Қазақстан Республикасының Ұлттық Банкі

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

Национальный Банк Республики Казахстан

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

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 Республикасы
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. 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.

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» 1995 жылғы 31 тамыздағы 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.

Ескерту. 1-тармақ жаңа редакцияда – ҚР Ұлттық Банкі Басқармасының 19.11.2019 № 203 (01.01.2020 бастап қолданысқа енгізіледі); 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) қаулыларымен.

2. Талаптарда мынадай ұғымдар пайдаланылады:

1) ақпаратты штаттық тасымалдаушы – ақпараттық-коммуникациялық инфрақұрылым объектісінің құрамдас бөлігі болып табылатын ақпаратты тасымалдаушы;

2) ақпараттық жүйелердегі бұзушылықтар, іркілістер туралы мәліметтерді қоса алғанда, 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;

3) ақпараттық жүйелердегі бұзушылықтарды, іркілістерді қоса алғанда, ақпараттық қауіпсіздіктің оқыс оқиғасы (бұдан әрі – 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) банктің, ұйымның электрондық ақпараттық ресурстарын заңсыз алу, көшіру, тарату, модификациялау, жою немесе бұғаттауға арналған талаптар;

4) ақпараттық жүйенің АТ-менеджері – банктің ақпараттық жүйені ақпараттық жүйенің 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 автоматтандыратын негізгі бизнес-процестің иесі болып табылатын бөлімшесі (қызметкері);

6) ақпараттық-коммуникациялық инфрақұрылымды қорғау шегі – банктің, ұйымның ақпараттық-коммуникациялық инфрақұрылымын сыртқы ақпараттық желілерден оқшаулайтын және ақпараттық қауіпсіздік қауіпінен қорғауды қамтамасыз ететін бағдарламалық-ақпараттық құралдарының жиынтығы;

7) ақпараттық қауіпсіздік – электрондық ақпараттық ресурстардың, ақпараттық жүйелердің және ақпараттық-коммуникациялық инфрақұрылымның сыртқы және ішкі қауіптерден қорғалу жай-күйі;

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

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

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

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

12) артықшылық берілген есептік жазба – ақпараттық жүйеде жасалу, жойылу және басқа есептік жазбаларға кіру құқықтарын өзгерту артықшылықтары бар есептік жазба;

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

14) банктің, ұйымның ақпараттық активі – ақпараттың және оны сақтауға және (немесе) өңдеуге пайдаланылатын ақпараттық-коммуникациялық инфрақұрылым объектісінің жиынтығы;

15) банктің, ұйымның ақпараттық-коммуникациялық инфрақұрылымы (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;

16) бизнес-процесс – сыртқы (клиент) немесе ішкі (банктің, ұйымның қызметкері, бөлімшесі, басқа бизнес-процесс) 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 циклына 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 есептеуіш ресурстар 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 инфрақұрылым жүйелері және бөлшектері орналасатын арнайы бөлінген үй-жай;

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

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

24) кіру – ақпараттық активтерді 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 жойылған 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 дабылы, 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 арасында бірегейлендіру жүргізуге 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) ақпараттық активтерді санатқа жатқызуға қойылатын талаптар;

3) ақпараттық активтерге қол жеткізуді ұйымдастыруға қойылатын талаптар;

4) ақпараттық инфрақұрылымның қауіпсіздігін қамтамасыз етуге қойылатын талаптар;

5) ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі қызметті және қауіптерді анықтау мен талдау, шабуылдарға қарсы іс-қимыл және ақпараттық қауіпсіздік оқиғаларын зерттеу жөніндегі іс-шараларды мониторингтеуді жүзеге асыруға қойылатын талаптар;

6) ақпараттық жүйелердегі бұзылулар, іркілістер туралы мәліметтерді қоса алғанда, ақпараттық қауіпсіздік оқиғалары туралы ақпаратты талдауға қойылатын талаптар;

7) ақпаратты криптографиялық қорғау құралдарына қойылатын талаптар;

8) үшінші тұлғаларды ақпараттық активтерге жіберу кезінде ақпараттық қауіпсіздікті қамтамасыз етуге қойылатын талаптар;

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

10) ақпараттық қауіпсіздікті басқару жүйесінің процестеріне қойылатын талаптар.

2-тарау. Ақпараттық қауіпсіздікті басқару жүйесін ұйымдастыруға қойылатын талаптар

4. Банк, ұйым банктің, ұйымның ақпараттық қауіпсіздікті қамтамасыз етуге арналған жалпы басқару жүйесінің бір бөлігі болып табылатын ақпараттық қауіпсіздікті басқару жүйесін құруды және оның жұмыс істеуін қамтамасыз етеді.

5. Ақпараттық қауіпсіздікті басқару жүйесі банктің, ұйымның ақпараттық активтерінің банктің, ұйымның бизнес-процестері үшін әлеуетті залалдың ең төмен деңгейіне жол беретін қорғауын қамтамасыз етеді.

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

7. Банктің, ұйымның ақпараттық қауіпсіздікті 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.

Ұйымда осы тармақтың 4), 5), 6), 7), 8), 9) 10) және 11) тармақшаларында көрсетілген бөлімшелердің функцияларын жауапты қызметкерлердің жүзеге асыруына рұқсат етіледі.

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 жүйелерінде жасалатын, сақталатын және өңделетін ақпаратқа кіруге қойылатын талаптар және ақпараттың және оған кірудің мониторингі;

4) ақпараттық қауіпсіздікті қамтамасыз ету бойынша қызметке және қауіптерді анықтау және талдау, шабуылдарға қарсы іс-қимыл жасау және ақпараттық қауіпсіздіктің оқыс оқиғаларын тергеу бойынша іс-шараларға мониторинг 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 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.

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

12. Банк, ұйым алқалы органды құрады, оның құрамына ақпараттық қауіпсіздік бөлімшесінің, ақпараттық қауіпсіздіктің тәуекелдерін басқару бөлімшесінің, ақпараттық технологиялар бөлімшесінің өкілдері, сондай-ақ қажет болған кезде банктің, ұйымның басқа бөлімшелерінің өкілдері кіреді. Банктің, ұйымның атқарушы органының басшысы не банктің, ұйымның атқарушы органының ақпараттық қауіпсіздік бөлімшесінің қызметіне жетекшілік ететін мүшесі алқалы органның басшысы болып тағайындалады.

13. Ақпараттық қауіпсіздік бөлімшесі банк, ұйым ақпаратының құпиялылығын, 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 қолдауын қамтамасыз етеді;

4) өз құзыреті шегінде банктің немесе ұйымның ақпараттық қауіпсіздігін басқарудың, қамтамасыз етудің және бақылаудың әдістерін, құралдарын және 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 қаупсіздігін 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 шектеулерді 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-күйінің мониторингін жүзеге асырады;

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

14. 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.

15. Банк, ұйым ақпараттық қауіпсіздік бөлімшесінің мынадай функцияларын басқа бөлімшелерге:

1) банктің, ұйымның ақпараттық қауіпсіздікті қамтамасыз ету процесін автоматтандыратын бағдарламалық-техникалық құралдарын ендіру және әкімшілеуді – ақпараттық технологиялар жөніндегі бөлімшеге;

2) банк, ұйым қызметкерлерінің ақпараттық қауіпсіздік мәселелері жөнінде хабардар болуын қамтамасыз ету бойынша іс-шараларды ұйымдастыруды және жүргізуді – қызметкерлермен жұмыс жүргізу бөлімшесіне;

3) ақпараттық қауіпсіздік жай-күйінің бұзылуына байланысты оқиғаларды және оқыс оқиғаларды есепке алуды және өңдеуді – қауіпсіздік бөлімшесіне немесе ақпараттық технологиялар бөлімшесіне тәуелді емес, жеке бөлініп шыққан оқыс оқиғаларды өңдеу бөлімшесіне беру мүмкіндігін айқындайды.

16. Ақпараттық технологиялар бөлімшесі мынадай функцияларды жүзеге асырады:

1) банктің, ұйымның ақпараттық инфрақұрылымының схемаларын әзірлейді;

2) кіру рұқсатын ақпараттық технологиялар бөлімшесіне қатысты емес ақпараттық жүйелердің АТ-менеджерлері беретін мамандандырылған ақпараттық активтерді қоспағанда, банктің, ұйымның пайдаланушыларға ақпараттық активтеріне кіру рұқсатын беруді қамтамасыз етеді;

3) банктің, ұйымның жүйелік және қолданбалы бағдарламалық қамтамасыз етуді конфигурациялауды қамтамасыз етеді;

4) банктің, ұйымның ішкі құжаттарына сәйкес ақпараттық инфрақұрылымның үзіліссіз жұмыс істеуі, банктің ақпараттық жүйелері деректерінің құпиялылығы, тұтастығы және қолжетімділігі (ақпаратты резервтеуді және (немесе) мұрағаттауды 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. Қауіпсіздік бөлімшесі мынадай функцияларды жүзеге асырады:

1) банкте, ұйымда жеке басының қауіпсіздігі және техникалық қауіпсіздік шараларын іске асырады, оның ішінде кіру және объектішілік режимін ұйымдастырады;

2) банктің, ұйымның қызметкерлерін жұмысқа қабылдаған және жұмыстан босатқан кезде ақпараттық қауіпсіздік қауіптерінің туындауы тәуекелдерін барынша азайтуға бағытталған алдын алу іс-шараларын жүргізеді.

18. Қызметкерлермен жұмыс жүргізу бөлімшесі мынадай функцияларды жүзеге асырады:

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

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

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

20. Комплаенс-бақылау бөлімшесі банктің, ұйымның заң бөлімшесімен бірлесе отырып Талаптардың 10-тармағында көзделген қорғалатын ақпараттың тізбесіне енгізуге жататын ақпараттың барлық түрін айқындайды.

21. 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.

22. 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 арналған тәуекелдерді басқару және ішкі бақылау жүйесін қалыптастыру қағидаларында көзделген функцияларды жүзеге асырады.

Ескерту. 22-тармақ жаңа редакцияда – ҚР Қаржы нарығын реттеу және дамыту агенттігі Басқармасының 03.08.2020 № 72 (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) қаулысымен.

23. 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.

24. Ақпараттық жүйеледің немесе шағын жүйелердің бизнес-иелері:

1) өнімдерді және қызметтерді құру, ендіру, модификациялау, клиенттерге беру кезінде ақпараттық қауіпсіздік талаптарының сақталуы үшін жауап береді;

2) ақпараттық жүйелерге кіру матрицаларының жаңартылуын қалыптастырады және қолдайды.

25. 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 ақпараттық активтермен жұмыс істеу кезіндегі барлық күдікті жағдайлар мен бұзушылықтар туралы хабарлайды.

26. 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.

27. 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 – ақпарат) береді.

28. Ақпарат еркін нысандағы мәтін түрінде жасалады және ұсынылатын деректердің құпиялылығы мен түзетілмеуін қамтамасыз ететін криптографиялық қорғау құралдарымен ақпаратты кепілді жеткізудің тасымалдау жүйесін пайдалана отырып, уәкілетті органға ұсынылады.

29. Ақпаратта мыналар:

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

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.

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

3-тарау. Ақпараттық активтерді санатқа жатқызуға қойылатын талаптар

31. Банк, ұйым ақпараттық активтерді санатқа жатқызуды оларды оларда сақталатын және өңделетін ақпараттың маңыздылығының ең жоғары деңгейінің негізінде маңызды және маңызды емеске бөлу арқылы жүзеге асырады.

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

33. Банк, ұйым Талаптарға сәйкес маңызды санатына жатқызылған ақпараттық активтердің ақпараттық қауіпсіздігін қамтамасыз етеді.

34. Банк, ұйым маңызды емес санатына жатқызылған ақпараттық активтерді қорғау әдістері мен құралдарын дербес айқындайды.

35. Қорғалатын ақпаратты анықтау кезінде банк, ұйым оны ықтимал зиянды бағалау негізінде маңызды және маңызды емеске бөлу арқылы банктің, ұйымның ақпаратты санатқа жатқызу процесін реттейтін ішкі құжатында айқындалған тәртіппен оны санатқа жатқызады.

4-тарау. Ақпараттық активтерге кіруді ұйымдастыруға қойылатын талаптар

36. Банктің, ұйымның ақпараттық активтеріне нақты кіруді ұсыну банктің ішкі құжаттарына сәйкес жүзеге асырылады.

37. Қызметкерлерге ақпаратқа кіру олардың функционалдық міндеттерін орындау үшін қажетті көлемде беріледі.

38. Банктің, ұйымның маңызды ақпараттық активтер санатына жатқызылған ақпараттық жүйелерге (бұдан әрі – маңызды ақпараттық жүйелер) кіруді ұсыну ақпараттық жүйелерді пайдаланушылардың кіру құқықтарының олардың функционалдық міндеттеріне сәйкестігін қамтамасыз ету үшін рольдерді

қалыптастыру және енгізу арқылы жүргізіледі. Осындай рольдердің жиынтығы ақпараттық жүйеге кіру матрицасы болып табылады, банк немесе ұйым оны электрондық нысанда немесе қағаз тасымалдағышта қалыптастырады.

39. Банктің, ұйымның ақпараттық жүйелеріне кіру матрицаларын құру және пайдалану процесі Талаптардың 11-тарауына сәйкес банктің, ұйымның ақпараттық жүйелерге кіруді басқару процесін реттейтін ішкі құжатында айқындалады.

40. 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:

«есептік жазба (сәйкестендіруші) – пароль» деген жұпты енгізу немесе екі факторлық бірегейлендіру тәсілдерін қолдану арқылы;

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

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

42. Технологиялық есептік жазбаларды пайдалануға және жаңартылуына дербес жауапкершілік атқаратын адамдарды көрсете отырып, әрбір ақпараттық жүйе үшін ақпараттық қауіпсіздік бөлімшесі басшысының келісімімен ақпараттық технологиялар бөлімшесінің басшысы бекітетін осындай есептік жазбалардың тізбесіне сәйкес технологиялық есептік жазбаларды пайдалануға жол беріледі.

43. Банктің, ұйымның ақпараттық жүйелерінде Талаптардың 11-тарауына сәйкес әзірленген банктің, ұйымның ішкі құжатында айқындалатын есептік жазбаларды және парольдерді басқару, сондай-ақ пайдаланушылардың есептік жазбаларын оқшаулау бойынша функциялар пайдаланылады.

5-тарау. Ақпараттық инфрақұрылымның қауіпсіздігін қамтамасыз етуге қойылатын талаптар

44. Банктің, ұйымның ақпараттық технологиялар бөлімшесі банктің мыналарды:

1) элементтерінің нақты орналасқан жерін көрсете отырып, ақпараттық инфрақұрылымының жалпы схемасын;

2) ақпараттық инфрақұрылым тораптарының (телекоммуникациялық құрылғылардың, серверлердің және онда орналасқан операциялық жүйелердің, дерекқорын және қосымшаларды басқару жүйелерінің) жауапты әкімшілерінің тізбесін айқындайтын ішкі құжаттарын әзірлейді.

45. Ақпараттық жүйенің АТ-менеджері ақпараттық қауіпсіздік бөлімшесінің келісімімен банктің, ұйымның мыналардың:

1) операциялық жүйелердің;

2) дерекқорын басқару жүйелерінің;

3) телекоммуникациялық құрылғылардың;

4) ақпараттық жүйелердің;

5) ақпараттық инфрақұрылымның, жұмыс станцияларының және мобильді құрылғылар тораптарының және түпкі нүктелерінің үлгі теңшеулерін айқындайтын ішкі құжаттарын әзірлейді.

46. Ақпараттық қауіпсіздік бөлімшесі маңызды ақпараттық жүйелерде жүйелік және конфигурациялық файлдардың, сондай-ақ аудиторлық із журналдарының қауіпсіздігі мен тұтастығы теңшеулерінің өзгеруін бақылау жүйелерін ұйымдастыруды қамтамасыз етеді.

47. 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.

48. Әрбір ақпараттық жүйенің немесе шағын жүйенің бизнес-иесі анықталады. Инфрақұрылымдық ақпараттық жүйелер үшін ақпараттық технологиялар бөлімшесі бизнес-иесі болып табылады.

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

50. Банктің, ұйымның ақпараттық жүйелерінің қауіпсізідігін оларды әзірлеу және пайдалану барысында қамтамасыз ету Талаптардың 11-тарауына сәйкес жүзеге асырылады.

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

Ақпаратты резервтік көшіру, сақтау, қалпына келтіру тәртібі мен кезеңділігі, резервтік көшірмелерден маңызды ақпараттық жүйелердің жұмыс істеу қабілетін қалпына келтіруді тестілеуден өткізу кезеңділігі банктің, ұйымның ішкі құжатында айқындалады.

52. Банк, ұйым Талаптардың 11-тарауына сәйкес әзірленген банктің, ұйымның ішкі құжатында белгіленген тәртіппен ақпараттық инфрақұрылымды вирусқа қарсы қорғауды қамтамасыз етеді.

53. Банктің, ұйымның деректерді өңдеу орталықтарының нақты қауіпсіздігін қамтамасыз ету тәртібі Талаптардың 11-тарауына сәйкес әзірленген банктің, ұйымның ішкі құжатында айқындалады.

54. Банк, ұйым қызметкерлерінің жұмыс станцияларына және корпоративтік мобильді құрылғыларына функционалды міндеттерді орындауға қажетті бағдарламалық қамтамасыз ету орнатылады.

55. Пайдалануға енгізу алдында банкте, ұйымда бағдарламалық қамтамасыз ету оның банктің, ұйымның ақпараттық қауіпсіздік талаптарына сәйкестігі бойынша ақпараттық қауіпсіздік бөлімшесінде тексеруден өтеді.

56. Банк, ұйым банкте, ұйымда пайдалануға рұқсат етілетін бағдарламалық қамтамасыз етудің және жабдықтың тізбесін айқындайды. Бағдарламалық қамтамасыз ету Талаптардың 55-тармағына сәйкес тексеру жүргізілгеннен кейін тізбеге енгізіледі.

57. Банктің, ұйымның ішкі құжатында Талаптардың 11-тарауына сәйкес банктің, ұйымның жұмыс станцияларының және мобильді құрылғыларының, сондай-ақ ақпарат тасымалдағыштарының және желілік ресурстарының қорғауын қамтамасыз ететін ұйымдастыру және техникалық шаралар айқындалады.

6-тарау. Ақпараттық қауіпсіздікті қамтамасыз ету бойынша қызметтің мониторингіне қойылатын талаптар және қауіптерді анықтау және талдау, шабуылдарға қарсы іс-қимыл жасау және ақпараттық қауіпсіздіктің оқыс оқиғаларын тергеу бойынша іс-шаралар

58. Банк, ұйым ақпараттық қауіпсіздікті қамтамасыз ету бойынша қызметтің және қауіптерді анықтау және талдау, шабуылдарға қарсы іс-қимыл жасау және ақпараттық қауіпсіздіктің оқыс оқиғаларын тергеу бойынша іс-шаралардың мониторингін жүргізеді.

59. Банк, ұйым ақпараттық қауіпсіздік оқиғаларына мониторинг жүргізеді және ақпараттық қауіпсіздіктің оқыс оқиғаларын басқару.

Банктің, ұйымның мониторингті жүзеге асыратын бөлімшесіне қосымша бақылаулар енгізуге, ақпараттық қауіпсіздіктің оқыс оқиғасы анықталған жағдайда бизнес-процесті ішінара немесе толық тоқтатуға өкілеттіктер беріледі.

60. Банк, ұйым мониторингке жататын ақпараттық қауіпсіздік оқиғаларының тізбесін, оқиғалардың көздерін, кезеңділігін, мониторинг жүргізу қағидаларын және олардың әдістерін айқындайды.

61. Мониторингке жататын ақпараттық қауіпсіздіктің оқыс оқиғаларының, оқиғалар көздерінің, кезеңділігінің тізбелері, мониторинг қағидалары және олардың әдістері бар статистиканы және мониторингтің тиімділігін ескере отырып, кемінде жылына бір рет қайта қаралады.

62. Банк, ұйым ақпараттық қауіпсіздік оқиғасын ақпараттық қауіпсіздіктің оқыс оқиғаларына жатқызу тәртібін айқындайды.

63. Ақпараттық қауіпсіздіктің оқыс оқиғаларын басқару тәртібі банктің, ұйымның Талаптардың 11-тарауына сәйкес әзірленген ішкі құжатында айқындалады.

7-тарау. Ақпараттық жүйелердегі бұзушылықтар, іркілістер туралы мәліметтерді қоса алғанда, ақпараттық қауіпсіздіктің оқыс оқиғалары туралы ақпаратты талдау жүргізуге қойылатын талаптар

64. Ақпараттық қауіпсіздіктің оқыс оқиғасын өңдеу нәтижесі бойынша ақпараттық қауіпсіздіктің оқыс оқиғасының туындау себептеріне, оның тетігіне және салдарына жан-жақты талдау жүргізіледі. Ақпараттық қауіпсіздіктің оқыс оқиғасына қатысты бағдарламалық-техникалық құралдардан техникалық деректерді жинау кезінде жинақталған деректердің сақталуы және өзгермеуі қамтамасыз етіледі.

65. Талдау нәтижесі бойынша қорытынды еркін нысанда дайындалады, онда ақпараттық қауіпсіздіктің оқыс оқиғасы бойынша барлық ақпарат, сондай-ақ ақпараттық қауіпсіздіктің қайталанған оқыс оқиғасының болу ықтималын және ықтимал залалды төмендету мақсатында түзету шараларын қабылдау бойынша ұсыныстар көрсетіледі.

66. Туындау ықтималы жоғары және өте қысқа мерзімде төмендеуі мүмкін емес ақпараттық қауіпсіздіктің оқыс оқиғалары үшін осындай ақпараттық қауіпсіздіктің оқыс оқиғаларын өңдеудің алгоритімін, оқыс оқиғаны және оның салдарын оқшаулау бойынша үлгі жедел шараларын, ақпараттық қауіпсіздіктің оқыс оқиғаларын өңдеу әдістерін сипаттайтын құжаттар жасалады.

67. Ақпараттық қауіпсіздіктің оқыс оқиғаларын талдау нәтижелерін, сондай-ақ ақпараттық қауіпсіздіктің оқыс оқиғаларының туындау ықтималын және оларды ықтимал залалын барынша төмендету бойынша ұсынымдар жыл сайын алқалы органның қарауына енгізіледі және болашақта ақпараттық қауіпсіздіктің тәуекелдерін бағалау, ақпараттық қауіпсіздікті қамтамасыз ету әдістері мен құралдарын түзету, бизнес-процестерді өзгерту үшін пайдаланылады.

8-тарау. Ақпаратты криптографиялық қорғау құралдарына қойылатын талаптар

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

69. Банк, ұйым Талаптардың 11-тарауына сәйкес ақпаратты криптографиялық қорғау құралдарын пайдалану тәртібін реттейтін ішкі құжатты, сондай-ақ пайдалануын, олардағы криптографиялық алгоритмдерін, ақпараттық жүйенің атауын, ақпаратты криптографиялық қорғау құралдарын пайдаланатын ақпараттық жүйенің иесін көрсете отырып, қолданылатын ақпаратты криптографиялық қорғау құралдарының тізбесін бекітеді.

9-тарау. Үшінші тұлғалардың ақпараттық активтеріне кіруі кезінде ақпараттық қауіпсіздікті қамтамасыз етуге қойылатын талаптар

70. Банктің, ұйымның ішкі құжатында банктің, ұйымның қызметкері болып табылмайтын үшінші тұлғалардың (бұдан әрі – үшінші тұлғалар) ақпараттық активтерге кіру кезінде ақпараттық қауіпсіздікке қойылатын талаптар көзделеді.

71. Үшінші тұлғалардың банктің, ұйымның ақпараттық активтеріне кіру рұқсаты Қазақстан Республикасының заңнамасында көзделген жағдайларды қоспағанда, ақпараттық қауіпсіздік талаптарын сақтау туралы келісім негізінде жұмыстар жүргізуге қажетті кезеңге және көлемде беріледі. Үшінші тұлғалармен жасалатын ақпараттық қауіпсіздік талаптарын сақтау туралы келісімдерде конфиденциалдылық туралы ережелер, ақпараттық қауіпсіздіктің бұзылуы салдарынан туындаған шығынды қайтару туралы, сондай-ақ үшінші тұлғалардың араласуы салдарынан болған ақпараттық жүйелердің жұмысындағы іркілістер мен олардың қауіпсіздігін бұзуы салдарынан туындаған зиянды өтеу туралы талаптар қамтылады.

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

73. Жүргізілген тәуекелді бағалаудың негізінде үшінші тұлғалардың қызметін бақылау бойынша 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) ақпараттық активтерге кіру сессиясын арнайы бағдарламалық-техникалық кешендерге жазу.

74. Үшінші тұлғаларға банктің, ұйымның ақпараттық активтерінің бір бөлігін беру (мысалы, серверлік қуаттарды тысқары деректерді өңдеу орталықтарына орналастыру, бұлттық сервистерді пайдалану) жағдайында ақпараттық қауіпсіздікті қамтамасыз етудің мынадай шаралары қабылданады:

1) үшінші тұлғалармен жасалған тиісті шартта ақпараттық қауіпсіздікті және ақпараттық жүйелердің жұмыс істеу қабілетінің бұзылуы салдарынан туындаған шығынды қайтару туралы талаптарды көрсету;

2) Қазақстан Республикасының азаматтық, банктік заңнамасының, Қазақстан Республикасының дербес деректер және оларды қорғау туралы заңнамасына сәйкес үшінші тарапқа беруге болмайтын ақпаратқа үшінші тұлғалардың кіру мүмкіндігін болдырмау. Бұлттық серверлерді пайдалану кезінде бұл мақсаттар үшін ақпараттың банк тарапына ашылуымен ақпаратты шифрланған күйінде сақтау әдісі қолданылады. Бұл ретте шифрлау кілттері банкте, ұйымда сақталады.

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

75. Ақпараттық қауіпсіздіктің жай-күйі құрылымдық бөлімшелердің қызметін 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.

76. Ақпараттық қауіпсіздік бөлімшесі тексерудің нәтижесі бойынша тексеру материалдарын тіркей отырып, есеп жасайды, оны тексерілетін бөлімшеге мәлімет үшін жібереді.

11-тарау Ақпараттық қауіпсіздікті басқару жүйесінің процестеріне қойылатын талаптар

1-параграф. Ақпараттық жүйелерге кіруді ұйымдастыру процесіне қойылатын талаптар

77. Ақпараттық жүйеге кіру матрицасын құру процесі мынадай кезеңдерден тұрады:

1) процесті бастама ету – банктің, ұйымның ақпараттық жүйесіне кіру матрицасын құруға бастамашы ақпараттық жүйенің бизнес-иесі болып табылады;

2) бизнес-процестің иесі бар автоматтандырылған бақылаудан айналып өтуге мүмкіндік беретін қайшы келетін кіру құқықтарының берілуін болдырмау бойынша шараларды ескере отырып, әрбір роль бойынша ақпараттық жүйеде автоматтандырылған функцияларды сипаттайды және формалдандырады;

3) нысандандырылған функциялар ақпараттық жүйенің бизнес-иесімен келісіледі;

4) ақпараттық жүйенің бизнес-иесі ақпараттық жүйеде рольдерді әзірлеуге техникалық тапсырманы дайындайды;

5) ақпараттық жүйеге қолдау көрсетуге жауапты бөлімше ақпараттық жүйеде рольдердің іске асырылуын әзірлейді;

6) ақпараттық жүйенің бизнес-иесі және басқа да мүдделі бөлімшелер құрылған рольдерді тестілеуден өткізеді;

7) ақпараттық жүйеге қолдау көрсетуге жауапты бөлімше ақпараттық жүйеге рольдерді енгізеді.

78. Ақпараттық жүйеге кіру матрицасына өзгерістер мен толықтыруларды енгізу Талаптардың 77-тармағында белгіленген тәртіппен автоматтандырылатын бизнес-процеске қатысушының бастамасы бойынша жүзеге асырылады.

79. Банктің, ұйымның маңызды ақпараттық жүйесіне кіруді басқарудың шағын жүйесі мыналарды:

1) жаңа пайдаланушыны қосымша деңгейінде тіркеу мүмкіндігін;

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

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

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

5) ақпараттық жүйелерге кіруге жеке, топтық, аумақтық шектеулерді қолдауды;

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

7) бір аппараттық құралдан (компьютерден) әртүрлі есептік деректер арқылы бір ақпараттық жүйеге бірмезгілде кіруді оқшаулау мүмкіндігін;

8) аудиторлық із жүргізуді қамтамасыз етеді.

80. Банктің, ұйымның маңызды ақпараттық жүйесінің деректеріне кіруді басқарудың шағын жүйесіне мыналар:

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

2) белгіленген пайдаланушыларға ақпараттық жүйенің деректеріне қосымшасыз кіруді беру кіреді. Осындай пайдаланушылардың тізбесін банктің, ұйымның атқарушы органының ақпараттық қауіпсіздік бөлімшесіне жетекшілік ететін мүшесі бекітеді.

81. Қызметкердің функционалдық міндеттері өзгерген кезде қолда бар кіру құқықтары ажыратылады және оның жаңа функционалдық міндеттеріне сәйкес жаңа кіру құқықтары тағайындалады. Қызметкер жұмыстан босатылған кезде оның барлық ақпараттық жүйелерге кіру құқықтары ажыратылады. Қызметкер жұмыс орнында ұзақ уақыт болмаған кезде оның ақпараттық жүйесіне кіру банктің, ұйымның ішкі құжатында белгіленген тәртіппен оқшауланады.

82. Ақпараттық қауіпсіздік бөлімшесі ақпараттық қауіпсіздікті қамтамасыз ету бойынша қызметке мониторинг жүргізу шеңберінде ақпараттық жүйелерге кіру құқықтарының кіру матрицаларына сәйкестігін тексеру, сондай-ақ жұмыстан босатылған қызметкерлердің кіру құқықтарының ажыратылуын және ұзақ мерзімде жұмыс орнында болмаған қызметкерлердің кіруін оқшаулауды бақылау жүргізеді.

83. Банк, ұйым ақпараттық жүйеге кіруді басқару тәртібін реттейтін банктің, ұйымның ішкі құжатында белгіленген тәртіппен ақпараттық жүйеге кіру матрицасын жаңартады. Ақпараттық жүйелердің бизнес-иесі ақпараттық жүйелерге кіру құқықтарын қайта қарауды мүдделі бөлімшелерді тарта отырып жүргізеді.

84. Осы тараудың бір немесе бірнеше талабын іске асыруға техникалық мүмкіндіктер болмаған кезде банкте, ұйымда оның орнын басатын шаралар ретінде ақпараттық қауіпсіздіктің тәуекелдерін ішінара немесе толық болдырмау бойынша қосымша техникалық және ұйымдастыру шараларын қолданылады.

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

85. Банктің, ұйымның ақпараттық жүйелерінде пайдаланушылардың парольдерін және есептік жазбаларды 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 (пайдаланушыны бұдан ертерек ескерту мүмкін). 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 жүйелі түрде 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 бірегейлендіру деректерін енгізген кезде ғана оқшалаусыздандыру мүмкіндігімен жұмыс станциясын оқшаулайды.

86. Талаптардың 85-тармағының талаптары мынадай:

1) ақпараттық жүйе Талаптардың 85-тармағының талаптарына сәйкес келетін ақпараттық жүйемен бірегейлендіру бөлігінде ықпалдастырылған;

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

87. Банк, ұйым есептік жазбаларды және парольдерді басқару процесін реттейтін ішкі құжатты әзірлейді, онда мыналар:

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

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

3) есептік жазбаларды өзгертуге немесе жоюға өтінімдерді беру тәртібі;

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

5) ақпараттық жүйелерді басқарушыларды және банктің, ұйымның өзге де қызметкерлерін қоса алғанда, үшінші тұлғаларға парольдерді беруге тыйым салу;

6) ақпараттық жүйелерде бөтен есептік жазбалар арқылы жұмыс істеуге тыйым салу (қызметтің үздіксіз жұмыс істеуін қамтамасыз ету мақсатында ақпараттық қауіпсіздік бөлімшесімен келісім бойынша көрсетілген уақыт аралығында бөтен есептік жазбаларды пайдалануға жол беріледі, бұл ретте пайдаланушыны нақты сәйкестендіру қамтамасыз етіледі).

3-параграф. Ақпарат қауіпсіздігін қамтамасыз ету процесіне қойылатын талаптар

88. Интернетті және электрондық поштаны пайдаланған кезде ақпаратты қорғау тәртібі мынадай әдістердің кез келгенін пайдалана отырып, бірақ олармен шектелмей банктің, ұйымның ішкі құжатында айқындалады:

1) ұйымдастырушылық: банктің, ұйымның ішкі құжаттарында белгіленген шектеулер, қызметкерлердің хабардар болуын қамтамасыз ету, Интернет

желісіне, жедел хабарламалар қызметіне, бұлттық сервистерге, IP-телефонияға және сыртқы электрондық почтаға кіру рұқсаты бар қызметкерлердің санын азайту;

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 мерзімі банктің, ұйымның ішкі құжатында айқындалады, 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.

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

1) ұйымдастырушылық: банктің, ұйымның ішкі құжаттарында белгіленген 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.

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

1) ұйымдастырушылық: банктің, ұйымның ішкі құжаттарында белгіленген шектеулер, қызметкерлердің хабардар болуын қамтамасыз ету, 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.

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

1) ұйымдастырушылық: банктің, ұйымның ішкі құжаттарында белгіленген шектеулер, 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).

92. 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

93. Банк, ұйым ақпараттық 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 қолдайды.

94. Банктің, ұйымның қорғау периметрінен шығатын қалалық телефон желісімен қосылғыштарды қоспағанда, телекоммуникациялық қосылғыштар, сондай-ақ аумақтық қашықты желілер және маңызды ақпаратты беру үшін пайдаланылатын банктің, ұйымның құрылғылары арасындағы қосылғыштар шифрленуі тиіс.

95. Сымсыз қосылғыштарды пайдалану кезінде шифрлеу сымсыз қосылғыш хаттамасында ұсынылатын шифрлеу әдісінен бөлек әдіспен жүргізіледі.

96. Қосылуды шифрлеудің орнына берілетін ақпаратты шифрлеуге рұқсат беріледі.

97. Банктің, ұйымның қорғау периметрінде ақпараттық инфрақұрылымға кіруді шектеу үшін желі аралық экрандар орнатылады.

98. Желі аралық экрандар орнатылған кіру қағидалары банктің, ұйымның бизнес-процестері жұмыс істеп тұру үшін қажетті қосылғыштарға ғана рұқсат беруге теңшеледі. Көрсетілген қағидалар ақпараттық қауіпсіздік бөлімшесімен келісіледі. Қорғау периметріне жасалған шабуылдарды анықтау және көрсету үшін басып кіруді анықтау және алдын алу құралдары пайдаланылады.

99. 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 типтегі шабуылдан қорғау бойынша тиісті функционалы бар арнайы жүйелерді орнату және басқа тәсілдер) пайдаланылады.

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

101. 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.

102. Қорғау периметрінің қауіпсіздігін қамтамасыз ету құралының конфигурациясы өндірушілердің ұсынымдарын ескере отырып орындалады және

банктің, ұйымның ішкі құжаттарында айқындалған кезеңділікпен қайта қаралады. Алдын ала белгіленген есептік жазбаларға парольдер міндетті тәртіпте өзгертіледі. Осындай есептік жазбаларға қажетті болмағанда, олар бұғатталады немесе жойылады.

103. Банктің, ұйымның ішкі құжаттарында айқындалған кезеңділікпен банктің, ұйымның ақпараттық инфрақұрылымына рұқсатсыз кіруге осы салада тәуелсіз сыртқы сарапшылар тестілеу жүргізеді. Осы тестілеудің шегінде, жүйелік және қолданбалы бағдарламалық қамтамасыз етудің 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

104. Ақпараттық жүйенің АТ-менеджері ақпараттық инфрақұрылымның барлық тораптарын эталондық дереккөз уақыты бойынша орталықтан үйлестіреді.

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

1) клиенттік (пайдаланушылық);

2) серверлік (инфрақұрылымдық);

3) әзірлемелер (бар болса);

4) тестілік бөлуді қамтамасыз етеді.

106. Банк, ұйым ақпараттық инфрақұрылымды қорғау мақсатында банктің, ұйымның ақпараттық инфрақұрылымындағы шамадан тыс белсенділікті анықтауға мүмкіндік беретін әдістер мен жүйелерді қолданады.

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

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

108. Бір серверде немесе гипервизорда бірнеше ақпараттық жүйелерді орналастырған кезде, аталған серверде немесе гипервизорда орналастырылған барынша өзекті ақпараттық жүйеге сәйкес келетін деңгейде қорғау қамтамасыз етіледі.

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

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

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

111. Қорғалатын ақпарат әзірлеу және тестілеу ортасында пайдаланылған жағдайда оларды қорғау жөнінде тиісті шаралар қолданылуға тиіс.

112. 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.

113. 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.

114. 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.

115. Бастапқы эталондық кодтар (болған жағдайда) және ақпараттық жүйелердің қалыпқа келтіру үшін қолайлы түрдегі орындалатын модульдері сақталатын бағдарламалық қамтамасыз етудің қорғалған депозитарийі жүргізіледі.

116. Банктің, ұйымның ақпараттық жүйелері техникалық қолдаумен қамтамасыз етіледі, оның құрамына тиісті ақпараттық жүйенің жаңарту, оның ішінде қауіпсіздікті жаңарту ұсыну бойынша қызметтер кіреді.

7-параграф. Ақпараттық жүйелердегі бұзушылықтар, іркілістер туралы мәліметтерді қоса алғанда, ақпараттық қауіпсіздіктің оқыс оқиғалары туралы ақпаратты жинақтау, шоғырландыру және сақтау процесіне қойылатын талаптар

117. Ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі қызметті мониторингтеу барысында алынған ақпараттық қауіпсіздік оқиғалары туралы ақпарат шоғырландырылуға, жүйелендірілуге және сақталуға тиіс.

118. Ақпараттық қауіпсіздіктің оқыс оқиғалары туралы ақпаратты сақтау мерзімі кемінде 5 (бес) жылды құрайды.

119. Егер банк, ұйым жұмыстан тыс уақытта ақпараттық қауіпсіздіктің оқыс оқиғаларының жекелеген көздерін мониторингтеу қажеттілігін айқындаса, тәулік бойы мониторингтеу қызметі құрылады.

120. Банк, ұйым банктің, ұйымның басшы қызметкерлеріне және бөлімшелеріне ақпараттық қауіпсіздіктің орын алған оқыс оқиғалары туарлы хабарлау тәртібін айқындайды.

121. Банк, ұйым ақпараттық қауіпсіздіктің оқыс оқиғаларын, оның себептері мен салдарын жою үшін кезек күттірмес шаралар қабылдау тәртібін айқындайды.

122. Банкте, ұйымда ақпараттық қауіпсіздіктің оқыс оқиғасы, қабылданған шаралар және ұсынылған түзету шаралары туралы барлық ақпаратты қағаз тасымалдағышта немесе электронды түрде көрсете отырып ақпараттық қауіпсіздіктің оқыс оқиғаларын есепке алу журналын жүргізеді.

8-параграф. Қызметкерлермен жұмыс жүргізу процесіне қойылатын талаптар

123. Банктің, ұйымның жаңа қызметкері жұмысқа қабылданған кезде қорғалатын ақпаратты жария етпеу туралы міндеттемеге қол қояды. Міндеттеме қызметкердің жеке ісіне қоса беріледі.

124. 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 қоса беріледі.

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

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

127. 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 тестілеу жүргізу жоспарына сәйкес ақпараттық қауіпсіздік жөніндегі ішкі құжаттардың талаптарын білуіне тест жүргізу;

3) банк, ұйым айқындаған өзге әдістер.

128. 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.

129. 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 екі жылда кемінде бір реттен).

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

1) құжаттарды қабылдау-өткізу;

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

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

4) ақпараттық жүйелерде есептік жазбаларды оқшаулау немесе жою.

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

131. Ақпараттық жүйелерде аудиторлық із жүргізу функциясы бар, ол мыналарды көрсетеді:

1) ақпараттық жүйедегі қосылғыштарды ойдағыдай, сол сияқты ойдағыдай емес орнату, сәйкестендіру, бірегейлендіру және авторизациялау оқиғасы;

2) қауіпсіздікті іске қосуды түрлендіру оқиғасы;

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.

132. 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 (CREATE, INSERT, UPDATE, DELETE және басқалары);

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

133. Аудиторлық ізді сақтау мерзімі жедел кірумен кемінде 3 (үш) айды және архивтік кірумен кемінде 1 (бір) жылды құрайды. Аудиторлық ізді оқиғаларды сақтаудың, өңдеудің және талдаудың мамандандырылған ақпараттық жүйесіндегі бірнеше ақпараттық жүйелерде жинақтап сақтауға рұқсат беріледі.

134. Банк, ұйым аудиторлық іздің ұйымдастыру, сол сияқты техникалық деңгейдегі тұрақтылығын қамтамасыз етеді. Ақпараттық жүйелердің басқарушыларына аудиторлық із журналдарын архивке ауыстыруға ғана кіруге рұқсат беріледі.

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

135. Банк, ұйым лицензиялық вирусқа қарсы бағдарламалық қамтамасыз етуді немесе жұмыс стансаларында, мобилді құрылғыларда, сол сияқты серверлерде бағдарламалық ортаның тұтастығы мен тұрақтылығын қамтамасыз ететін жүйелерді пайдаланады.

136. 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 сканирлеу;

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

5) басқарудың және мониторинг жүргізудің орталықтандырылған консолийінің 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 (жүктемені теңестіру, орталықтандырылған қондырғы және гипервизор деңгейінде тексеру және басқа функциялар) 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.

137. 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 консолийінің 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.

138. Вирусқа қарсы бағдарламалық қамтамасыз етуді таңдауды ақпараттық технологиялар бөлімшесі ақпараттық қауіпсіздік бөлімшесінің міндетті қатысуымен банктің, ұйымның ішкі құжаттарымен белгіленген тәртіпте жүргізеді.

Банктің, ұйымның ішкі құжаттары вирусқа қарсы қорғауды қамтамасыз ету процесіне тартылған жауапты құрылымдық бөлімшелерді беліглейді (вирусқа қарсы қорғауды бағдарламалық қамтамасыз етуді және вирустық шабуылдарға ден қоюды орнату, сүйемелдеу, мониторингі).

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

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

140. Ақпараттық технологиялар бөлімшесі ақпараттық жүйелерді жаңартуларды қадағалап отырады және ақпараттық қауіпсіздік бөлімшесінің келісімі бойынша ақпараттық жүйелерді жаңартуларды басқару тәртібін белгілейді.

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

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

143. Ақпараттық қауіпсіздік бөлімшесі ақпараттық жүйелерді мамандандырылған бағдарламалық қамтамасыз етуді қолданумен осалдығы тұрғысынан сканирлеу (бұдан әрі – сканирлеу) жүргізеді. Сканирлеу әрбір ақпараттық жүйе үшін жылына кемінде бір рет жоспарлы негізде жүргізілуі тиіс. Сканирлеуді банктің, ұйымның қызметкерлері және (немесе) сырттан мамандандырылған компаниялар жүргізе алады. Сканирлеудің нәтижелері анықталған осалдықтарды жою бойынша түзету және алдын алу шараларының қажеттілігі жөнінде ұсынымдарды көрсетумен, ақпараттық қауіпсіздіктің жағдайы туралы есеп түрінде қалыптастырылады.

144. Банк, ұйым анықталған осалдықтарды жою бойынша қажетті шаралар қабылдайды.

Осалдықтарды жою бойынша жұмыстар аяқталысымен бұрын анықталған осалдықтардың жойылғанын растайтын ақпараттық жүйені қайтадан сканерлеу жүргізіледі.

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

145. Ақпараттық технологиялар бөлімшесі ақпараттық қауіпсіздік бөлімшесінің келісімімен банктің, ұйымның ақпаратты криптографиялық қорғау құралдарын пайдалануды реттейтін ішкі құжатын әзірлейді, оған ең кемі мыналар кіреді:

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

2) ақпаратты криптографиялық қорғау құралдарын пайдалану саласы;

3) ақпаратты криптографиялық қорғау құралдарын күйге келтірудің сипаттамасы;

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

5) негізгі ақпарат әшкереленген кездегі іс-әрекет;

6) ақпаратты криптографиялық қорғау құралдарын соңғы пайдаланушылардың пайдалану тәртібі;

7) ақпаратты криптографиялық қорғау құралдарына әкімшілендіруге және негізгі ақпаратты басқаруға жіберілген тұлғалар тізбесі;

8) пайдаланушылар ретінде ақпаратты криптографиялық қорғау құралдарымен жұмысқа жіберілген тұлғалар тізбесі.

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

146. 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.

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

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

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

150. 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.

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

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

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

14-параграф. Жұмыс станциялары мен мобильдік құрылғыларды қорғауды қамтамасыз ету процесіне қойылатын талаптар

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

155. Жергілікті әкімшінің құқықтары немесе ұқсас құқықтар пайдаланушылар орындайтын функцияларды автоматтандыратын бағдарламалық қамтамасыз етулердің жұмыс істеуіне қажет болған жағдайларды қоспағанда, пайдаланушыларға осындай құқықтарды беруге тыйым салынады.

156. Ерекше жағдайларда пайдаланушылардың жекелеген топтарына бағдарламалық қамтамасыз етуді және жабдықты өз бетінше орнату және теңшеу құқығы беріледі. Пайдаланушылардың бұл топтарына жергілікті әкімшінің құқықтары немесе ұқсас құқықтар беріледі.

157. Талаптардың 155 және 156-тармақтарында көрсетілген пайдаланушылардың тізбесін ақпараттық қауіпсіздік бөлімшесімен келісу бойынша ақпараттық технологиялар бөлімшесінің басшысы қалыптастырады, жаңартады және бекітеді. Пайдаланушыларға қосымша құқықтар берілген жағдайда Талаптардың 155 және 156-тармақтарына сәйкес ақпараттық қауіпсіздік бөлімшесі олардың пайдаланылуын бақылайды.

158. Банктің, ұйымның жұмыс станцияларын және корпоративтік желісіндегі мобильдік құрылғыларды есепке алу жүйесі осы жұмыс станциясының орналасқан орнын немесе мобильдік құрылғының тиесілігін нақты сәйкестендіруге мүмкіндік береді.

159. Мобильдік құрылғыларды банктің, ұйымның ақпараттық жүйелеріне қосқан жағдайда, банкті, ұйымды қорғау периметрінің шектері салдарынан аталған құрылғыларды ақпараттық жүйелерге қорғалған кіруді қамтамасыз ететін арнайы бағдарламалық қамтамасыз ету (байланыс арнасын шифрлеу, екі факторлы бірдейлендіруді қамтамасыз ету, деректерді құрылғылардан қашықтан жою) орналастырылады.

160. Банктің, ұйымның ақпараттық активтерін өңдеу үшін банк, ұйым қызметкерлерінің жеке құрылғыларын пайдалану кезінде осы құрылғыларға банктің, ұйымның жеке деректерін және ақпараттық активтерін өңдеу ортасын бөлуді қамтамасыз ететін арнайы бағдарламалық қамтамасыз ету орнатылады.

161. Мобильдік құрылғыларда орналастырылған банктің, ұйымның барлық ақпараты шифрленген түрде сақталады.

Қазақстан Республикасы
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

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» 1995 жылғы 31 тамыздағы 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 жүйелердегі бұзушылықтар, іркілістер туралы мәліметтерді қоса алғанда, ақпараттық қауіпсіздіктің оқыс оқиғалары туралы ақпаратты беру тәртібі мен мерзімін белгілейді.

Ескерту. 1-тармақ жаңа редакцияда – ҚР Ұлттық Банкі Басқармасының 19.11.2019 № 203 (01.01.2020 бастап қолданысқа енгізіледі); 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) қаулыларымен.

2. Қағидаларда мынадай ұғымдар пайдаланылады:

1) ақпараттық жүйелердегі бұзушылықтар, іркілістер туралы мәліметтерді қоса алғанда, 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;

2) ақпараттық жүйелердегі бұзушылықтарды, іркілістерді қоса алғанда, ақпараттық қауіпсіздіктің оқыс оқиғасы (бұдан әрі – 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) банктің, ұйымның электрондық ақпараттық ресурстарын заңсыз алу, көшіру, тарату, модификациялау, жою немесе бұғаттауға арналған талаптар;

3) ақпараттық қауіпсіздік – электрондық ақпараттық ресурстардың, ақпараттық жүйелердің және ақпараттық-коммуникациялық инфрақұрылымның сыртқы және ішкі қауіптерден қорғалу жай-күйі;

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

5) банктің, ұйымның ақпараттық-коммуникациялық инфрақұрылымы (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;

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 нарығын және қаржы ұйымдарын реттеу, бақылау мен 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) банктің, ұйым қызметінің тұрақтылығына қауіп төндіретін ақпараттық қауіпсіздіктің өзге де оқыс оқиғалары.

Осы тармақта көрсетілген ақпараттық қауіпсіздіктің оқыс оқиғалары туралы ақпаратты банк, ұйым тез арада Қағидаларға қосымшаға сәйкес нысан бойынша ақпараттық қауіпсіздіктің оқыс оқиғасы картасы түрінде ұсынады.

Ақпараттық қауіпсіздіктің әрбір оқыс оқиғасына ақпараттық қауіпсіздіктің оқыс оқиғасының жеке картасы толтырылады.

4. Банк, ұйым ақпараттық қауіпсіздіктің анықталған оқыс оқиғаларына талдау жүргізеді, оның нәтижелері бойынша тоқсан сайын, есепті тоқсаннан кейінгі айдың 30 (отызынан) кешіктірмей уәкілетті органға мына мәліметтер:

1) ақпараттық қауіпсіздіктің оқыс оқиғасы тіркелген күні мен уақыты;

2) ақпараттық қауіпсіздіктің оқыс оқиғасы болған күні мен уақыты;

3) ақпараттық қауіпсіздіктің оқыс оқиғасының сипаттамасы;

4) ақпараттық қауіпсіздіктің оқыс оқиғасының санаты;

5) зиян сомасы (теңгемен);

6) ақпараттық қауіпсіздіктің оқыс оқиғасын өңдеуге (жинау, талдау, түзету шараларын қабылдау) жауапты адамның тегі, аты, әкесінің аты (ол бар болса);

7) ақпараттық қауіпсіздіктің оқыс оқиғасы бойынша орындалған іс-әрекеттердің қысқаша сипаты;

8) ақпараттық қауіпсіздіктің оқыс оқиғасының мәртебесі (ақпараттық қауіпсіздіктің оқыс оқиғасы аяқталған күні мен уақыты) кіретін ақпараттық қауіпсіздіктің өңделген оқыс оқиғалары бойынша ақпаратты еркін нысанда ұсынады.

Ақпараттық қауіпсіздіктің өңделген оқыс оқиғалары бойынша ақпарат ұсынылатын деректердің конфиденциалдылығын және түзетілмейтіндігін

қамтамасыз ететін криптографиялық қорғау құралдары бар ақпаратты кепілдікпен жеткізудің тасымалдау жүйесін пайдалана отырып электрондық форматта беріледі.

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

нысан

Ақпараттық қауіпсіздіктің оқыс оқиғасы картасы

№	Жалпы мәліметтер	
	Ақпараттық қауіпсіздіктің оқыс оқиғасының сипаттамасы	Ақпараттық қауіпсіздіктің оқыс оқиғасы туралы ақпарат
1	Ақпараттық қауіпсіздіктің оқыс оқиғасының атауы	
2	Анықталған күні мен уақыты (кк.аа.жжжж және сс:мм сағат белдеуін көрсете отырып UTC+X)	
3	Анықталған орны (ұйым, филиал, ақпараттық инфрақұрылым сегменті)	
4	Ақпараттық қауіпсіздіктің оқыс оқиғасы туралы ақпараттың дереккөзі (пайдаланушы, әкімші, ақпараттық қауіпсіздік әкімшісі, ақпараттық қауіпсіздік бөлімшесінің қызметкері немесе техникалық құрал)	
5	Ақпараттық қауіпсіздіктің оқыс оқиғасы іске асырылған кезде қолданылған әдістер (әлеуметтік инженерия, зиянды кодты ендіру)	
	Ақпараттық қауіпсіздіктің оқыс оқиғасының мазмұны	
6	Ақпараттық қауіпсіздіктің оқыс оқиғасының белгілері	
7	Негізгі оқиғалар (қолданбалы және жүйелік бағдарламалық қамтамасыз етуде осалдылықтарды пайдалану; ақпараттық жүйеге санкцияланбаған кіру; ақпараттық жүйеге немесе деректерді беру желісіне «қызмет көрсетуден бас тартуға» шабуылы; сервердің зиянды бағдарламамен немесе кодпен зақымдануы; ақша қаражатын санкцияланбай аудару; банктің, ұйым қызметінің тұрақтылығына қауіп төндіретін ақпараттық қауіпсіздіктің өзге де оқыс оқиғалары)	
8	Зақымданған активтер (банктің, ұйымның ақпараттық инфрақұрылымының нақты деңгейі, желілі жабдығының деңгейі, желілі қосымшалар мен сервистердің деңгейі, операциялық жүйе деңгейі, технологиялық процестер мен қосымшаларының деңгейі және бизнес-процестердің деңгейі)	
9	Ақпараттық қауіпсіздіктің оқыс оқиғасының мәртебесі (аяқталған ақпараттық қауіпсіздіктің оқыс оқиғасы, ақпараттық қауіпсіздіктің оқыс оқиғасын жүзеге асыру әрекеті, ақпараттық қауіпсіздіктің оқыс оқиғасына күмән)	
10	Зиян	
11	Қауіп көздері (анықталған идентификаторлар)	
12	Ниеттілік (қасақана, қате)	
	Оқыс оқиға бойынша қабылданған шаралар	
13	Қабылданған іс-әрекеттер (осалдылықты идентификаттау, оқшаулау, қалпына келтіру және өзгелер)	

14	Жоспарланған іс-әрекеттер	
15	Хабардар болған тұлғалар (лауазымды тұлғалардың (тегі, аты, әкесінің аты (ол бар болса), мемлекеттік органдардың, ұйымдардың атауы)	
16	Тартылған мамандар (тегі, аты, әкесінің аты (ол бар болса), жұмыс орны, қызметі.)	

Ақпараттық қауіпсіздік бөлімшесінің басшысы

_____ _____

(тегі, аты, әкесінің аты (ол бар болса) (қолы)

Күні _____