

**Екiншi деңгейдегi банктердiң және банк операцияларының жекелеген түрлерiн жүзеге асыратын ұйымдардың ақпарат жүйелерiнiң қауiпсiздiгiн қамтамасыз ету жөнiндегi ереженi бекiту 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.

      Екiншi деңгейдегi банктердiң және банк операцияларының жекелеген түрлерiн жүзеге асыратын ұйымдардың ақпарат жүйелерiнiң қауiпсiздiгiн қамтамасыз ету жөнiндегi жұмысты жүргiзу тәртiбiн реттеу мақсатында Қазақстан Республикасы Ұлттық Банкiнiң Басқармасы ҚАУЛЫ ЕТЕДI:

      1. Екiншi деңгейдегi банктердiң және банк операцияларының жекелеген түрлерін жүзеге асыратын ұйымдардың ақпарат жүйелерiнiң қауiпсiздiгiн қамтамасыз ету жөнiндегi ереже бекiтiлсiн, Ереже мен осы қаулы Қазақстан Республикасының Әдiлет министрлiгiнде мемлекеттiк тiркелген күннен бастап он төрт күндiк мерзiм өткеннен кейiн күшiне енгiзiлсiн.

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

      1) Заң департаментiмен (Шәрiпов С.Б.) бiрлесiп осы қаулыны және Екiншi деңгейдегi банктердiң және банк операцияларының жекелеген түрлерiн жүзеге асыратын ұйымдардың ақпарат жүйелерiнiң қауіпсiздiгiн қамтамасыз ету жөнiндегi ереженi (бұдан әрi - Ереже) Қазақстан Республикасының Әдiлет министрлiгiнде мемлекеттiк тiркеуден өткiзу шараларын қабылдасын;

      2) осы қаулы және Ереже Қазақстан Республикасының Әдiлет министрлiгiнде мемлекеттiк тiркеуден өткiзiлген күннен бастап он күндiк мерзiмде Қазақстан Республикасы Ұлттық Банкiнiң орталық аппаратының барлық бөлiмшелерiне, ұйымдарына және өкiлдiгiне жiберсiн.

      3. Қазақстан Республикасы Ұлттық Банкiнiң аумақтық филиалдарының басшылары осы қаулыны және Ереженi алған күннен бастап төрт күндiк мерзiмде екiншi деңгейдегi банктерге және банк операцияларының жекелеген түрлерiн жүзеге асыратын ұйымдарға - ломбардтар мен айырбастау пункттерiнен басқаларына жiберсiн.

      4. Қазақстан Республикасы Ұлттық Банкiнiң Орталық филиалы (Астана қаласы) (Сейфуллин М.Х.) осы қаулыны және Ереженi 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 Басқармасының2001 жылғы 31 наурыздағыN 80 қаулысымен бекітілген |
|   |  |
|   |   |
|   |  Екiншi деңгейдегi банктердiң және банк операцияларының  |
|   |  жекелеген түрлерiн жүзеге асыратын ұйымдардың ақпарат  |
|   |  жүйелерiнiң қауiпсiздiгiн қамтамасыз ету жөнiндегi  |
|   |  ереже  |
|   |   |
|   |  1-тарау. Жалпы ережелер  |
|   |   |

      1. Екiншi деңгейдегi банктер мен банк операцияларының жекелеген түрлерін жүзеге асыратыН ұйымдардың ақпарат жүйелерiнiң қауіпсiздiгiн қамтамасыз ету жөнiндегi ереже (бұдан әрi - Ереже) екiншi деңгейдегi банктер мен банк операцияларының жекелеген түрлерiн жүзеге асыратын ұйымдардың (бұдан әрi - банктiк ұйымдар) ақпарат жүйесi қауiпсiздiгiнiң мақсатын, стратегиясын және жалпы саясатын айқындайды.

      2. Ереже Қазақстан Республикасының нормативтiк құқықтық актiлерiне сәйкес жасалған және ақпарат жүйелерiнiң қауiпсiздiгiне төнетiн қатерлердiң түрлерiн, қорғауға тиiстi ресурстарды, сондай-ақ ұйымдастырушылық және бағдарламалық-техникалық қорғау шараларымен қоса қауiпсiздiк жүйесiн iске асырудың негiзгi бағыттарын анықтайды.

      3. Ереженiң нормалары ломбардтар мен айырбастау пункттерiн қоспағанда, банктiк ұйымдардың қолдануы үшiн мiндеттi.

      2-тарау. Ережеде қолданылатын негiзгi ұғымдар

      4. Ережеде мынадай ұғымдар қолданылады:

      1) ақпарат қауiпсiздiгi - ақпараттың және оның инфрақұрылымының кездейсоқ немесе әдейi жасалған, табиғи немесе жасанды сипаттағы iс-әрекеттерден, жария болудан, ұрлықтан, жоғалудан, жойылудан, бұрмаланудан, көшiруден, қолдан жасаудан, шек қоюдан және рұқсатсыз кiру салдарынан туындайтын басқа да қауiптерден қорғалуы;

      2) ақпаратты қорғау - ақпарат қауiпсiздiгiн қамтамасыз ететiн iс-шаралар кешенi;

      3) қауiпсiздiк жүйесi - ұйымдастыру шараларының кешенi және ақпаратты қорғаудың бағдарламалық-техникалық құралдары;

      4) зиян келтiретiн бағдарламалық қамтамасыз ету (компьютер вирустары) - орындалатын код жиынтығы, ол (түпнұсқамен iшiнара немесе толық сәйкес келетiн) өз көшiрмелерiн жасауға және оларды пайдаланушымен келiспей-ақ компьютерлiк жүйелердiң, тораптардың түрлi объектiлерiне/ресурстарына енгiзуге қабiлеттi. Мұндайда көшiрме әрi қарай таралу қабiлетiн сақтайды, ақпарат жүйесiнiң және/немесе жабдықтардың қалыпты жұмысын бұзады, көбiнесе ақпарат жүйесiндегi мәлiметтердiң жоғалуына әкелiп соқтырады;

      5) ақпарат жүйелерi - құжаттардың, техникалық құралдар жүйесiнiң және ақпаратты өңдеу тәсiлдерiнiң ұйымдастырылған түрде тәртiпке келтiрiлген жиынтығы;

      6) қауiпсiздiк саясаты - ақпараттың шектеулi таратылуын басқаруды, қорғауды және бөлудi реттейтiн нормалар мен iс жүзiндегi тәсiлдер;

      7) бiрегейлiк - өз ретiнде жалғыз, нақты ақпарат жүйесi шегiнде қайталанбайтын қасиет;

      8) сәйкестендiрушi - субъектiге және/немесе объектiге берiлген және жүйеге және/немесе жүйе ресурстарына тәртiппен кiру рұқсаты үшiн тағайындалған бiрегей дербес код немесе аты;

      9) сәйкестендiру - жүйеге және/немесе сәйкестендiру жүйесiнiң ресурсына кiру рұқсатын алу үшiн ұсынылған жүйеде бар сәйкестендiрушi тiзбенiң сәйкестiгiн беру немесе анықтау;

      10) аутентификация - кiру субъектiсiнiң немесе объектiсiнiң түпнұсқалығын жүйеде көрсетiлiп отырған кiру деректемелерiн анықтау жолымен мақұлдау;

      11) ақпаратты (деректердi, бағдарламалық қамтамасыз етудi, ақпарат хабарларын) жария ету - ақпаратқа рұқсатсыз кiру және алынған мәлiметтердiң кездейсоқ немесе авторсыз әдейi түрде ашып алу нәтижесiнде болған iс-әрекет;

      12) қауiпсiздiк белгiсi - мәлiметтерге қатысты саланың құпиялылығы мен санатының деңгейiнен тұратын ақпараттың жабық болу дәрежесi.

      3-тарау. Қауiпсiздiк жүйесiнiң негiзгi мақсаты

      5. Қауiпсiздiк жүйесiнiң мақсаты банктiк ұйымдардағы ақпарат жүйесiнiң тұрақты қызмет етуiн, есептеу және телекоммуникациялық құралдардың көмегiмен қаржылық қылмыс жасау мүмкiндiгiнiң алдын алуды, таратылуы шектелген ақпараттың жоғалуына, жария болуына, бұрмалануына және жойылуына жол бермеудi қамтамасыз ету болып табылады.

      6. Банктiк ұйымдардың ақпарат жүйелерiнiң қауiпсiздiк жүйесi мыналарды қамтамасыз етуге тиiс:

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

      2) ақпараттың сақталуы - ақпаратты сақтау, өңдеу барысында немесе коммуникациялық арналар бойынша жiберiлген кезде бүлiнуден қорғау, бүтiндiгiн сақтау және рұқсатсыз өзгертуден, толықтырудан, көшiруден немесе өшiруден қорғау;

      3) кiру рұқсаты - ақпараттық хабарларды орта жолдан ұстап қалудан және/немесе деректердiң кешiктiрiлуiнен, сондай-ақ бiрiгiп қолдануға арналған ақпарат жүйесiнiң деректерiн және басқа ресурстарын бiр пайдаланушының қолдануынан қорғау.

      4-тарау. Қауiпсiздiк саясаты

      7. Әрбiр банктiк ұйымда тиiстi басқару органы бекiтетiн және есептеушi және коммуникациялық ресурстар мен ақпаратты пайдаланудың ең тиiмдi әдiсiн анықтайтын қауiпсiздiк саясаты, сондай-ақ қауiпсiздiк режимiн қамтамасыз ету жөнiндегi iс-шаралар жасалуға тиiс.

      8. Қауiпсiздiк саясаты:

      1) ақпарат қауiпсiздiгi саласындағы жұмыстың жалпы бағыттарын;

      2) ақпарат жүйесiн қорғаудың мақсатын;

      3) ақпарат жүйесiн тұтастай және оның жекелеген бөлiктерiн қорғаудың жалпы талаптарын;

      4) банктiк ұйымның қауiпсiздiк саясатын анықтаушы қажеттi талаптарды жасауға жауапты тұлғаларды бекiтуiн;

      5) банктiк ұйымның ақпарат жүйесiн және оны қорғау жүйесiн құруға және жұмыс iстеуiн қолдауға жауапты бөлiмшенi бекiтуiн анықтайды.

      9. Қауiпсiздiк саясатының мақсаты ақпарат жүйесiнiң қызмет етуiнiң тұрақтылығын және ақпараттың сақталуын қамтамасыз ету болып табылады.

      10. Қауiпсiздiк саясаты банктiк ұйымдардың ақпарат жүйесi үшiн дұрыс деп саналатын тәуекелдердi талдау негiзiнде құрылады және онда:

      1) ақпарат жүйесi құрамының сипаттамасы;

      2) ұйымның ақпарат жүйесiн пайдаланушылардың тiзiмi, олардың ақпаратқа, бағдарламалық және техникалық құралдарға кiру құқықтары мен артықшылықтары (олардың қызмет жағдайы мен атқаратын қызметiнiң сипатына қарай) болады.

      5-тарау. Тәуекелдердi бағалау

      11. Қауiпсiздiк саясатын қалыптастырудың шешушi құрамдас бөлiгi қауiпсiздiк жүйесi объектiлерiн анықтауға мүмкiндiк беретiн тәуекелдi бағалау және ақпаратты қорғауға қажеттi материалдық ресурстардың қолайлы көлемi болып табылады.

      12. Ақпарат қауiпсiздiгiнiң мәнi болып табылатын тәуекелдердi бағалау үшiн банктiк ұйымдардың лауазымды тұлғалары мен жауапты бөлiмшелерi ақпарат жүйесiнiң қауiпсiздiгiне төнген қатерге: назар салатын қатердiң сипатына (қатер әсер ететiн спектрi) талдау жүргiзедi. Тәуекелдi талдау процесi екi кезеңнен тұрады:

      1) ақпарат жүйесi объектiлерiн сәйкестендiру;

      2) қатердi анықтау.

      13. Ақпарат жүйесi объектiлерiн сәйкестендiру кезiнде қорғауды қажет ететiн объектiлердiң тiзiмi жасалады:

      1) техникалық құралдар - компьютерлер (серверлер және жұмыс станциялары), перифериялық қондырғылар, сыртқы интерфейстер, кабельдiк жүйе, активтi желiлiк жабдық (өткiзгiштер, маршрутизаторлар және экрандар);

      2) бағдарламалық қамтамасыз ету - операциялық жүйелер (желiлiк, серверлiк және клиенттiк), қолданбалы бағдарламалық қамтамасыз ету, бастапқы мәтiндерi, объект модульдерi, қызметтiк бағдарламалар, желiнi және жекелеген жүйелердi басқару құралдары;

      3) ақпарат - өңделетiн, байланыс арналары бойынша берiлетiн, сақталған (архив, резервтiк көшiрме, мәлiметтер базасы, тiркеу журналы және басқа мәлiметтер);

      4) құжаттама - жалпы жүйелiк және қолданбалы бағдарламалық қамтамасыз етуге, компьютерлiк және телекоммуникациялық жабдыққа және басқа техникалық құралдарға, басқару iс-шараларына арналған;

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

      Сәйкестендiру барысында ақпарат ресурстарына пайдаланушылардың, қызмет көрсететiн қызметкерлердiң және олардың құқықтарының спектрiне тәртiппен кiрудi анықтайтын тiзiм жасалады.

      14. Банктiк ұйымдардың лауазымды тұлғалары қатердi анықтау кезiнде:

      1) қорғауды қажет ететiн объектiлерге бөтен ұйымдар мен тұлғалардың рұқсатсыз кiруiнен;

      2) құпия ақпараттың түрлi сипаттағы өндiрiстiк қызметтi қамтамасыз ететiн және орындау техникалық құралдар арқылы жария болуынан;

      3) пайдаланушылардың, операторлардың, жүйелiк администраторлардың және ақпарат жүйесiне қызмет көрсетушi басқа тұлғалардың байқаусыз жiберген қателерiнiң салдарынан ақпараттың жоғалуынан келетiн болжалды шығынның мөлшерiне бағалау жүргiзуi қажет.

      15. Ақпарат ресурстарына мына жолдармен қатер төнуi мүмкiн:

      1) таратылуы шектелген ақпаратқа рұқсатсыз кiру және алу;

      2) ұйымда немесе құрылымда жұмыс iстейтiн қызметi тiкелей байланысты тұлғаға пара беру;

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

      4) зиян келтiретiн бағдарламалық қамтамасыз ету арқылы деректердi

      және бағдарламалық қамтамасыз етудi бұзу;

      5) таратылуы шектелген ақпаратты (мәлiметтi) авторсыз беру

      және/немесе алу.

      16. Тәуекелдi талдағаннан және қауiпсiздiк саясатын жасағаннан кейiн

      банктiк ұйымның лауазымды тұлғалары тиiмдi және үнемдi қорғау

      механизмдерiне таңдау жүргiзедi және ақпаратты қорғау жоспарын жасайды.

      6-тарау. Ақпаратты қорғау жоспарын iске асыру

      17. Ақпаратты қорғау жоспарына:

      1) ұйымдастырушылық;

      2) бағдарламалық-техникалық шаралар кiредi.

      18. Банктiк ұйымдарда ақпарат жүйелерiнiң тиiмдi қорғау жүйесiн құру үшiн мынадай негiзгi принциптер мен тәсiлдер пайдаланылуы керек:

      1) пайдаланушыларды сәйкестендiру - ақпарат жүйесiн пайдаланушылардың әрқайсысы өзiнiң жеке, айрықша сәйкестендiрушi (тиiстi қосалқы жүйенiң шеңберiнде), немесе бiрнешеуi немесе барлық автоматтандырылған жүйелер үшін айрықша сәйкестендіруші иемденуі тиіс;

      2) кiру рұқсаты бойынша шектеу - пайдаланушыға немесе пайдаланушылар тобына әртүрлi мәлiметке, мәлiметтер тобына немесе ресурстарына кiру рұқсатының тиiстi деңгейi ұсынылады;

      3) қызметкерлердi дайындау - банктiк ұйымдар ақпаратты қорғау жүйесiн басқаруға, пайдалануға немесе қызмет етуiне қатысатын барлық қызметкерлердi мiндеттi кезеңдiк оқытумен қамтамасыз етуi тиiс;

      4) ақпарат жүйесiн орталықтан басқару - банктiк ұйымдардың әрбiр ақпарат жүйесiнде тиiстi өкiммен ақпарат жүйесiнiң қауiпсiздiк басқарушысы тағайындалуы тиiс;

      5) бағдарламалық қамтамасыз етудiң тазалығы - пайдаланылатын қолданбалы және жалпы жүйелiк бағдарламалық қамтамасыз етудiң лицензиясы болуы тиiс, бағдарламалық қамтамасыз ету сертификатталған жеткiзушiлерден алынған немесе Қазақстан Республикасының нормативтiк құқықтық актiлерiне сәйкес сертификатталған болуы керек;

      6) сапалы қызметтi пайдалану - ақпарат жүйелерiн қорғау құралдары мен жүйелерiн жасау және қондыру үшін шарт негiзiнде тек көрсетілген қызмет түрiне лицензиясы (сертификаты) бар мамандандырылған ұйымдар тартылуы тиiс.

      &1. Ақпарат қауiпсiздiгiн қамтамасыз етудiң

      ;

      ұйымдастыру шаралары

      19. Ұйымдастыру шаралары Қазақстан Республикасының нормативтiк құқықтық актiлерiн және банктiк ұйымның iшкi талаптарын сақтауды, ұйым iшiндегi қауiпсiздiк жағдайын қадағалауды, тәртiп бұзу жағдайларында әрекет ету, ұйымдағы өзгерiстердi ескере отырып қорғау шараларын дамытуды қамтамасыз етуi тиiс.

      20. Қауiпсiздiктi қамтамасыз етудi ұйымдастыру шараларына мынадай

      iс-шаралар жатады:

      1) ақпарат жүйесiн нақты қорғау;

      2) ақпарат қауiпсiздiгiне қатысы бар ақпарат жүйелерiнiң жұмысына

      қолдау көрсету;

      3) ақпарат жүйесiнiң деректерiн өзгерту бойынша iс-әрекеттердi

      орындау кезiнде мiндеттердi бөлу және оның қажеттiгiн кем дегенде 2 (екi)

      қызметкердiң растауы (санкция беруi);

      4) әрбiр пайдаланушыға өзiне берiлген лауазымдық мiндеттерiн

      орындауға қажеттi тиiстi кiру құқығын белгiлеу және өзара ауыстыруын

      қамтамасыз ету;

      5) жауапты тұлғаның ақпарат қауiпсiздiгi режимiн бұзуына жол

      бермеу;

      6) қалпына келтiру жұмыстарын жоспарлау.

      21. Нақты қорғау мыналарға бөлiнедi:

      1) кiру рұқсатын нақты басқару;

      2) өртке қарсы қауiпсiздiк шаралары;

      3) қолдау көрсетушi инфрақұрылымды қорғау;

      4) мәлiметтердi орта жолдан ұстап қалудан қорғау, ықшамды жүйелердi

      қорғау.

      22. Ақпарат жүйелерiнiң жұмыс iстеуiне қолдау көрсету жөнiндегi

      iс-шаралар мыналарға бөлiнедi:

      1) пайдаланушыларға қолдау көрсету - ақпарат қауiпсiздiгi мәселелерi бойынша кеңес берудi ұйымдастыру, олардың әдеттегiдей қателерiн анықтау және кең таралған жағдайларға арналған ұсынысы бар ескертпемен қамтамасыз ету;

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

      3) конфигурациялық басқару - бағдарламалық және техникалық конфигурацияға енгiзiлген өзгертулерге бақылау және белгiлеу жасау;

      4) апат және дүлей күштiң басқа жағдайында ақпарат жүйесiн және

      деректердi қалпына келтiру үшiн резервтiк көшiрме жасау;

      5) деректердi тасымалдаушыны басқару - есеп, күтiп ұстау және сақтау

      тәртiбi;

      6) құжаттау - iстiң ағымдағы жағдайының өзектi көрсетiлуi.

      23. Ақпарат жүйесi қауiпсiздiгiнiң режимi бұзылған жағдайда

      банктiк ұйымдардың жауапты тұлғалары:

      1) келтiрiлген зиянды азайту мақсатында шұғыл шараларды орындауға -

      рұқсатсыз кiрген тұлғаны анықтауға және оны қоршауға;

      2) бұзудың жинақталған статистикасына шолу жасауға - келеңсiз

      оқиғаға талдау жасауға, қайталама бұзуды анықтауға, қорғау жүйесiн

      жетiлдiру жөнiнде шаралар әзiрлеуге мiндеттi.

      24. Ақпараттық жүйелердiң жұмыс iстеу қабiлеттiлiгi жоғалғаннан

      кейiн резервтiк көшiру және қалпына келтiру банк ұйымында белгiленген

      талаптармен анықталады.

      &2. Ақпараттық қамтамасыз етудің

      ; бағдарламалық-техникалық шаралары

      25. Банк ұйымын ақпараттық қамтамасыз ету жөнiндегi

      бағдарламалық-техникалық шараларға мына жүйе енуге тиiс:

      1) кiру-алу рұқсатын басқару;

      2) хаттама жасау және техникалық жағдайын тексеру;

      3) деректердi криптографиялық қорғау.

      26. Кiру-алу рұқсатын басқару жүйесi мынадай iс-шаралардың орындалуын

      қамтамасыз етуi тиiс:

      1) деректер, мiндеттер тобының тiзбесiн анықтау және олардың

      құпиялылық деңгейiн белгiлеу;

      2) әрбiр дерек топтарын қорғаудың тәсiлдерi мен iс-шараларын белгiлеу;

      3) ақпарат жүйелерiн пайдаланушылар тобын анықтау және оларды орындайтын қызметтерi бойынша санаттарға бөлу және ақпаратқа кiру рұқсатының деңгейiн белгiлеу;

      4) пайдаланушылардың сәйкестiлiк санаттарының тәртiбiн белгiлеу;

      5) әрбiр "пайдаланушылар санаты - деректер типi" жұптары үшiн кiру рұқсаты санаттарын анықтау;

      6) жүйеге арнайы қондырғылар (жетондар, карталар, электрондық кiлттер) бойынша кiру кезiнде және ұзақтығы сегiз әрiптi-цифрлы символдардан кем емес уақытша әрекет жасайтын парольге пайдаланушыларды сәйкестендiру және дәлме-дәл келтiру;

      7) терминалдарды, персоналды компьютерлердi, компьютерлiк желiлер тораптарын, байланыс арналарын, сыртқы есептеу машиналарын бiрiктiрiлген ерекше қондырғылар бойынша аппараттық сәйкестендiру және дәлме-дәл келтiру;

      8) бағдарламаларды, атаулы дискiлi кеңiстiктердi (логикалық дискiлер томдары, каталогтар, файлдар), жазбаларды, аты және бақылау сомалары бойынша жазбалар жолдарын (парольдер, кiлттер) сәйкестендiру және дәлме-дәл келтiру;

      9) ақпарат ағындарын қауiпсiздiк белгiлерi көмегiмен басқару.

      Мұндайда жинақтағыштар құпиялылығының деңгейi оған жазылатын ақпараттың

      құпиялылық деңгейiнен төмен болмауы тиiс.

      27. Пайдаланушыларға, пайдаланушылар тобына, қызмет көрсетушiлерге

      ақпарат жүйесiнiң ресурстарына кiру рұқсаты құқығын белгiлеген сәттен

      бастап жүйенiң бағдарламалық-техникалық құралдармен жүйеде болып жатқан

      оқиғалар туралы ақпараттарды хаттамалау, жинау және жинақтау жүргiзiледi.

      28. Жүйе оқиғаларын хаттамалау барысында мынадай ақпарат жазылады:

      1) оқиғаның күнi мен уақыты;

      2) оқиғаның бастамашысын сәйкестендiрушi;

      3) оқиғаның түрi;

      4) әрекеттiң нәтижесi (сәттi немесе сәтсiз);

      5) сұраушының көзi (терминалдың атауы);

      6) қозғалған объектiлердiң аттары (ашылатын, көшiрiлетiн немесе

      алынып тасталынатын файлдардың);

      7) деректердi қорғау базасына енгiзiлген өзгерiстердi сипаттау

      (объектi қауiпсiздiгiнiң жаңа белгiсi);

      8) оқиға субъектiлерiнiң және объектiлерiнiң қауiпсiздiк белгiсi.

      29. Хаттамалау нәтижелерi келесiде жүйенiң техникалық жағдайын

      тексеру үшiн қолданылады.

      30. Жинақталған ақпаратты бақылау мақсатында техникалық жағдайын

      тексеру, қауiпсiздiктiң бұзылғанын байқауды жеңiлдету, туындау себептерiн

      анықтау үшiн банктiк ұйымдардың лауазымды тұлғаларымен күнделiктi

      жүргiзiледi.

      31. Ақпарат жүйесiнiң қауiпсiздiгiне қатысты және тексерудi талап

      ететiн оқиғаларға мыналар жатады:

      1) жүйеге кiру (сәттi немесе сәтсiз);

      2) жүйеден шығу;

      3) алыстағы жүйемен байланысу;

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

      тастау, көшiру);

      5) кiру рұқсатының немесе қауiпсiздiктiң басқа белгiлерiнiң деңгейiнiң өзгерiстерi (рұқсат режимi, пайдаланушының ақпарат ресурстарына кiру рұқсатының құқығы).

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

      1) деректердi бөлiнетiн тасымалдаушыларға жазу (әртүрлi пайдаланушылар мен пайдаланушылар топтарымен бiрiгiп қолданылатын);

      2) байланыс арналары бойынша хабарлау;

      3) деректердi ұзақ мерзiмдi сақтайтын кез келген алынатын тасымалдаушыларда жұмыстық, архивтiк және резервтiк көшiрмелердi жасау.

      33. Әртүрлi пайдаланушыларға жататын (пайдаланушылар топтарына) ақпаратты шифрлеу (шифрын ашу) үшiн әртүрлi криптографиялық кiлттердi қолдану қажет.

      34. Ақпаратты шифрлеу (шифрын ашу) операциясын тек тиiстi

      криптографиялық кiлттерге арнайы рұқсаты бар пайдаланушылар немесе

      пайдаланушылар топтары орындауы мүмкiн.

      35. Шифрлеу (шифрын ашу) жөнiндегi жұмыстарды ұйымдастыру және

      бақылауды мына төмендегiлердi орындайтын банктiк ұйымның жауапты адамы

      жүргiзедi:

      1) криптографиялаудың бағдарламалық құралдарын есепке алу, сақтау

      және қолдау;

      2) криптографиялық кiлттердiң генерациясын, кiлттерi бар ақпарат

      тасымалдаушыларды есепке алу, сақтау және беру;

      3) криптографиялық кiлттердiң иелерiнiң тiзiмiн жүргiзу;

      4) криптографиялық кiлттердiң иелерiнiң қауiпсiздiгiн қажеттi

      нұсқаулармен қамтамасыз ету.

      7-тарау. Ақпарат жүйесiн әзiрлеу iсiнiң

      технологиясы мен құжаттауы

      36. Банктiк ұйымдардағы ақпарат жүйелерiн әзiрлеу, енгiзу және қолдау iсi әзiрлеу кезеңдерiн, өзгерiстер енгiзу тәртiбiн, өнеркәсiптiк пайдалануға қабылдау, тесттен өткiзу және iске қосу, барлық кезеңдердi құжаттауды талап етудi қосуы тиiс.

      37. Банктiк ұйымдардағы ақпарат жүйелерiн әзiрлеу, енгiзу және қолдау iсi Қазақстан Республикасы аумағында қолданылып жүрген банктiк ұйымдарда белгiленген ақпарат технологияларының стандарттары мен талаптарына сәйкес орындалады.

      38. Ақпарат жүйелерiн әзiрлеу банктiк ұйымды басқарушы тиiстi органмен бекiтiлген жүйенiң техникалық тапсырмасының негiзiнде және жобалау кезеңдерiне нақпа-нақ сәйкес орындалуы тиiс.

      39. Өндiрiстiк пайдаланудағы ақпарат жүйесiнiң бағдарламалық қамтамасыз етуi өзгерiссiз қалпында ұсталуы тиiс.

      40. Бағдарламалық қамтамасыз етуге және/немесе ақпарат жүйесiнiң деректерiне рұқсат етiлмеген өзгерiстердi болдырмау, қажет болған кезде бағдарламалық қамтамасыз етуге өзгерiстер енгiзу (кемшiлiктердi жою немесе жүйенi толықтыру үшiн) мақсатында өзгерiстер енгiзу ісi және оны құжаттау Қазақстан Республикасы аумағында қолданылып жүрген банктiк ұйымдарда белгiленген ақпарат технологияларының стандарттары мен талаптарына сәйкес орындалады.

      8-тарау. Бақылау және жауапкершiлiк

      41. Қауiпсiздiк саясатын әзiрлеудi бақылау және ереже нормаларын сақтауды банктiк ұйымдардың лауазымды адамдары жүзеге асырады.

      42. Қауiпсiздiк саясатының нақты орындалуы үшiн жауапкершiлiк арнайы тағайындалған жауапты орындаушыларға жүктелуi тиiс.

      43. Банктiк ұйымдардың ақпарат қауiпсiздiгiн сақтау үшін жауапкершiлiктi әдеттегiдей лауазымдық мiндеттерiне сәйкес мына төмендегiлерге жүктеледi:

      1) бiрiншi басшылар;

      2) ақпарат жүйесiн және оларды қорғау жүйесiн жасау және жұмыс iстеу қабiлеттiлiгiн қолдауға, қауiпсiздiк саясатын пайдаланушыларға жеткiзудi және пайдаланушылармен байланыстарды қамтамасыз етушi жауапты бөлiмшелердiң басшылары;

      3) қауiпсiздiк саясатын iске асыруға қажеттi ақпарат жүйесiнiң үздiксiз қызмет етуiн және техникалық шаралардың жүзеге асырылуын қамтамасыз етушi ақпарат жүйесi қауiпсiздiгiн басқарушылар;

      4) қауiпсiздiк саясатына сәйкес ақпарат жүйесiн пайдалануға жауапкершiлiк атқаратын пайдаланушылар қауiпсiздiктiң жекелеген аспектiлерi үшiн жауапты адамдардың өкiмдерiне бағынуға, басшыларды барлық күдiктi жағдайлар туралы хабардар етуге мiндеттi.

      44. Банктiк ұйымдардың лауазымды адамдары:

      1) қауiпсiздiк режимiнiң бұзылуынан мүмкiн болатын шығынның мөлшерiн бағалай және тиiмдi қорғау құралдарын таңдай отырып, ақпарат жүйелерiнiң ұрымтал жерлерiнiң тәуекелдерiн талдауды, қорғауды талап ететiн объектiлердi анықтауды жүргiзедi;

      2) төтенше (шұғыл) жағдайларда қауiпсiздiк шараларына және әрекет ету ережелерiне, вирусқа қарсы бақылауға және жүйеге дұрыс кiруге қатысты мәселелерге (тiркеу кезiнде тек өзiнiң сәйкестендiрушiсiн көрсете отырып) айрықша назар аудару арқылы қызметкерлердi оқытуды қамтамасыз етедi;

      3) кез келген қызметкер басқа бөлiмшеге ауысқан жағдайда, демалыста, iссапарда болғанда немесе жұмыстан шыққан жағдайда бұл жөнiнде ақпарат жүйелерiнiң қауiпсiздiгiне жауапты арнайы тағайындалған жауапты орындаушыларды және басқарушыларды дереу хабарлауды қамтамасыз етедi.

      45. Ақпарат жүйесiнiң қауiпсiздiк басқарушылары қорғау жүйесiн күнделiктi басқару және жұмыс iстеу қабiлеттiлiгiне қолдау көрсету және үздiксiз қызмет ету жөнiндегi жұмыстарды орындайды.

      46. Ақпарат жүйесiнiң қауiпсiздiк басқарушылары:

      1) ақпарат жүйелерiнiң ресурстарына кiру рұқсатына арналған сәйкестендiру және дәлме-дәл келтiру iс-шараларының мiндеттiлiгiн қамтамасыз етуге;

      2) қосарланбаған пайдаланушыларға ақпарат ресурстарына кiру рұқсаты құқығын алуға жол бермеу, пайдаланушыларға тек тiркеу нысандарын толтырғаннан кейiн кiру есiмдерiн және бастапқы парольдердi беруге;

      3) ақпарат жүйесi өңдейтiн ақпараттардың резервтiк көшiрмелерiн орындалуын қайталануын бақылауға;

      4) жүйе ресурстарының қорғалу берiктiлiгiне жоспарлы және жоспардан тыс тексеру жүргiзу, қолдағы қауiпсiздiк саясатының тиiмдiлiгi туралы арнайы тағайындалған жауапты орындаушыларды хабардар етiп және олардың қарауына қорғау жүйесiн жетiлдiру жөнiнде ұсыныс енгiзуге;

      5) корпоративтiк желi жабдығының, оның iшiнде арнайы желi аралық бағдарламалық құралдардың қорғанысын қамтамасыз етуге;

      6) қауiп төндiрушi оқиғаларға жедел және тиiмдi жауап қайтару, қауiптiң бетiн қайтару жөнiнде шаралар қабылдауға және бұзғыштарды анықтау, тiркеу және қорғанысты бұзуға тырысу туралы арнайы тағайындалған жауапты орындаушыларға хабарлауға;

      7) күдiктi жағдайларды байқау, зиянды бағдарламалық қамтамасыз етудiң бар екендiгiн және оның ақпарат жүйесi мен оның құрамдас бөлiктерiнiң жұмысына әсерiн байқау мақсатында ақпарат жүйесiнiң қызмет ету барысын қадағалаудың тексерiлген бағдарламалық-техникалық құралдарын пайдалануға;

      8) күнделiктi жалпы ақпарат жүйесiне және айрықша файлдық серверлерге қатысты тiркеу ақпаратын талдауға;

      9) ақпарат қауiпсiздiгi саласындағы жаңалықтарға шолу жасау, олар жөнiнде пайдаланушыларды және арнайы тағайындалған жауапты орындаушыларды хабардар етуге мiндеттi.

      47. Ақпарат жүйесi қауiпсiздiгiнiң басқарушылары оларға берiлген өкілеттікті өз мақсатына немесе зиянкестік пиғылда қолдануға құқығы жоқ.

      48. Банктiк ұйымдардың бөлiмшелерiнiң қызметкерлерi (пайдаланушылар):

      1) ақпарат жүйесiнiң қауiпсiздiгiн қамтамасыз ететiн iшкi талаптарды бiлуге және сақтауға;

      2) өзiнiң ақпараттарының құпиялылығын және бiртұтастығын қамтамасыз етуге арналған қолдағы тiркелген қорғау тетiктерiн пайдалануға;

      3) ұзындығы сегiзден кем емес әрiптi-цифрлы символдары бар жеке парольдердi таңдауға;

      4) жеке парольдерге басқа адамдар кiре алмауын қамтамасыз етуге;

      5) ақпарат жүйесiнiң қауiпсiздiгiнiң басқарушыларын және/немесе арнайы тағайындалған жауапты орындаушыларды қауiпсiздiктiң бұзылғаны және басқа күдiктi жағдайлар туралы хабардар етуге;

      6) ақпарат жүйелерiнiң ресурстарын қорғауда әлсiз жерлерiн байқаған жағдайда бұл жөнiнде ақпарат жүйесiнiң қауiпсiздiгiнiң басқарушыларын және/немесе арнайы тағайындалған жауапты орындаушыларды дереу хабардар етуге;

      7) дұрыс сәйкестендiрiлген және дәлме-дәл келтiрiлген ақпаратты

      берудi қамтамасыз етуге;

      8) өз компьютерiнiң қатты дискiсiндегi ақпараттың резервтiк

      көшiрмесiн жасауды қамтамасыз етуге;

      9) қауiптi кодтың кiруiнiң алдын алу үшiн оны байқау және жоюға

      арналған шараларды орындауға;

      10) төтенше жағдайларда әрекет ету нормаларын, апат және басқа да

      дүлей күштiң салдарларын жою кезiнде iс-қимылдардың бiрiздiлiгiн орындауға

      мiндеттi.

      49. Банктiк ұйымдардың бөлiмшелерiнiң қызметкерлерi (пайдаланушылар)

      ақпарат жүйесiнiң деректерiмен қосарланбаған жұмыс iстеуге, басқа

      пайдаланушыларға кедергi келтiруге, басқа пайдаланушылардың атынан жұмыс

      iстеуге 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.

 © 2012. Қазақстан Республикасы Әділет министрлігінің «Қазақстан Республикасының Заңнама және құқықтық ақпарат институты» ШЖҚ РМК