Екінші деңгейдегі банктердің және банк операцияларының жекелеген түрлерін жүзеге асыратын ұйымдардың ақпарат жүйелерінің қауіпсіздігін қамтамасыз ету жөніндегі ережені бекіту туралы

Күшін жойған

Қазақстан Республикасының Ұлттық Банкі Басқармасының 2001 жылғы 31 наурыздағы N 80 қаулысы Қазақстан Республикасы Әділет министрлігінде 2001 жылғы 18 мамырда тіркелді. Тіркеу N 1517. Күші жойылды - Қазақстан Республикасы Ұлттық Банкі Басқармасының 2018 жылғы 27 наурыздағы № 48 қаулысымен

Ескерту. Күші жойылды – ҚР Ұлттық Банкі Басқармасының 27.03.2018 № 48 (01.12.2018 бастап қолданысқа енгізіледі) қаулысымен.

Екінші деңгейдегі банктердің және банк операцияларының жекелеген түрлерін жүзеге асыратын ұйымдардың ақпарат жүйелерінің қауіпсіздігін қамтамасыз ету жөніндегі жұмысты жүргізу тәртібін реттеу мақсатында Қазақстан Республикасы Ұлттық Банкінің Басқармасы ҚАУЛЫ ЕТЕДІ:

1. Екінші деңгейдегі банктердің және банк операцияларының жекелеген түрлерін жүзеге асыратын ұйымдардың ақпарат жүйелерінің қауіпсіздігін қамтамасыз ету жөніндегі ереже бекітілсін, Ереже мен осы қаулы Қазақстан Республикасының Әділет министрлігінде мемлекеттік тіркелген күннен бастап он төрт күндік мерзім өткеннен кейін күшіне енгізілсін.

2. Ақпарат технологиясы департаменті (Молчанов С.Н.):

1) Заң департаментімен (Шәріпов С.Б.) бірлесіп осы қаулыны және Екінші деңгейдегі банктердің және банк операцияларының жекелеген түрлерін жүзеге асыратын ұйымдардың ақпарат жүйелерінің қауіпсіздігін қамтамасыз ету жөніндегі ережені (бұдан әрі - Ереже) Қазақстан Республикасының Әділет министрлігінде мемлекеттік тіркеуден өткізу шараларын қабылдасын;

2) осы қаулы және Ереже Қазақстан Республикасының Әділет министрлігінде мемлекеттік тіркеуден өткізілген күннен бастап он күндік мерзімде Қазақстан Республикасы Ұлттық Банкінің орталық аппаратының барлық бөлімшелеріне, ұйымдарына және өкілдігіне жіберсін.

3. Қазақстан Республикасы Ұлттық Банкінің аумақтық филиалдарының басшылары осы қаулыны және Ережені алған күннен бастап төрт күндік мерзімде екінші деңгейдегі банктерге және банк операцияларының жекелеген түрлерін жүзеге асыратын ұйымдарға - ломбардтар мен айырбастау пункттерінен басқаларына жіберсін.

4. Қазақстан Республикасы Ұлттық Банкінің Орталық филиалы (Астана қаласы) (Сейфуллин М.Х.) осы қаулыны және Ережені алған күннен бастап төрт күндік мерзімде Қазақстан Республикасы Қаржы министрлігінің Қазынашылық Комитетіне жіберсін.

5. Осы қаулының орындалуын бақылау Қазақстан Республикасының Ұлттық Банкі Төрағасының орынбасарлары Н.Қ. Абдулинаға (2-тармақ бойынша) және Б.Ш. Тәжіяковқа (3 және 4-тармақ бойынша) жүктелсін.

Ұлттық Банк
Төрағасы

Қазақстан Республикасының

Ұлттық Банкі Басқармасының
2001 жылғы 31 наурыздағы
N 80 қаулысымен бекітілген

Екінші деңгейдегі банктердің және банк операцияларының
жекелеген түрлерін жүзеге асыратын
ұйымдардың ақпарат
жүйелерінің қауіпсіздігін қамтамасыз ету
жөніндегі
ереже

1-тарау. Жалпы ережелер

1. Екінші деңгейдегі банктер мен банк операцияларының жекелеген түрлерін жүзеге асыратын ұйымдардың ақпарат жүйелерінің қауіпсіздігін қамтамасыз ету жөніндегі ереже (бұдан әрі - Ереже) екінші деңгейдегі банктер мен банк операцияларының жекелеген түрлерін жүзеге асыратын ұйымдардың (бұдан әрі - банктік ұйымдар) ақпарат жүйесі қауіпсіздігінің мақсатын, стратегиясын және жалпы саясатын айқындайды.

2. Ереже Қазақстан Республикасының нормативтік құқықтық актілеріне сәйкес жасалған және ақпарат жүйелерінің қауіпсіздігіне төнетін қатерлердің түрлерін, қорғауға тиісті ресурстарды, сондай-ақ ұйымдастырушылық және бағдарламалық-техникалық қорғау шараларымен қоса қауіпсіздік жүйесін іске асырудың негізгі бағыттарын анықтайды.

3. Ереженің нормалары ломбардтар мен айырбастау пункттерін қоспағанда, банктік ұйымдардың қолдануы үшін міндетті.

2-тарау. Ережеде қолданылатын негізгі ұғымдар

4. Ережеде мынадай ұғымдар қолданылады:

1) ақпарат қауіпсіздігі - ақпараттың және оның инфрақұрылымының кездейсоқ немесе әдейі жасалған, табиғи немесе жасанды сипаттағы іс-әрекеттерден, жария болудан, ұрлықтан, жоғалудан, жойылудан, бұрмаланудан, көшіруден, қолдан жасаудан, шек қоюдан және рұқсатсыз кіру салдарынан туындайтын басқа да қауіптерден қорғалуы;

2) ақпаратты қорғау - ақпарат қауіпсіздігін қамтамасыз ететін іс-шаралар кешені;

3) қауіпсіздік жүйесі - ұйымдастыру шараларының кешені және ақпаратты қорғаудың бағдарламалық-техникалық құралдары;

4) зиян келтіретін бағдарламалық қамтамасыз ету (компьютер вирустары) - орындалатын код жиынтығы, ол (түпнұсқамен ішінара немесе толық сәйкес келетін) өз көшірмелерін жасауға және оларды пайдаланушымен келіспей-ақ компьютерлік жүйелердің, тораптардың түрлі объектілеріне/ресурстарына енгізуге қабілетті. Мұндайда көшірме әрі қарай таралу қабілетін сақтайды, ақпарат жүйесінің және/немесе жабдықтардың қалыпты жұмысын бұзады, көбінесе ақпарат жүйесіндегі мәліметтердің жоғалуына әкеліп соқтырады;

5) ақпарат жүйелері - құжаттардың, техникалық құралдар жүйесінің және ақпаратты өңдеу тәсілдерінің ұйымдастырылған түрде тәртіпке келтірілген жиынтығы;

6) қауіпсіздік саясаты - ақпараттың шектеулі таратылуын басқаруды, қорғауды және бөлуді реттейтін нормалар мен іс жүзіндегі тәсілдер;

7) бірегейлік - өз ретінде жалғыз, нақты ақпарат жүйесі шегінде қайталанбайтын қасиет;

8) сәйкестендіруші - субъектіге және/немесе объектіге берілген және жүйеге және/немесе жүйе ресурстарына тәртіппен кіру рұқсаты үшін тағайындалған бірегей дербес код немесе аты;

9) сәйкестендіру - жүйеге және/немесе сәйкестендіру жүйесінің ресурсына кіру рұқсатын алу үшін ұсынылған жүйеде бар сәйкестендіруші тізбенің сәйкестігін беру немесе анықтау;

10) аутентификация - кіру субъектісінің немесе объектісінің түпнұсқалығын жүйеде көрсетіліп отырған кіру деректемелерін анықтау жолымен мақұлдау;

11) ақпаратты (деректерді, бағдарламалық қамтамасыз етуді, ақпарат хабарларын) жария ету - ақпаратқа рұқсатсыз кіру және алынған мәліметтердің кездейсоқ немесе авторсыз әдейі түрде ашып алу нәтижесінде болған іс-әрекет;

12) қауіпсіздік белгісі - мәліметтерге қатысты саланың құпиялылығы мен санатының деңгейінен тұратын ақпараттың жабық болу дәрежесі.

3-тарау. Қауіпсіздік жүйесінің негізгі мақсаты

5. Қауіпсіздік жүйесінің мақсаты банктік ұйымдардағы ақпарат жүйесінің тұрақты қызмет етуін, есептеу және телекоммуникациялық құралдардың көмегімен қаржылық қылмыс жасау мүмкіндігінің алдын алуды, таратылуы шектелген ақпараттың жоғалуына, жария болуына, бұрмалануына және жойылуына жол бермеуді қамтамасыз ету болып табылады.

6. Банктік ұйымдардың ақпарат жүйелерінің қауіпсіздік жүйесі мыналарды қамтамасыз етуге тиіс:

1) ақпараттың құпиялылығы - оны сақтау, өңдеу немесе коммуникациялық арналар арқылы беру кезінде жария болудан қорғау;

2) ақпараттың сақталуы - ақпаратты сақтау, өңдеу барысында немесе коммуникациялық арналар бойынша жіберілген кезде бүлінуден қорғау, бүтіндігін сақтау және рұқсатсыз өзгертуден, толықтырудан, көшіруден немесе өшіруден қорғау;

3) кіру рұқсаты - ақпараттық хабарларды орта жолдан ұстап қалудан және/ немесе деректердің кешіктірілуінен, сондай-ақ бірігіп қолдануға арналған ақпарат жүйесінің деректерін және басқа ресурстарын бір пайдаланушының қолдануынан қорғау.

4-тарау. Қауіпсіздік саясаты

7. Әрбір банктік ұйымда тиісті басқару органы бекітетін және есептеуші және коммуникациялық ресурстар мен ақпаратты пайдаланудың ең тиімді әдісін анықтайтын қауіпсіздік саясаты, сондай-ақ қауіпсіздік режимін қамтамасыз ету жөніндегі іс-шаралар жасалуға тиіс.

8. Қауіпсіздік саясаты:

1) ақпарат қауіпсіздігі саласындағы жұмыстың жалпы бағыттарын;

2) ақпарат жүйесін қорғаудың мақсатын;

3) ақпарат жүйесін тұтастай және оның жекелеген бөліктерін қорғаудың жалпы талаптарын;

4) банктік ұйымның қауіпсіздік саясатын анықтаушы қажетті талаптарды жасауға жауапты тұлғаларды бекітуін;

5) банктік ұйымның ақпарат жүйесін және оны қорғау жүйесін құруға және жұмыс істеуін қолдауға жауапты бөлімшені бекітуін анықтайды.

9. Қауіпсіздік саясатының мақсаты ақпарат жүйесінің қызмет етуінің тұрақтылығын және ақпараттың сақталуын қамтамасыз ету болып табылады.

10. Қауіпсіздік саясаты банктік ұйымдардың ақпарат жүйесі үшін дұрыс деп саналатын тәуекелдерді талдау негізінде құрылады және онда:

1) ақпарат жүйесі құрамының сипаттамасы;

2) ұйымның ақпарат жүйесін пайдаланушылардың тізімі, олардың ақпаратқа, бағдарламалық және техникалық құралдарға кіру құқықтары мен артықшылықтары (олардың қызмет жағдайы мен атқаратын қызметінің сипатына қарай) болады.

5-тарау. Тәуекелдерді бағалау

11. Қауіпсіздік саясатын қалыптастырудың шешуші құрамдас бөлігі қауіпсіздік жүйесі объектілерін анықтауға мүмкіндік беретін тәуекелді бағалау және ақпаратты қорғауға қажетті материалдық ресурстардың қолайлы көлемі болып табылады.

12. Ақпарат қауіпсіздігінің мәні болып табылатын тәуекелдерді бағалау үшін банктік ұйымдардың лауазымды тұлғалары мен жауапты бөлімшелері ақпарат жүйесінің қауіпсіздігіне төнген қатерге: назар салатын қатердің сипатына (қатер әсер ететін спектрі) талдау жүргізеді. Тәуекелді талдау процесі екі кезеңнен тұрады:

1) ақпарат жүйесі объектілерін сәйкестендіру;

2) қатерді анықтау.

13. Ақпарат жүйесі объектілерін сәйкестендіру кезінде қорғауды қажет ететін объектілердің тізімі жасалады:

1) техникалық құралдар - компьютерлер (серверлер және жұмыс станциялары), перифериялық қондырғылар, сыртқы интерфейстер, кабельдік жүйе, активті желілік жабдық (өткізгіштер, маршрутизаторлар және экрандар);

2) бағдарламалық қамтамасыз ету - операциялық жүйелер (желілік, серверлік және клиенттік), қолданбалы бағдарламалық қамтамасыз ету, бастапқы мәтіндері , объект модульдері, қызметтік бағдарламалар, желіні және жекелеген жүйелерді басқару құралдары;

3) ақпарат - өңделетін, байланыс арналары бойынша берілетін, сақталған (архив, резервтік көшірме, мәліметтер базасы, тіркеу журналы және басқа мәліметтер);

4) құжаттама - жалпы жүйелік және қолданбалы бағдарламалық қамтамасыз етуге, компьютерлік және телекоммуникациялық жабдыққа және басқа техникалық құралдарға, басқару іс-шараларына арналған;

5) ақпарат тасымалдаушылар - қағаз, магнитті, оптикалық және басқа тасымалдаушылар.

Сәйкестендіру барысында ақпарат ресурстарына пайдаланушылардың, қызмет көрсететін қызметкерлердің және олардың құқықтарының спектріне тәртіппен кіруді анықтайтын тізім жасалады.

14. Банктік ұйымдардың лауазымды тұлғалары қатерді анықтау кезінде:

1) қорғауды қажет ететін объектілерге бөтен ұйымдар мен тұлғалардың рұқсатсыз кіруінен;

2) құпия ақпараттың түрлі сипаттағы өндірістік қызметті қамтамасыз ететін және орындау техникалық құралдар арқылы жария болуынан;

3) пайдаланушылардың, операторлардың, жүйелік администраторлардың және ақпарат жүйесіне қызмет көрсетуші басқа тұлғалардың байқаусыз жіберген қателерінің салдарынан ақпараттың жоғалуынан келетін болжалды шығынның мөлшеріне бағалау жүргізуі қажет.

15. Ақпарат ресурстарына мына жолдармен қатер төнуі мүмкін:

1) таратылуы шектелген ақпаратқа рұқсатсыз кіру және алу;

2) ұйымда немесе құрылымда жұмыс істейтін қызметі тікелей байланысты тұлғаға пара беру;

3) байланыс құралдары мен жүйелерінде және есептеу техникаларында айналымдағы ақпаратты байқайтын техникалық құралдардың көмегімен орта жолдан ұстап қалу, ақпаратты тауып алу және түсіру, ақпаратқа рұқсатсыз кіру және оны өңдеу, беру және сақтау барысында бағдарламалық және саймандық құралдармен әдейі түрде әсер ету;

4) зиян келтіретін бағдарламалық қамтамасыз ету арқылы деректерді

және бағдарламалық қамтамасыз етуді бұзу;

5) таратылуы шектелген ақпаратты (мәліметті) авторсыз беру және/немесе алу.

16. Тәуекелді талдағаннан және қауіпсіздік саясатын жасағаннан кейін банктік ұйымның лауазымды тұлғалары тиімді және үнемді қорғау механизмдеріне таңдау жүргізеді және ақпаратты қорғау жоспарын жасайды.

6-тарау. Ақпаратты қорғау жоспарын іске асыру

17. Ақпаратты қорғау жоспарына:

1) ұйымдастырушылық;

2) бағдарламалық-техникалық шаралар кіреді.

18. Банктік ұйымдарда ақпарат жүйелерінің тиімді қорғау жүйесін құру үшін мынадай негізгі принциптер мен тәсілдер пайдаланылуы керек:

1) пайдаланушыларды сәйкестендіру - ақпарат жүйесін пайдаланушылардың әрқайсысы өзінің жеке, айрықша сәйкестендіруші (тиісті қосалқы жүйенің шеңберінде), немесе бірнешеуі немесе барлық автоматтандырылған жүйелер үшін айрықша сәйкестендіруші иемденуі тиіс;

2) кіру рұқсаты бойынша шектеу - пайдаланушыға немесе пайдаланушылар тобына әртүрлі мәліметке, мәліметтер тобына немесе ресурстарына кіру рұқсатының тиісті деңгейі ұсынылады;

3) қызметкерлерді дайындау - банктік ұйымдар ақпаратты қорғау жүйесін басқаруға, пайдалануға немесе қызмет етуіне қатысатын барлық қызметкерлерді міндетті кезеңдік оқытумен қамтамасыз етуі тиіс;

4) ақпарат жүйесін орталықтан басқару - банктік ұйымдардың әрбір ақпарат жүйесінде тиісті өкіммен ақпарат жүйесінің қауіпсіздік басқарушысы тағайындалуы тиіс;

5) бағдарламалық қамтамасыз етудің тазалығы - пайдаланылатын қолданбалы және жалпы жүйелік бағдарламалық қамтамасыз етудің лицензиясы болуы тиіс, бағдарламалық қамтамасыз ету сертификатталған жеткізушілерден алынған немесе Қазақстан Республикасының нормативтік құқықтық актілеріне сәйкес сертификатталған болуы керек;

6) сапалы қызметті пайдалану - ақпарат жүйелерін қорғау құралдары мен жүйелерін жасау және қондыру үшін шарт негізінде тек көрсетілген қызмет түріне лицензиясы (сертификаты) бар мамандандырылған ұйымдар тартылуы тиіс.

&1. Ақпарат қауіпсіздігін қамтамасыз етудің
;
ұйымдастыру шаралары

19. Ұйымдастыру шаралары Қазақстан Республикасының нормативтік құқықтық актілерін және банктік ұйымның ішкі талаптарын сақтауды, ұйым ішіндегі қауіпсіздік жағдайын қадағалауды, тәртіп бұзу жағдайларында әрекет ету, ұйымдағы өзгерістерді ескере отырып қорғау шараларын дамытуды қамтамасыз етуі тиіс.

20. Қауіпсіздікті қамтамасыз етуді ұйымдастыру шараларына мынадай

іс-шаралар жатады:

1) ақпарат жүйесін нақты қорғау;

2) ақпарат қауіпсіздігіне қатысы бар ақпарат жүйелерінің жұмысына қолдау көрсету;

3) ақпарат жүйесінің деректерін өзгерту бойынша іс-әрекеттерді орындау кезінде міндеттерді бөлу және оның қажеттігін кем дегенде 2 (екі) қызметкердің растауы (санкция беруі);

4) әрбір пайдаланушыға өзіне берілген лауазымдық міндеттерін орындауға қажетті тиісті кіру құқығын белгілеу және өзара ауыстыруын қамтамасыз ету;

5) жауапты тұлғаның ақпарат қауіпсіздігі режимін бұзуына жол бермеу;

6) қалпына келтіру жұмыстарын жоспарлау.

21. Нақты қорғау мыналарға бөлінеді:

1) кіру рұқсатын нақты басқару;

2) өртке қарсы қауіпсіздік шаралары;

3) қолдау көрсетуші инфрақұрылымды қорғау;

4) мәліметтерді орта жолдан ұстап қалудан қорғау, ықшамды жүйелерді қорғау.

22. Ақпарат жүйелерінің жұмыс істеуіне қолдау көрсету жөніндегі іс-шаралар мыналарға бөлінеді:

1) пайдаланушыларға қолдау көрсету - ақпарат қауіпсіздігі мәселелері бойынша кеңес беруді ұйымдастыру, олардың әдеттегідей қателерін анықтау және кең таралған жағдайларға арналған ұсынысы бар ескертпемен қамтамасыз ету;

2) бағдарламалық қамтамасыз етуге қолдау көрсету - бағдарламалық қамтамасыз етудің лицензиялық (сертификаттық) тазалығын бақылау;

3) конфигурациялық басқару - бағдарламалық және техникалық конфигурацияға енгізілген өзгертулерге бақылау және белгілеу жасау;

4) апат және дүлей күштің басқа жағдайында ақпарат жүйесін және

деректерді қалпына келтіру үшін резервтік көшірме жасау;

5) деректерді тасымалдаушыны басқару - есеп, күтіп ұстау және сақтау тәртібі;

6) құжаттау - істің ағымдағы жағдайының өзекті көрсетілуі.

23. Ақпарат жүйесі қауіпсіздігінің режимі бұзылған жағдайда банктік ұйымдардың жауапты тұлғалары:

1) келтірілген зиянды азайту мақсатында шұғыл шараларды орындауға - рұқсатсыз кірген тұлғаны анықтауға және оны қоршауға;

2) бұзудың жинақталған статистикасына шолу жасауға - келеңсіз оқиғаға талдау жасауға, қайталама бұзуды анықтауға, қорғау жүйесін жетілдіру жөнінде шаралар әзірлеуге міндетті.

24. Ақпараттық жүйелердің жұмыс істеу қабілеттілігі жоғалғаннан кейін резервтік көшіру және қалпына келтіру банк ұйымында белгіленген талаптармен анықталады.

&2. Ақпараттық қамтамасыз етудің

; бағдарламалық-техникалық шаралары

25. Банк ұйымын ақпараттық қамтамасыз ету жөніндегі бағдарламалық-техникалық шараларға мына жүйе енуге тиіс:

1) кіру-алу рұқсатын басқару;

2) хаттама жасау және техникалық жағдайын тексеру;

3) деректерді криптографиялық қорғау.

26. Кіру-алу рұқсатын басқару жүйесі мынадай іс-шаралардың орындалуын қамтамасыз етуі тиіс:

1) деректер, міндеттер тобының тізбесін анықтау және олардың құпиялылық деңгейін белгілеу;

2) әрбір дерек топтарын қорғаудың тәсілдері мен іс-шараларын белгілеу;

3) ақпарат жүйелерін пайдаланушылар тобын анықтау және оларды орындайтын қызметтері бойынша санаттарға бөлу және ақпаратқа кіру рұқсатының деңгейін белгілеу;

4) пайдаланушылардың сәйкестілік санаттарының тәртібін белгілеу;

5) әрбір "пайдаланушылар санаты - деректер типі" жұптары үшін кіру рұқсаты санаттарын анықтау;

6) жүйеге арнайы қондырғылар (жетондар, карталар, электрондық кілттер) бойынша кіру кезінде және ұзақтығы сегіз әріпті-цифрлы символдардан кем емес уақытша әрекет жасайтын парольге пайдаланушыларды сәйкестендіру және дәлме-дәл келтіру;

7) терминалдарды, персоналды компьютерлерді, компьютерлік желілер тораптарын, байланыс арналарын, сыртқы есептеу машиналарын біріктірілген ерекше қондырғылар бойынша аппараттық сәйкестендіру және дәлме-дәл келтіру ;

8) бағдарламаларды, атаулы дискілі кеңістіктерді (логикалық дискілер томдары, каталогтар, файлдар), жазбаларды, аты және бақылау сомалары бойынша жазбалар жолдарын (парольдер, кілттер) сәйкестендіру және дәлме-дәл келтіру;

9) ақпарат ағындарын қауіпсіздік белгілері көмегімен басқару.

Мұндайда жинақтағыштар құпиялылығының деңгейі оған жазылатын ақпараттың құпиялылық деңгейінен төмен болмауы тиіс.

27. Пайдаланушыларға, пайдаланушылар тобына, қызмет көрсетушілерге ақпарат жүйесінің ресурстарына кіру рұқсаты құқығын белгілеген сәттен бастап жүйенің бағдарламалық-техникалық құралдармен жүйеде болып жатқан оқиғалар туралы ақпараттарды хаттамалау, жинау және жинақтау жүргізіледі.

28. Жүйе оқиғаларын хаттамалау барысында мынадай ақпарат жазылады:

1) оқиғаның күні мен уақыты;

2) оқиғаның бастамашысын сәйкестендіруші;

3) оқиғаның түрі;

4) әрекеттің нәтижесі (сәтті немесе сәтсіз);

5) сұраушының көзі (терминалдың атауы);

6) қозғалған объектілердің аттары (ашылатын, көшірілетін немесе алынып тасталынатын файлдардың);

7) деректерді қорғау базасына енгізілген өзгерістерді сипаттау (объекті қауіпсіздігінің жаңа белгісі);

8) оқиға субъектілерінің және объектілерінің қауіпсіздік белгісі.

29. Хаттамалау нәтижелері келесіде жүйенің техникалық жағдайын тексеру үшін қолданылады.

30. Жинақталған ақпаратты бақылау мақсатында техникалық жағдайын тексеру, қауіпсіздіктің бұзылғанын байқауды жеңілдету, туындау себептерін анықтау үшін банктік ұйымдардың лауазымды тұлғаларымен күнделікті жүргізіледі.

31. Ақпарат жүйесінің қауіпсіздігіне қатысты және тексеруді талап ететін оқиғаларға мыналар жатады:

1) жүйеге кіру (сәтті немесе сәтсіз);

2) жүйеден шығу;

3) алыстағы жүйемен байланысу;

4) файлдармен операциялар жасау (ашу, жабу, атауын өзгерту, алып тастау, көшіру);

5) кіру рұқсатының немесе қауіпсіздіктің басқа белгілерінің деңгейінің өзгерістері (рұқсат режимі, пайдаланушының ақпарат ресурстарына кіру рұқсатының құқығы).

32. Ақпарат құпиялылығын қамтамасыз ету мақсатын жүзеге асыру кезінде криптографиялық құралдармен және/немесе осы ақпаратты шифрлеу жүйелерімен мыналарды орындау қажет:

1) деректерді бөлінетін тасымалдаушыларға жазу (әртүрлі пайдаланушылар мен пайдаланушылар топтарымен бірігіп қолданылатын);

2) байланыс арналары бойынша хабарлау;

3) деректерді ұзақ мерзімді сақтайтын кез келген алынатын тасымалдаушыларда жұмыстық, архивтік және резервтік көшірмелерді жасау.

33. Әртүрлі пайдаланушыларға жататын (пайдаланушылар топтарына) ақпаратты шифрлеу (шифрын ашу) үшін әртүрлі криптографиялық кілттерді қолдану қажет.

34. Ақпаратты шифрлеу (шифрын ашу) операциясын тек тиісті

криптографиялық кілттерге арнайы рұқсаты бар пайдаланушылар немесе пайдаланушылар топтары орындауы мүмкін.

35. Шифрлеу (шифрын ашу) жөніндегі жұмыстарды ұйымдастыру және

бақылауды мына төмендегілерді орындайтын банктік ұйымның жауапты адамы

жүргізеді:

1) криптографиялаудың бағдарламалық құралдарын есепке алу, сақтау және қолдау;

2) криптографиялық кілттердің генерациясын, кілттері бар ақпарат тасымалдаушыларды есепке алу, сақтау және беру;

3) криптографиялық кілттердің иелерінің тізімін жүргізу;

4) криптографиялық кілттердің иелерінің қауіпсіздігін қажетті нұсқаулармен қамтамасыз ету.

7-тарау. Ақпарат жүйесін әзірлеу ісінің технологиясы мен құжаттауы

36. Банктік ұйымдардағы ақпарат жүйелерін әзірлеу, енгізу және қолдау ісі әзірлеу кезеңдерін, өзгерістер енгізу тәртібін, өнеркәсіптік пайдалануға қабылдау , тесттен өткізу және іске қосу, барлық кезеңдерді құжаттауды талап етуді қосуы тиіс.

37. Банктік ұйымдардағы ақпарат жүйелерін әзірлеу, енгізу және қолдау ісі Қазақстан Республикасы аумағында қолданылып жүрген банктік ұйымдарда белгіленген ақпарат технологияларының стандарттары мен талаптарына сәйкес орындалады.

38. Ақпарат жүйелерін әзірлеу банктік ұйымды басқарушы тиісті органмен бекітілген жүйенің техникалық тапсырмасының негізінде және жобалау кезеңдеріне нақпа-нақ сәйкес орындалуы тиіс.

39. Өндірістік пайдаланудағы ақпарат жүйесінің бағдарламалық қамтамасыз етуі өзгеріссіз қалпында ұсталуы тиіс.

40. Бағдарламалық қамтамасыз етуге және/немесе ақпарат жүйесінің деректеріне рұқсат етілмеген өзгерістерді болдырмау, қажет болған кезде бағдарламалық қамтамасыз етуге өзгерістер енгізу (кемшіліктерді жою немесе жүйені толықтыру үшін) мақсатында өзгерістер енгізу ісі және оны құжаттау Қазақстан Республикасы аумағында қолданылып жүрген банктік ұйымдарда белгіленген ақпарат технологияларының стандарттары мен талаптарына сәйкес орындалады.

8-тарау. Бақылау және жауапкершілік

41. Қауіпсіздік саясатын әзірлеуді бақылау және ереже нормаларын сақтауды банктік ұйымдардың лауазымды адамдары жүзеге асырады.

42. Қауіпсіздік саясатының нақты орындалуы үшін жауапкершілік арнайы тағайындалған жауапты орындаушыларға жүктелуі тиіс.

43. Банктік ұйымдардың ақпарат қауіпсіздігін сақтау үшін жауапкершілікті әдеттегідей лауазымдық міндеттеріне сәйкес мына төмендегілерге жүктеледі:

1) бірінші басшылар;

2) ақпарат жүйесін және оларды қорғау жүйесін жасау және жұмыс істеу қабілеттілігін қолдауға, қауіпсіздік саясатын пайдаланушыларға жеткізуді және пайдаланушылармен байланыстарды қамтамасыз етуші жауапты бөлімшелердің басшылары;

3) қауіпсіздік саясатын іске асыруға қажетті ақпарат жүйесінің үздіксіз қызмет етуін және техникалық шаралардың жүзеге асырылуын қамтамасыз етуші ақпарат жүйесі қауіпсіздігін басқарушылар;

4) қауіпсіздік саясатына сәйкес ақпарат жүйесін пайдалануға жауапкершілік атқаратын пайдаланушылар қауіпсіздіктің жекелеген аспектілері үшін жауапты адамдардың өкімдеріне бағынуға, басшыларды барлық күдікті жағдайлар туралы хабардар етуге міндетті.

44. Банктік ұйымдардың лауазымды адамдары:

1) қауіпсіздік режимінің бұзылуынан мүмкін болатын шығынның мөлшерін бағалай және тиімді қорғау құралдарын таңдай отырып, ақпарат жүйелерінің ұрымтал жерлерінің тәуекелдерін талдауды, қорғауды талап ететін объектілерді анықтауды жүргізеді;

2) төтенше (шұғыл) жағдайларда қауіпсіздік шараларына және әрекет ету ережелеріне, вирусқа қарсы бақылауға және жүйеге дұрыс кіруге қатысты мәселелерге (тіркеу кезінде тек өзінің сәйкестендірушісін көрсете отырып) айрықша назар аудару арқылы қызметкерлерді оқытуды қамтамасыз етеді;

3) кез келген қызметкер басқа бөлімшеге ауысқан жағдайда, демалыста, іссапарда болғанда немесе жұмыстан шыққан жағдайда бұл жөнінде ақпарат жүйелерінің қауіпсіздігіне жауапты арнайы тағайындалған жауапты орындаушыларды және басқарушыларды дереу хабарлауды қамтамасыз етеді.

45. Ақпарат жүйесінің қауіпсіздік басқарушылары қорғау жүйесін күнделікті басқару және жұмыс істеу қабілеттілігіне қолдау көрсету және үздіксіз қызмет ету жөніндегі жұмыстарды орындайды.

46. Ақпарат жүйесінің қауіпсіздік басқарушылары:

1) ақпарат жүйелерінің ресурстарына кіру рұқсатына арналған сәйкестендіру және дәлме-дәл келтіру іс-шараларының міндеттілігін қамтамасыз етуге;

2) қосарланбаған пайдаланушыларға ақпарат ресурстарына кіру рұқсаты құқығын алуға жол бермеу, пайдаланушыларға тек тіркеу нысандарын толтырғаннан кейін кіру есімдерін және бастапқы парольдерді беруге;

3) ақпарат жүйесі өңдейтін ақпараттардың резервтік көшірмелерін орындалуын қайталануын бақылауға;

4) жүйе ресурстарының қорғалу беріктілігіне жоспарлы және жоспардан тыс тексеру жүргізу, қолдағы қауіпсіздік саясатының тиімділігі туралы арнайы тағайындалған жауапты орындаушыларды хабардар етіп және олардың қарауына қорғау жүйесін жетілдіру жөнінде ұсыныс енгізуге;

5) корпоративтік желі жабдығының, оның ішінде арнайы желі аралық бағдарламалық құралдардың қорғанысын қамтамасыз етуге;

6) қауіп төндіруші оқиғаларға жедел және тиімді жауап қайтару, қауіптің бетін қайтару жөнінде шаралар қабылдауға және бұзғыштарды анықтау, тіркеу және қорғанысты бұзуға тырысу туралы арнайы тағайындалған жауапты орындаушыларға хабарлауға;

7) күдікті жағдайларды байқау, зиянды бағдарламалық қамтамасыз етудің бар екендігін және оның ақпарат жүйесі мен оның құрамдас бөліктерінің жұмысына әсерін байқау мақсатында ақпарат жүйесінің қызмет ету барысын қадағалаудың тексерілген бағдарламалық-техникалық құралдарын пайдалануға;

8) күнделікті жалпы ақпарат жүйесіне және айрықша файлдық серверлерге қатысты тіркеу ақпаратын талдауға;

9) ақпарат қауіпсіздігі саласындағы жаңалықтарға шолу жасау, олар жөнінде пайдаланушыларды және арнайы тағайындалған жауапты орындаушыларды хабардар етуге міндетті.

47. Ақпарат жүйесі қауіпсіздігінің басқарушылары оларға берілген өкілеттікті өз мақсатына немесе зиянкестік пиғылда қолдануға құқығы жоқ.

48. Банктік ұйымдардың бөлімшелерінің қызметкерлері (пайдаланушылар):

1) ақпарат жүйесінің қауіпсіздігін қамтамасыз ететін ішкі талаптарды білуге және сақтауға;

2) өзінің ақпараттарының құпиялылығын және біртұтастығын қамтамасыз етуге арналған қолдағы тіркелген қорғау тетіктерін пайдалануға;

3) ұзындығы сегізден кем емес әріпті-цифрлы символдары бар жеке парольдерді таңдауға;

4) жеке парольдерге басқа адамдар кіре алмауын қамтамасыз етуге;

5) ақпарат жүйесінің қауіпсіздігінің басқарушыларын және/немесе арнайы тағайындалған жауапты орындаушыларды қауіпсіздіктің бұзылғаны және басқа күдікті жағдайлар туралы хабардар етуге;

6) ақпарат жүйелерінің ресурстарын қорғауда әлсіз жерлерін байқаған жағдайда бұл жөнінде ақпарат жүйесінің қауіпсіздігінің басқарушыларын және/ немесе арнайы тағайындалған жауапты орындаушыларды дереу хабардар етуге;

7) дұрыс сәйкестендірілген және дәлме-дәл келтірілген ақпаратты

беруді қамтамасыз етуге;

8) өз компьютерінің қатты дискісіндегі ақпараттың резервтік

көшірмесін жасауды қамтамасыз етуге;

9) қауіпті кодтың кіруінің алдын алу үшін оны байқау және жоюға арналған шараларды орындауға;

10) төтенше жағдайларда әрекет ету нормаларын, апат және басқа да дүлей күштің салдарларын жою кезінде іс-қимылдардың бірізділігін орындауға

міндетті.

49. Банктік ұйымдардың бөлімшелерінің қызметкерлері (пайдаланушылар) ақпарат жүйесінің деректерімен қосарланбаған жұмыс істеуге, басқа пайдаланушыларға кедергі келтіруге, басқа пайдаланушылардың атынан жұмыс

істеуге әрекет жасауға құқықтары жоқ.

50. Ұлттық Банк Қазақстан Республикасының қолданылып жүрген заңдарында белгіленген өз өкілеттіктері шеңберінде банктік ұйымдардың қызметін тексеру кезеңінде Ереже талаптарының орындалуын бақылауды жүзеге

асырады.

Ұлттық Банк

Төрағасы

Мамандар:

Икебаева А.Ж.

Жұманазарова А.Б.