқан еңбек шартында ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі талаптарды сақтау туралы міндеттеме қамтылады.

107. Банк, ұйым қызметкерлердің ақпараттық қауіпсіздікті қамтамасыз ету мәселелері жөнінде хабардар болуын арттыру бағдарламасын әзірлейді. Бұл ретте қызметкерлердің хабардар болуын арттырудың мынадай әдістері қолданылуы мүмкін:

1) банктің, ұйымның ішкі құжаттарымен, сондай-ақ оларға енгізілген өзгерістермен және толықтырулармен танысу;

2) банктің, ұйымның атқарушы органы бекітетін банк, ұйым қызметкерлеріне тест жүргізу жоспарына сәйкес банктің, ақпараттық қауіпсіздік жөніндегі ұйымның ішкі құжаттарының талаптарын білуге арналған тест жүргізу;

3) банк, ұйым айқындаған әдістер.

108. Нұсқаулық жүргізу кезінде сондай-ақ хабардар болуды арттыру жөніндегі одан кейінгі іс-шаралар өткізу кезінде:

1) "әлеуметтік инженерияға" қарсы іс-қимыл әдістері;

2) Қазақстан Республикасының банктік заңнамасында тыйым салынған ақпаратты таратуға тыйым салу;

3) банктің, ұйымның ақпараттық жүйелерінде құрылатын, сақталатын және өңделетін кез келген ақпаратты мониторингтеуді жүзеге асыруға банктің, ұйымның құқығы туралы ереже;

4) ақпараттық қауіпсіздікті қамтамасыз етуге қойылатын талаптар белгіленетін ішкі құжаттарды бұзғаны үшін көзделген жауапкершілік туралы талаптар.

109. Банк, ұйым ақпараттық қауіпсіздік, ақпараттық қауіпсіздік тәуекелдерін басқару бөлімшелері және ішкі аудит бөлімшесі қызметкерлерінің біліктілігін көтеруді мыналарды жүргізу арқылы қамтамасыз етеді:

1) ішкі іс-шаралар (лекциялар, семинарлар);

2) сырттай оқыту (курстарға, семинарларға қатысу – әрбір қызметкер үшін үш жылда кемінде бір реттен).

110. Қызметкер жұмыстан босатылған кезде, ақпараттық қауіпсіздікті қамтамасыз ету мақсатында мыналар бойынша іс-шаралар жүзеге асырылады:

1) банктің, ұйымның құжаттары мен ақпараттық активтерін қабылдау-өткізу;

2) куәліктерді, рұқсат қағаздарын және рұқсат ету құжаттарын тапсыру;

3) жұмыстан босатылатын қызметкерлермен конфиденциалды ақпаратты жария етпеу туралы нұсқама жүргізу;

4) ақпараттық жүйелерде есептік жазбаларды оқшаулау немесе жою.

8-параграф. Ақпараттық жүйелерде аудиторлық із жүргізу процесіне қойылатын талаптар

111. Ақпараттық жүйенің АТ-менеджері ұйымдастырушылық және техникалық деңгейде аудиторлық іздің жүргізілуін және өзгермеуін қамтамасыз етеді.

112. Банктің, ұйымның ақпараттық активтерінде аудиторлық із жүргізу функциясы пайдаланылады, ол мыналарды көрсетеді:

1) ақпараттық активте қосылғыштарды орнату, сәйкестендіру, бірегейлендіру және авторизациялау (табысты және сәтсіз) оқиғалары;

2) қауіпсіздік теңшеулерін түрлендіру оқиғалары;

3) пайдаланушылардың топтарын және олардың өкілеттіктерін түрлендіру оқиғасы;

4) пайдаланушылардың есептік жазбаларын және олардың өкілеттіктерін түрлендіру оқиғасы;

5) ақпараттық жүйедегі жаңартуларды және (немесе) өзгерістерді орнатуды көрсететін оқиға;

6) аудиттің өлшемдерінің өзгеру оқиғасы;

7) жүйелік өлшемдердің өзгерістер оқиғасы.

113. Аудиторлық із форматы мынадай ақпаратты қамтиды:

1) іс-қимыл жасайтын пайдаланушының сәйкестендіргіші (логины);

2) іс-қимыл жасау күні және уақыты;

3) пайдаланушының жұмыс станциясының атауы және (немесе) іс-қимыл жасалған IP мекенжайы;

4) іс-қимыл жүргізілген объектілердің атауы;

5) жасалған іс-қимылдың түрі және атауы;

6) іс-қимылдың нәтижесі (ойдағыдай немесе ойдағыдай емес).

114. Аудиторлық ізді сақтау мерзімі жедел қолжетімділікте кемінде 3 (үш) айды және архивтік қолжетімділікте кемінде 1 (бір) жылды не жедел қолжетімділікте кемінде 1 (бір) жылды құрайды.

9-параграф. Вирусқа қарсы қорғауды қамтамасыз ету процесіне қойылатын талаптар

115. Банк, ұйым лицензиялық вирусқа қарсы бағдарламалық қамтамасыз етуді немесе жұмыс стансаларында, ноутбуктарда, мобилді құрылғыларда, сол сияқты серверлерде, банкоматтарда және банктік киоскілерде бағдарламалық ортаның тұтастығы мен тұрақтылығын қамтамасыз ететін жүйелерді пайдаланады.

116. Банк, ұйым пайдаланатын вирусқа қарсы бағдарламалық қамтамасыз ету төмендегі талаптарға сәйкес келеді

1) белгілі сигнатурлар негізінде вирустарды анықтау;

2) эвристикалық талдау негізінде (вирустарға тән командалар мен тәртіптік талдауды іздестіру) вирустарды анықтау;

3) қосу кезінде ауыстырылатын тасымалдағыштарды сканерлеу;

4) кесте бойынша вирусқа қарсы базаны сканерлеуді және жаңартуды іске қосу;

5) басқарудың және мониторинг жүргізудің орталықтандырылған консолінің болуы;

6) пайдаланушы үшін вирусқа қарсы бағдарламалық қамтамасыз етудің, сондай-ақ вирусқа қарсы бағдарламалық қамтамасыз етуді жаңарту және вирустардың болмауын жоспарлы тексеру процестерінің жұмыс істеуін үзу мүмкіндігін оқшаулау;

7) виртуалды орта үшін – вирусқа қарсы бағдарламалық қамтамасыз етудің виртуалды орта қауіпсіздігінің қоса орнатылған функцияларын пайдалануы, мұндай мүмкіндіктер болмаған кезде – өндірушінің банк, ұйым пайдаланатын виртуалды орталарда вирусқа қарсы бағдарламалық қамтамасыз етуді тестіден өткізуі туралы растауы;

8) банкті, ұйымды қорғаудың периметрінен тыс пайдаланылатын мобилді құрылғылар және өзге де құрылғылар үшін желіаралық экранға шығарудың қоса орнатылған функцияларымен вирусқа қарсы бағдарламалық қамтамасыз етуді пайдалану.

117. Бағдарламалық ортаның тұтастығы мен тұрақтылығын қамтамасыз ететін жүйелерді пайдаланған кезде төмендегілер ең төменгі талаптар болып табылады:

1) жаңартуды және техникалық қолдауды көздейтін лицензиялық бағдарламалық қамтамасыз етудің болуы;

2) басқарудың және мониторинг жүргізудің орталықтандырылған консолінің болуы;

3) түпкілікті пайдаланушы үшін осы жүйенің жұмыс істеуін үзу үшін оқшаулау мүмкіндігінің болуы;

4) түпкілікті құрылғыларға орнату алдында вирусқа қарсы бағдарламалық қамтамасыз ету арқылы бағдарламалық ортаның бейінін тексеру мүмкіндігінің болуы;

5) қорғаудың периметрінен тыс пайдаланылатын мобилді құрылғылар және өзге де құрылғылар үшін желіаралық экранның болуы.

118. Вирусқа қарсы бағдарламалық қамтамасыз етуді таңдауды ақпараттық технологиялар бөлімшесі ақпараттық қауіпсіздік бөлімшесінің міндетті қатысуымен жүргізеді.

119. Вирусқа қарсы бағдарламалық қамтамасыз ету пайдаланушының барлық қызметтік процестерді барынша үздіксіз қолдануын қамтамасыз етеді (кесте бойынша сканерлеу, жаңарту және басқалары). Вирусқа қарсы бағдарламалық қамтамасыз етуді жаңарту тәулігіне кемінде бір рет, компьютерді толық сканерлеу – аптасына кемінде бір рет жүргізіледі.

10-параграф. Ақпараттық жүйелердің жаңартуларын және осалдығын басқару процесіне қойылатын талаптар

120. Ақпараттық жүйенің АТ-менеджері банктің, ұйымның ақпараттық активтерінің қауіпсіздік жаңартуларын уақытылы орнатуды қамтамасыз етеді.

121. Маңызды осалдықтарды жоятын ақпараттық жүйелерді жаңартулар ақпараттық қауіпсіздік бөлімшесімен келісілген жағдайларды қоспағанда, оларды жариялау және өндіруші таратқан күннен бастап бір айдан кешіктірмей орнатылады.

122. Ақпараттық жүйелерді жаңартулар өнеркәсіптік ортаға орнатылғанға дейін тестілеу ортасында сынақтан өтеді.

123. Ақпараттық қауіпсіздік жүйесімен келісу бойынша жаңартуларды орнату мүмкіндігі болмаған жағдайда, ақпараттық жүйенің АТ-менеджері түзету шараларын жүзеге асырады.

124. Ақпараттық қауіпсіздік бөлімшесі ақпараттық активтерді мамандандырылған бағдарламалық қамтамасыз етуді пайдалана отырып, осалдықтың болуына сканерлеуді (бұдан әрі – сканерлеу) (қорғаныстың техникалық талдауы) қамтамасыз етеді. Банктің, ұйымның ақпараттық активтерін сканерлеу 6 (алты) айда кемінде бір рет жоспарлы негізде жүргізіледі. Сканерлеуді банктің, ұйымның қызметкерлері және (немесе) сырттан мамандандырылған компаниялар жүргізе алады. Сканерлеудің нәтижелері анықталған осалдықтарды жою бойынша түзету шаралары жөнінде ұсынымдарды көрсете отырып, ақпараттық қауіпсіздіктің жағдайы туралы есеп түрінде қалыптастырылады.

125. Ақпараттық жүйенің АТ-менеджері анықталған осалдықтарды жою бойынша түзету шараларын іске асыруды қамтамасыз етеді.

Осалдықтарды жою бойынша жұмыстар аяқталысымен ақпараттық жүйенің АТ-менеджері анықталған осалдықтардың жойылғаны туралы растаманы ақпараттық қауіпсіздік бөлімшесіне ұсынады.

11-параграф. Ақпаратты криптографиялық қорғау құралдарын пайдалану процесіне қойылатын талаптар

126. Ақпаратты криптографиялық қорғау құралдарын пайдалану процесін банктің, ұйымның ақпараттық қауіпсіздік бөлімшесінің келісімі бойынша ақпараттық технологиялар бөлімшесі мыналарды қоса алғанда, бірақ олармен шектелмей:

1) ақпаратты криптографиялық қорғау құралдарының сипаттамасын (жүйенің атауы , криптоалгоритм, кілттің ұзындығы);

2) ақпаратты криптографиялық қорғау құралдарын пайдалану саласын;

3) ақпаратты криптографиялық қорғау құралдарын күйге келтірудің сипаттамасын;

4) негізгі ақпаратты басқару: генерация, қауіпсіз беру (кілт пен қорғалатын ақпаратты беру үшін түрлі арналарды пайдалану талаптары есебімен кілттерді алмастыру), сақтау, пайдалану және жою тәртібін;

5) негізгі ақпарат әшкереленген кездегі іс-әрекетті;

6) ақпаратты криптографиялық қорғау құралдарын соңғы пайдаланушылардың пайдалану тәртібін;

7) ақпаратты криптографиялық қорғау құралдарына әкімшілендіруге және негізгі ақпаратты басқаруға жіберілген тұлғалар тізбесін айқындайды.

12-параграф. Деректерді өңдеу орталықтарының нақты қауіпсіздігін қамтамасыз ету процесіне қойылатын талаптар

127. Банктің, ұйымның деректерді өңдеу орталықтары техникалық қауіпсіздіктің мынадай жүйелерімен:

1) кіруді бақылау және басқару жүйесімен;

2) күзет сигнализациясымен;

3) өрт сигнализациясымен;

4) өртті автоматты сөндіру жүйесімен;

5) температура мен ылғалдылықтың белгіленген өлшемдерін ұстап тұру жүйесімен;

6) бейнебақылау жүйесімен жарақтандырылады.

Серверлік және коммуникациялық жабдық үздіксіз қуат көздері арқылы электр қуаты жүйесіне қосылады.

Банкте, ұйымда деректерді өңдеу орталығы болмаған жағдайда аталған тармақтың талаптары банктің, ұйымның ақпараттық инфрақұрылымы жүйесі мен құрамдастары орналастырылған банктің, ұйымның үй-жайына қолданылады.

128. Деректерді өңдеу орталығына кіру рұқсаты тізбесін ақпараттық қауіпсіздік бөлімшесінің келісімі бойынша ақпараттық технологиялар бөлімшесінің басшысы бекітетін адамдарға беріледі.

129. Банк, ұйым деректерді өңдеу орталығына кіруді бақылау және басқару жүйесінің журналын жүргізеді, ол кемінде 1 (бір) жыл сақталады.

130. Деректерді өңдеу орталығының өртті автоматты сөндіру жүйесі бүкіл үй-жай көлемінің тұтануын болдырмауды қамтамасыз етеді.

131. Деректерді өңдеу орталығының бейне бақылау жүйесі деректерді өңдеу орталығының барлық кіреберістерін бақылауды қамтамасыз етеді. Деректерді өңдеу орталығында бейнекамераларды орналастыру деректерді өңдеу орталығы үй-жайының ішінде және кіреберісі алдында бейнебақылаумен қамтамасыз етілмеген аймақтардың болуына жол бермейді.

132. Деректерді өңдеу орталығының бейнебақылау жүйесі оқиғаларының жазбасы үздіксіз немесе қозғалыс детекторын пайдалана отырып жүргізіледі.

133. Деректерді өңдеу орталығының бейнебақылау жүйесінің мұрағаты кемінде 3 (үш) ай сақталады.

134. Деректерді өңдеу орталығынан тыс орналасқан серверлерге және белсенді желілік жабдыққа санкцияланбаған нақты кірудің алдын алу мақсатында олардың қауіпсіздігін қамтамасыз ету бойынша шаралар анықталады және іске асырылады.

135. Банктің, ұйымның ақпараттық активтеріне нақты рұқсатты ұсынуды банк, ұйым айқындайды.

13-параграф. Жұмыс станцияларын, ноутбуктарды және мобильдік құрылғыларды қорғауды қамтамасыз ету процесіне қойылатын талаптар

136. Банкте, ұйымда пайдаланушыларға бағдарламалық қамтамасыз етуді, жұмыс станцияларын, ноутбуктар мен перифериялық жабдықты өз бетінше орнатуды және теңшеуді жүргізуге тыйым салынатын ұйымдастырушылық және техникалық шаралар анықталады және енгізіледі.

137. Жергілікті әкімшінің қол жеткізу құқығы немесе жергілікті әкімшінің қол жеткізу құқығына ұқсас құқықтар пайдаланушы орындайтын функцияларды автоматтандыратын бағдарламалық қамтылымның жұмыс істеуі үшін талап етілетін жағдайларды қоспағанда, пайдаланушыларға жергілікті әкімшінің қол жеткізу құқығы немесе осыған ұқсас қол жеткізу құқығы берілмейді.

138. Пайдаланушының өз функционалдық міндеттерін бағдарламалық қамтамасыз етуді және жабдықты өз бетінше орнату және теңшеуді жүзеге асырусыз орындау мүмкіндігі болмаған жағдайда, мұндай пайдаланушыға жергілікті әкімші құқығы немесе ұқсас құқықтар беріледі.

139. Талаптардың 137 және 138-тармақтарында көрсетілген пайдаланушылардың тізбесін ақпараттық қауіпсіздік бөлімшесімен келісу бойынша ақпараттық технологиялар бөлімшесінің басшысы қалыптастырады, жаңартады және бекітеді. Ақпараттық қауіпсіздік бөлімшесі пайдаланушылардың Талаптардың 137 және 138-тармақтарында көрсетілген кіру құқықтарын бақылауды жүзеге асырады.

140. Ақпараттық технологиялар бөлімшесі банктің, ұйымның жұмыс станцияларын, ноутбуктарын және корпоративтік желісіндегі мобильдік құрылғыларды есепке алу

жүйесі осы жұмыс станциясының орналасқан орнын немесе мобильдік құрылғының тиесілілігін нақты сәйкестендіруге мүмкіндік береді.

141. Банктің, ұйымның қорғаныс периметрінің аумағынан тыс мобильдік құрылғылар, ноутбуктар банктің, ұйымның ақпараттық активтеріне қосылған жағдайда бұл құрылғыларға ақпараттық активтерге қорғалған рұқсатты қамтамасыз ететін (байланыс арнасын шифрлеу, екіфакторлы аутентификаттауды қамтамсыз ету, қашықтықтан мобильдік құрылғыдан деректерді жою) арнайы бағдарламалық қамсыздандыру орнатылады.

142. Банктің, ұйымның ақпараттық активтерін өңдеу үшін банк, ұйым қызметкерлерінің жеке ноутбуктарын және мобильді құрылғыларын қолдану кезінде берілген ноутбуктар мен мобильді құрылғыларға жеке деректерді және банктің, ұйымның ақпараттық активтерін өңдеу ортасын жіктеуді қамтамасыз ететін арнайы бағдарламалық қамтылым орнатылады.

143. Банктің, ұйымның ноутбукта және мобильдік құрылғыларда орналасқан бүкіл ақпараты шифрленген түрде сақталады.

10-тарау. Банктің, ұйымның қашықтан қызмет көрсету бағдарламалық қамтылымының қауіпсіздігіне қойылатын талаптар

Ескерту. Талаптар 10-тараумен толықтырылды - ҚР Қаржы нарығын реттеу және дамыту агенттігі Басқармасының 17.10.2023 № 75 (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) қаулысымен.

144. Банктің, ұйымның қашықтан қызмет көрсету бағдарламалық қамтылымына:

1) веб-қосымшалар серверлерінің бағдарламалық қамтылымы (бұдан әрі – веб-қосымша);

2) мобильді құрылғыларға арналған бағдарламалық қамтылым (бұдан әрі – мобильді қосымша);

3) бағдарламалық интерфейстердің бағдарламалық қамтылымы (бұдан әрі – серверлік ҚБҚ) кіреді.

145. Қашықтан қызмет көрсету бағдарламалық қамтылымын әзірлеу және (немесе) пысықтауды банк, ұйым бағдарламалық қамтылымды әзірлеу және (немесе) пысықтау тәртібін, әзірлеу кезеңдерін және олардың қатысушыларын регламенттейтін банктің, ұйымның ішкі құжаттарына сәйкес жүзеге асырады.

146. Банктің, ұйымның қашықтан қызмет көрсету бағдарламалық қамтылымын әзірлеу және (немесе) пысықтау тысқары ұйымға және (немесе) үшінші тұлғаға берілген жағдайда, банк, ұйым тысқары ұйымның және (немесе) үшінші тұлғаның осы тараудың және ішкі құжаттардың талаптарын орындауын қамтамасыз етеді, қашықтан қызмет көрсету бағдарламалық қамтылымның қауіпсіздігі жағдайы үшін жауап береді.

147. Банкте, ұйымда әзірленетін қашықтан қызмет көрсету бағдарламалық қамтылымның бастапқы кодтарын сақтау резервтік көшірме жасауды қамтамасыз ете

отырып, банктің, ұйымның аясында орналастырылатын мамандандырылған код репозиторияларын басқару жүйесінде жүзеге асырылады.

148. Банкте, ұйымда қабылданған қашықтан қызмет көрсету бағдарламалық қамтылымды әзірлеу және (немесе) пысықтау тәсіліне қарамастан, қауіпсіздікті тестілеу міндетті кезең болып табылады, оның барысында кемінде мынадай іс-шаралар жүзеге асырылады:

1) бастапқы кодтың статикалық талдауы;

2) құрауыштардың және тысқары кітапханалардың талдауы.

149. Банктің, ұйымның қашықтан қызмет көрсету бағдарламалық қамтылымының бастапқы кодының статикалық талдауы тексерілетін бағдарламалық қамтылымда қолданылатын барлық бағдарламалау тілінің талдауын қолдайтын, бастапқы кодтың статикалық талдауының сканерін пайдаланумен жүргізіледі, оның функцияларына мынадай осалдықтарды анықтау кіреді, бірақ олармен шектелмейді:

1) зиянды кодтың кіруіне мүмкіндік беретін тетіктердің болуы;

2) осал операторларды және бағдарламалау тілдерінің функцияларын пайдалану;

3) әлсіз және осал криптографиялық алгоритмдерді қолдану;

4) белгілі бір жағдайларда қызмет көрсетуден бас тартуды немесе қосымшаның жұмысын айтарлықтай баяулатуды тудыратын кодты пайдалану;

5) қосымшаны қорғау жүйелерін айналып өту тетіктерінің болуы;

6) кодта құпияларды ашық түрде пайдалану;

7) қосымшаның қауіпсіздігін қамтамасыз ету үлгілері мен тәжірибелерін бұзу.

150. Банктің, ұйымның қашықтан қызмет көрсету бағдарламалық қамтылымының құрауыштарын және (немесе) тысқары кітапханаларын талдау құрауыштың және (немесе) тысқары кітапхананың қолданылатын нұсқасына тән белгілі осалдықтарды анықтау мақсатында, сондай-ақ құрауыштар және (немесе) тысқары кітапханалар және олардың нұсқалары арасындағы тәуелділіктерді бақылау үшін жүргізіледі.3. Осы қаулының орындалуын бақылау Қазақстан Республикасының Қаржы нарығын реттеу және дамыту агенттігі Төрағасының жетекшілік ететін орынбасарына жүктелсін.

151. Банк, ұйым атқарушы орган бекіткен ішкі құжатта айқындалған тәртіпте анықталған осалдықтарды жою жөнінде түзету шараларының іске асырылуын қамтамасыз етеді. Бұл ретте, маңызды осалдықтар қашықтан қызмет көрсету бағдарламалық қамтылымды және (немесе) оның жаңа нұсқаларын пайдалануға енгізуге дейін жойылады.

152. Банк, ұйым ақпараттық қауіпсіздік бөлімшесімен келісілгеннен кейін қашықтан қызмет көрсету бағдарламалық қамтылымын және (немесе) оның жаңа нұсқаларын пайдалануға енгізуді жүзеге асырады.

153. Банк, ұйым қашықтан қызмет көрсету бағдарламалық қамтылымының бастапқы кодтарының және соңғы 3 (үш) жыл ішінде пайдалануға енгізілген

қауіпсіздікті тестілеу нәтижелерінің барлық нұсқаларын жедел режимде сақтауды және оларға қол жеткізуді қамтамасыз етеді.

154. Қашықтан қызмет көрсету бағдарламалық қамтылымының клиенттік және серверлік тараптары арасында деректер алмасу Transport Layer Security (Транспорт Лейер Секьюрити) шифрлау хаттамасының 1.2-ден төмен емес нұсқасын пайдалана отырып шифрланады.

155. Банктің, ұйымның мобильді қосымшасында клиентті бастапқы тіркеу кезінде Сәйкестендіру деректерімен алмасу орталығы (бұдан әрі – СДАО) арқылы немесе банктің, ұйымның құрылғылары арқылы алынған биометриялық деректерді пайдалана отырып, клиентті биометриялық сәйкестендіруді жүзеге асырады.

156. Мобильді қосымшаға кіру кодын (құпиясөзін) өзгерту СДАО растаған немесе банктің, ұйымның құрылғылары арқылы алынған биометриялық деректерді пайдалана отырып, клиентті биометриялық сәйкестендіруді қолданумен жүзеге асырылады.

157. Қашықтан қызмет көрсету бағдарламалық қамтылымда клиентті сәйкестендіру және бірдейлендіру банктің, ұйымның ішкі құжаттарында белгіленген қауіпсіздік рәсімдеріне сәйкес екі факторлы (үш фактордың екеуін қолдану: білім, иелену, ажырамастық) бірдейлендіру әдістерін қолдана отырып жүзеге асырылады.

158. Қашықтан қызмет көрсету бағдарламалық қамтылымды кроссдомендік бірдейлендіру тетігі ақпараттық қауіпсіздік жөніндегі бөлімшемен келісіледі.

159. Веб-қосымша:

1) веб-қосымшаның тек қана банкке, ұйымға тиесілігін сәйкестендіруді (домендік аты, логотиптері, корпоративтік түстері);

2) браузердің жадысында авторландырылған деректерді сақтауға тыйым салуды;

3) енгізілген құпияларды бүркемелеуді;

4) клиентті авторландыру парақшасында веб-қосымшаны пайдалану кезінде басшылыққа алу ұсынылатын кибергигиенаны қамтамасыз ету шаралары туралы хабардар етуді;

5) қате туралы ең аз қажетті ақпарат бере отырып, клиенттің интерфейсінде конфиденциалды деректердің көрсетілуіне жол бермей қателер мен ерекшеліктерді қауіпсіз тәсілмен өңдеуді қамтамасыз етеді.

160. Мобильді қосымша:

1) мобильді қосымшаның тек қана банкке, ұйымға тиесілігін сәйкестендіруді (қосымшалардың ресми дүкеніндегі деректер, логотиптер, корпоративтік түстер);

2) операциялық жүйенің тұтастығын бұзу және (немесе) қорғау тетіктерін айналып өту белгілерін анықтаған, қашықтан басқару процестерін анықтаған жағдайда банктің, ұйымның қашықтан қызмет көрсету бойынша функционалын бұғаттауды;

3) клиентті мобильді қосымшаның жаңартуларының бар екендігі туралы хабардар етуді;

4) маңызды осалдықтарды жою қажет болған жағдайда, мобильді қосымшаның жаңартуларын мәжбүрлеп орнату немесе оларды орнатқанға дейін мобильді қосымшаның функционалын бұғаттау мүмкіндігін;

5) конфиденциалды деректерді мобильді қосымшаның қорғалған контейнерінде немесе жүйелік есепктік деректерді сақтау орнында сақтауды;

6) конфиденциалды деректерді кэштеуді алып тастауды;

7) мобильді қосымшаның резервтік көшірмелерінен ашық түрдегі конфиденциалды деректерді алып тастауды;

8) клиентті мобильді қосымшаны пайдалану кезінде басшылыққа алу ұсынылатын кибергигиенаны қамтамасыз етудің әдістері туралы хабардар етуді;

9) клиентті оның есептік жазбасындағы авторландыру оқиғалары, құпиясөзді өзгерту және (немесе) қалпына келтіру, банк, ұйым тіркеген мобильді телефон нөмірінің өзгеруі туралы хабардар етуді;

10) ақшалай қаражатпен операцияларды жүзеге асыру барысында -клиенттің рұқсаты болған жағдайда банктің, ұйымның серверлік ҚБҚ-ға мобильді құрылғының геолокациялық деректерін беру не мұндай рұқсаттың жоқ екендігі туралы ақпарат беруді қамтамасыз етеді.

161. Банк, ұйым өз тарапынан:

1) жауапта конфиденциалды деректердің жария болуына жол бермей, проблеманы анықтау үшін ең аз қажетті ақпарат ұсына отырып, қателер мен ерекшеліктерді қауіпсіз тәсілмен өңдеуді;

2) мобильді қосымшаларды және олармен байланысты құрылғыларды сәйкестендіруді және бірдейлендіруді;

3) жалған сұрау салулармен және зиянды кодтың кірулерімен шабуылдардың алдын алу үшін деректердің жарамдылығын тексеруді қамтамасыз етеді.

Қазақстан Республикасының
Ұлттық Банкі Басқармасының
2018 жылғы 27 наурыздағы
№ 48 қаулысына
2-қосымша

Ақпараттық жүйелердегі бұзушылықтар, іркілістер туралы мәліметтерді қоса алғанда, ақпараттық қауіпсіздіктің оқыс оқиғалары туралы ақпаратты беру қағидалары мен мерзімдері

Ескерту. Қағидалары мен мерзімдері жаңа редакцияда - ҚР Қаржы нарығын реттеу және дамыту агенттігі Басқармасының 29.04.2022 № 30 (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) қаулысымен.

1. Осы Ақпараттық жүйелердегі бұзушылықтар, іркілістер туралы мәліметтерді қоса алғанда, ақпараттық қауіпсіздіктің оқыс оқиғалары туралы ақпаратты беру қағидалары мен мерзімдері (бұдан әрі – Қағидалар) "Қазақстан Республикасындағы банктер және

банк қызметі туралы" Қазақстан Республикасы Заңы 61-5-бабының 7-тармағына сәйкес әзірленді және банктердің, Қазақстан Республикасының бейрезидент-банктері филиалдарының (бұдан әрі - банк) және банк операцияларының жекелеген түрлерін жүзеге асыратын ұйымдардың (бұдан әрі - ұйым) ақпараттық қауіпсіздігін қамтамасыз етуге қойылатын талаптарды, ақпараттық жүйелердегі бұзушылықтар, іркілістер туралы мәліметтерді қоса алғанда, ақпараттық қауіпсіздіктің оқыс оқиғалары туралы ақпаратты беру қағидалары мен мерзімдерін айқындайды.

2. Қағидаларда "Ақпараттандыру туралы" Қазақстан Республикасының Заңында көзделген ұғымдар, сондай-ақ мынадай ұғымдар пайдаланылады:

1) ақпараттандыру саласындағы ақпараттық қауіпсіздік (бұдан әрі – ақпараттық қауіпсіздік) – электрондық ақпараттық ресурстардың, ақпараттық жүйелердің және ақпараттық-коммуникациялық инфрақұрылымның сыртқы және ішкі қатерлерден қорғалуының жай-күйі;

2) ақпараттық-коммуникациялық инфрақұрылым (бұдан әрі – ақпараттық инфрақұрылым) – электрондық ақпараттық ресурстарды қалыптастыру және оларға қолжетімділік беру мақсатында технологиялық ортаның жұмыс істеуін қамтамасыз етуге арналған ақпараттық-коммуникациялық инфрақұрылым объектілерінің жиынтығы;

3) ақпараттық қауіпсіздік қатері – ақпараттық қауіпсіздіктің оқыс оқиғасының туындауына алғышарттар жасайтын жағдайлар мен факторлардың жиынтығы;

4) ақпараттық қауіпсіздіктің оқыс оқиғалары туралы ақпарат – ақпараттық-коммуникациялық инфрақұрылымның немесе оның жекелеген объектілерінің жұмысында жеке немесе сериялық туындайтын, олардың тиісінше жұмыс істеуіне қауіп келтіретін іркілістер туралы ақпарат және (немесе) банктің, ұйымның электрондық ақпараттық ресурстарын заңсыз алу, көшіру, тарату, модификациялау, жою немесе бұғаттауға арналған талаптар;

5) ақпараттық қауіпсіздіктің оқыс оқиғасы – ақпараттық-коммуникациялық инфрақұрылымның немесе оның жекелеген объектілерінің жұмысында жеке немесе сериялық туындайтын, олардың тиісінше жұмыс істеуіне қауіп келтіретін және (немесе) банктің, ұйымның электрондық ақпараттық ресурстарын заңсыз алу, көшіру, тарату, модификациялау, жою немесе бұғаттауға арналған талаптар;

6) кіру – ақпараттық активтерді пайдалану мүмкіндігі;

7) "қызмет көрсетуден бас тарту" түріндегі шабуыл (DoS немесе DDoS-шабуыл, шабуылдың сыртқы көздерінің санына байланысты) – ақпараттық жүйе жұмысының штаттық режимін бұзу мақсатында ақпараттық жүйеге шабуыл жасау немесе жүйенің заңды пайдаланушылары ұсынылатын ресурстарға қолжетімділік ала алмайтын, не бұл қолжетімділік қиын болатын жағдайлар жасау;

8) уәкілетті орган - қаржы нарығы мен қаржы ұйымдарын реттеу, бақылау және қадағалау жөніндегі уәкілетті орган.

3. Банк, ұйым уәкілетті органға ақпараттық қауіпсіздіктің мынадай анықталған оқыс оқиғалары туралы ақпаратты ұсынады:

1) қолданбалы және жүйелік бағдарламалық қамтамасыз етуде осалдықтарды пайдалану;

2) ақпараттық жүйеге санкцияланбаған кіру;

3) ақпараттық жүйеге немесе деректерді беру желісіне "қызмет көрсетуден бас тарту" шабуылы;

4) сервердің зиянды бағдарламамен немесе кодпен зақымдануы;

5) ақпараттық қауіпсіздік бақылауын бұзу салдарынан ақша қаражатын санкцияланбай аударуды жүзеге асыру;

6) ақпараттық жүйелердің бір сағаттан артық тұрып қалуына әкеп соққан ақпараттық қауіпсіздіктің өзге де оқыс оқиғалары жатады.

Осы тармақта көрсетілген ақпараттық қауіпсіздіктің оқыс оқиғалары туралы ақпаратты банк немесе ұйым ақпараттық қауіпсіздік оқиғалары мен оқыс оқиғалары туралы ақпаратты өңдеуге арналған және ақпараттық қауіпсіздік жүйелерімен немесе ақпараттық инфрақұрылымдағы оқиғалар туралы ақпаратты нақты уақытта жинауды және талдауды жүзеге асыратын банктің, ұйымның жүйелерімен ықпалдастырылған уәкілетті органның автоматтандырылған жүйесі (бұдан әрі – ААӨЖ) арқылы немесе ұсынылатын деректердің конфиденциалдығын және түзетілмеуін қамтамасыз ететін криптографиялық қорғау құралдары бар ақпараттың жеткізілуіне кепілдік беретін көлік жүйесін пайдалана отырып, электрондық форматта дереу береді.

4. Банк, ұйым ақпараттық қауіпсіздікті қамтамасыз етудің қабылданған шараларының бұзылғаны туралы не ақпараттық қауіпсіздікке ықтимал қатысы бар бұрын белгісіз болған жағдай туралы куәландыратын ақпараттық қауіпсіздік жүйелерін қоса алғанда, ақпараттық-коммуникациялық инфрақұрылымның немесе оның жекелеген объектілерінің жұмысында жеке немесе сериялы түрде туындайтын оқиғалар туралы мәліметтерді (бұдан әрі – ақпараттық жүйелердегі бұзушылықтар, іркілістер туралы мәліметтер) ААӨЖ арқылы беруді қамтамасыз етеді. Ақпараттық жүйелердегі бұзушылықтар, іркілістер туралы мәліметтер ақпараттық қауіпсіздік жүйелерінен немесе банктің, ұйымның ақпараттық инфрақұрылымындағы оқиғалар туралы ақпаратты нақты уақытта жинауды және талдауды жүзеге асыратын ұйымның жүйелерінен беру арқылы автоматтандырылған режимде ұсынылады.

Қазақстан Республикасы Ұлттық Банкінің құрылымына кіретін ұйымдар және дауыс беретін акцияларының елу және одан да көп пайызы Қазақстан Республикасының Ұлттық Банкіне тиесілі заңды тұлғалар үшін ақпараттық жүйелердегі бұзушылықтар, іркілістер туралы мәліметтерді Қазақстан Республикасы Ұлттық Банкінің ААӨЖ-мен ықпалдастырылған ақпараттандыру объектілері арқылы беруге рұқсат етіледі.