Евразийский Банк

Бекіткен:
«Еуразиялық банк» АҚ
Директорлар кеңесі
2023 ж. «12» шілдедегі
№ 60 хаттама

кеңінен пайдалану үшін

АҚПАРАТТЫҚ ҚАУІПСІЗДІК САЯСАТЫ

ІТ

Ақпараттық қауіпсіздік саясаты (бұдан әрі – Саясат) Қазақстан Республикасы (бұдан әрі - ҚР) Ұлттық Банк Басқармасының «Банктердің және банк операцияларының жекелеген түрлерін жүзеге асыратын ұйымдардың ақпараттық қауіпсіздігін қамтамасыз етуге қойылатын талаптарды бекіту туралы» 2018 жылғы 27 наурыздағы № 48 Қаулысына (бұдан әрі - №48 Қаулы), Қазақстан Республикасы Үкіметінің «Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарды бекіту туралы» 2016 жылғы 20 желтоқсандағы № 832 Қаулысына, СТ РК ISO/IEC 27001-2015 «Ақпараттық технология. Қауіпсіздікті қамтамасыз етудің әдістері мен құралдары. Ақпараттық қауіпсіздік менеджмент жүйелері. Талаптар», СТ РК ISO/IEC 27002-2015 «Ақпараттық технология. Қауіпсіздікті қамтамасыз етудің әдістері мен құралдары. Ақпаратты қорғауды басқару құралдары бойынша қағидалар жинағы» және «Еуразиялық банк» АҚ (бұдан әрі – Банк) ішкі нормативтік құжаттарына (бұдан әрі – ІНҚ), оның ішінде Ішкі нормативтік реттеу саясатына сәйкес әзірленді.

1-Бөлім ЖАЛПЫ ЕРЕЖЕЛЕР

1. Саясат ақпараттық қауіпсіздік (бұдан әрі - АҚ) саласындағы басты қағидаттар мен бағыттарды айқындау мақсатында әзірленген және Банк иеленушісі және пайдаланушы болып табылатын барлық бизнес-процестерді, ақпараттық жүйелер (бұдан әрі - АЖ) мен құжаттарды қамтиды.

2. Осы Саясат келесілерді айқындайды:

1) ақпараттық қауіпсіздікті басқару жүйесін (бұдан әрі - АҚБЖ) құрудың мақсаттарын, міндеттері және негізгі принциптерін;

2) АҚБЖ қолданылу саласы мен қатысушыларын;

3) АҚ басқаруға қойылатын талаптарды, оның ішінде:

– Банктің ақпараттық жүйелерінде құрылатын, сақталатын және өңделетін ақпаратқа қол жеткізуге қойылатын талаптар, ақпарат пен оған қолжетімділіктің мониторингі;

– АҚ қамтамасыз ету қызметінің және қауіп-қатерлерді анықтау және талдау, шабуылдарға қарсы іс-қимыл және АҚ инциденттерін тергеу жөніндегі іс-шаралар мониторингін жүзеге асыруға қойылатын талаптар;

– АҚ инциденттері (оқиғалары) туралы ақпаратты жинау, шоғырландыру және сақтауды жүзеге асыруға қойылатын талаптар;

– АҚ инциденттері туралы ақпаратқа талдау жүргізуге қойылатын талаптар;

– АҚ қамтамасыз ету үшін Банк қызметкерлерінің өздеріне жүктелген функционалдық міндеттерін орындау кезіндегі жауапкершілігі.

3. Банк АҚБЖ құруды және оның жұмыс істеуін қамтамасыз етеді, ол АҚ қамтамасыз ету процесін басқаруға арналған Банктің жалпы басқару жүйесінің бір бөлігі болып табылады.

4. АҚБЖ мақсаты Банктің бизнес-процестері үшін ықтимал залалдың ең төменгі деңгейде болуына жол беретін Банктің ақпараттық активтерін қорғауды қамтамасыз ету, ақпараттың қауіпсіздігіне қатер төндіретін оқиғалардан болатын залалды барынша азайту болып табылады.

5. АҚБЖ-ның Банктегі басты міндеттері болып табылатындар:

– ақпараттық активтерді, оларды сақталатын және өңделетін ақпараттың сынилығының жоғары деңгейі негізінде оларды сыни және сыни емес деп бөлу арқылы санаттау;

– Банктің ақпараттық активтеріндегі АҚ ықтимал қатерлерін және осалдықтарын уақтылы анықтау;

– Банктің ақпараттық активтеріндегі анықталған АҚ ықтимал қатерлері мен осалдықтары негізінде АҚ тәуекелдерін (қауіптерін) бағалауды жүйелі түрде жүргізу;

– анықталған қатерлерді болдырмау немесе азайту;

– АҚ қамтамасыз етудің дәлелденген, экономикалық тұрғыда тиімді ұйымдастырушылық және техникалық шараларын қолдану;

– АҚ оқиғаларының алдын алу немесе олардың салдарын азайту;

– АҚ саласындағы қолданыстағы заңнаманың және реттеушілердің қолданатын талаптарын анықтау, осы талаптарға сай болуға қол жеткізу;

– АҚ қамтамасыз ету мәселелері бойынша қызметкерлердің жауапкершілігін белгілеу, оларды оқыту және АҚ жағынан білімдерін арттыру;

– АҚБЖ процестерінің тиімділігінің мониторингі.

6. Саясатта ҚР заңнамасында, оның ішінде №48 Қаулыда, сондай-ақ электрондық анықтамалықта қарастырылған негізгі түсініктер қолданылады.

2-Бөлім ЕРЕКШЕ ЕРЕЖЕЛЕР

1-Тарау АҚБЖ қолдану саласы

7. Банк анықтаған ақпараттық қауіпсіздік менеджмент жүйесінің (бұдан әрі - АҚМЖ) қолданылу аясы мен шекарасына кіретіндер:

– Банктің барлық бизнес-процестері, оның ішінде клиенттер мен Банк контрагенттерінің ақпаратпен алмасу процестері;

– Банктің барлық қызметкерлері, сондай-ақ жұмыстарды Банктің инфрақұрылымында орындау кезінде, не Банк берген ақпаратты өңдеу кезінде контрагенттердің қызметкерлері;

– Банктің бизнес-процестері жұмыс істеу нәтижесінде жинаған, өңдейтін және сақтайтын барлық ақпарат, оның ішінде қауіпсіздікті қамтамасыз ету бойынша контрагенттермен ақпарат алмасу шеңберінде жауапкершілік үшінші тұлғаға берілген ақпарат.

8. Ақпараттық және коммуникациялық технологиялар үшін АҚМЖ -ның Банк анықтаған қолданылу аясы мен шекарасына қауіпсіздікті қамтамасыз ету бойынша жауапкершілік үшінші тарапқа берілген ақпараттық активтерді қоса алғанда, Банктің бизнес-процестерінің жұмыс істеуіне қажетті Банктің барлық ақпараттық активтері кіреді (серверлік қуаттарды деректерді өңдеудің басқа орталықтарына орналастыру, деректерді өңдеу және/немесе сақтаудың сыртқы сервистерін пайдалану).

9. АҚМЖ-ның Банк анықтаған физикалық қолданылу аясы мен шекарасына Банктің және/немесе оның филиалдарының (бөлімшелерінің) әкімшілік үй-жайлары мен ол (олар) пайдаланатын әртүрлі мақсаттағы, оларда орналасқан жабдықтары не іргелес аумағы бар өзге де үй-жайлар кіреді (Банктің белгіленген жауапкершілік аймағы болған кезде және/немесе шегінде)

10. Саясат онда айтылған ақпаратты талдау және өзектендіру мақсатында жылына кем дегенде бір рет қайта қаралады.

2-Тарау АҚБЖ құру қағидаттары

11. Банкте АҚБЖ құру және оның жұмыс істеуі төмендегі негізгі қағидаттарға сәйкес жүзеге асырылуы тиіс:

– заңдылық – АҚ қамтамасыз ету үшін қолданылатын кез келген әрекеттер ҚР қолданыстағы заңнамасы және Банктің ІНҚ негізінде, Банктің ақпаратты қорғау объектілеріне теріс әсерлерді анықтау, алдын алу, оқшаулау және жолын кесудің заңмен рұқсат етілген барлық әдістерді пайдалана отырып, жүзеге асырылады;

– бизнеске бағдарлану – ақпараттық қауіпсіздік Банктегі бизнес-процестерді қолдау процесі ретінде қарастырылады. АҚ қамтамасыз ету бойынша кез келген шаралар Банктің қызметіне айтарлықтай кедергі келтірмеуі тиіс;

– үздіксіздік – ақпаратты қорғау жүйелерін басқару құралдарын қолдану, Банкте ақпаратты қорғауды қамтамасыз ету бойынша кез келген шараларды іске асыру Банкте ағымдағы бизнес-процестерді үзбей немесе тоқтатпай жүзеге асырылуы тиіс;

– кешенділік – ақпараттық ресурстардың бүкіл өмірлік циклі ішінде, оларды пайдаланудың барлық технологиялық кезеңдерінде және жұмыс істеудің барлық режимдерінде қауіпсіздігін қамтамасыз ету;

– негізділік және экономикалық тиімділік – пайдаланылатын мүмкіндіктер мен қорғаныш құралдары ғылым мен техниканың тиісті даму деңгейінде іске асырылуы тиіс, тапсырылған қауіпсіздік деңгейі тарапынан негізделген және нормаларға қойылатын талаптарға сәйкес болуы тиіс;

– басымдық - Банктің барлық ақпараттық ресурстарын оларда сақталатын және өңделетін ақпараттың, сондай-ақ ақпараттық қауіпсіздікке төнетін ықтимал қауіптердің ең жоғары сыни деңгейі негізінде сыни дәрежесі бойынша санатқа жатқызу (саралау);

– қажетті білім және артықшылықтардың ең төменгі деңгейі – пайдаланушы өзінің өкілеттігі шеңберінде қызметтік міндеттерін орындау үшін қажет болатын деректерге ғана артықшылықтардың ең төменгі деңгейі мен қолжетімділік (кіруге рұқсат) алады;

– мамандану – техникалық құралдарды пайдалануды және АҚ шараларын іске асыруды Банктің кәсіби даярланған қызметкерлері жүзеге асырулары тиіс;

– ақпараттандыру және дербес жауапкершілік – Банктің барлық деңгейдегі басшылары мен қызметкерлері АҚ барлық талаптары туралы хабардар болуы және осы талаптардың орындалуына және АҚ белгіленген шараларының сақталуына дербес жауапты болулары тиіс;

– өзара әрекет және үйлестіру – АҚ шаралары Банктің тиісті құрылымдық бөлімшелерінің өзара байланысы, қойылған мақсаттарға жету үшін олардың күш-жігерін үйлестіру, сондай-ақ сыртқы ұйымдармен, кәсіби қауымдастықтармен және қоғамдармен, мемлекеттік органдармен, заңды және жеке тұлғалармен қажетті байланыс орнату негізінде жүзеге асырылады;

– растау – маңызды құжаттама және барлық жазбалар – АҚ бойынша талаптардың орындалуын және оны ұйымдастыру жүйесінің тиімділігін растаушы құжаттар жедел қолжетімділік және қалпына келтіру мүмкіндігімен құрылуы және сақталуы тиіс.

3-Тарау АҚБЖ қатысушыларының функциялары

12. Банктің ақпараттық қауіпсіздігін басқару жүйесіне негізгі қатысушылар болып табылатындар:

1) Директорлар кеңесі;
2) Басқарма;
3) АҚ комитеті (бұдан әрі – УАО (Уәкілетті Алқалы Орган));
4) АҚ бөлімшесі;
5) ақпараттық технологиялар бөлімшесі;
6) қауіпсіздік жөніндегі бөлімше;
7) қызметкерлермен жұмыс жүргізу жөніндегі бөлімше;
8) заң бөлімшесі;
9) комплаенс және ішкі бақылау бөлімшесі;
10) ішкі аудит бөлімшесі;
11) АТ және АҚ тәуекелдерін басқару бөлімшесі.

13. Директорлар кеңесі қорғалатын ақпараттар, оның ішінде қызметтік, коммерциялық немесе заңмен қорғалатын өзге де құпияны құрайтын мәліметтер туралы ақпаратты (бұдан әрі - қорғалатын ақпарат) қоса алғанда тізбесін және қорғалатын ақпаратпен жұмыс істеу тәртібін бекітеді.

14. Басқарма Төрағасы АҚ тиісті деңгейін ұйымдастыру және ұстану үшін стратегиялық жоспарлауды, Банктің барлық бөлімшелерінің қызметін үйлестіруді жүзеге асырады.

15. Банк Басқармасы ақпараттық қауіпсіздікті басқару процесін реттейтін, қайта қарау тәртібі мен кезеңділігі Ішкі нормативтік құжаттарды басқару жөніндегі нұсқаулықта айқындалатын ішкі құжаттарды бекітеді.

16. Банк УАО құрады, оның құрамына АҚ бөлімшесінің, АҚ тәуекелдерін басқару бөлімшесінің, ақпараттық технологиялар бөлімшесінің өкілдері, сондай-ақ қажет болған жағдайда Банктің басқа бөлімшелерінің өкілдері кіреді. УАО басшысы етіп Банк Басқармасының Төрағасы не Банк Басқармасы Төрағасының АҚ бойынша бөлімшенің қызметіне жетекшілік ететін орынбасары тағайындалады.

17. УАО ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі қызметке және қауіптерді анықтау және талдау, шабуылдарға қарсы іс-қимыл және ақпараттық қауіпсіздік оқыс оқиғаларын тергеу жөніндегі іс-шараларға мерзімді мониторингті жылына кем дегенде бір рет жүзеге асырады. АҚ қамтамасыз ету жөніндегі қызметті, қатерлерді анықтау және талдау, сондай-ақ шабуылдарға қарсы іс-қимыл жөніндегі іс-шараларға мониторинг жасау процесі анықталған қауіптердің, қабылданған шаралардың және АҚ оқиғаларының саны бойынша АҚ бөлімшесі ұсынған деректер негізінде қауіптерді анықтау, талдау және шабуылдарға қарсы іс-қимыл жөніндегі есепті қамтуы тиіс. АҚ оқыс оқиғаларын зерттеу жөніндегі іс-шаралардың мониторингіне оқыс оқиғалардың салдарларын бағалау, себептері мен алдын алу іс-шараларының жоспарларын көрсету, не АҚ оқыс оқиғаларының әсерін азайту кіреді.

18. АҚ бөлімшесінің басшысы АҚ қауіпсіздік саласындағы құжатталған стандарттар мен рәсімдерді әзірлеуді, енгізуді және жетілдіруді қамтамасыз етеді.

19. АҚ бөлімшесі АҚ оқиғаларына және АҚ оқыс оқиғаларын басқаруға мониторинг жүргізеді, оның шеңберінде мониторингке жататын АҚ оқиғаларының тізбесі, оқиғалардың көздері, кезеңділігі, мониторинг ережелері мен олардың әдістері анықталады. Мониторинг жүргізетін АҚ бөлімшесі АҚ

оқыс оқиғаларын анықтаған жағдайда, қосымша бақылау енгізуге, бизнес-процесті ішінара немесе толық тоқтатуға құқылы.

20. АҚ бөлімшесі АҚ оқыс оқиғалары туралы ақпараттың талдауын уақытында жүргізуді қамтамасыз етеді, оған АҚ оқыс оқиғалары орын алған жағдайдың мән-жайын ашу кіруі тиіс, соның арқасында АҚ оқыс оқиғаларын жүзеге асыру, АҚ тәуекелдерін басқару жөніндегі бөлімшемен өзара әрекетте болу мүмкін болады, қажет болған жағдайда, қорғаныш шараларын енгізу жөнінде ұсыныстар қалыптастыру қоса кіреді.

21. Ақпараттық технологиялар бөлімшесі Банктің ІНҚ-на сәйкес ақпараттық инфрақұрылымның, үздіксіз жұмыс істеуі, Банктің ақпараттық жүйесінің деректерінің (ақпаратты резервтеу және (немесе) мұрағаттауды және резервтік көшірмелерді қоса) құпиялылығы, тұтастығы мен қолжетімділігі бойынша белгіленген талаптардың орындалуын қамтамасыз етеді, сондай-ақ АЖ таңдау, енгізу, әзірлеу және тестілеуден өткізу кезінде АҚ талаптарының сақталуын қамтамасыз етеді.

22. АҚ тәуекелдерін басқару бөлімшесі ақпараттық активтерді оларда сақталатын және өңделетін ақпараттың сынылығының ең жоғары деңгейі негізінде оларды сыни және сыни емес деп бөлу арқылы санаттауды жүзеге асырады.

23. Қауіпсіздік жөніндегі бөлімше физикалық және техникалық қауіпсіздік шараларын іске асырады, оның ішінде объектіге өткізу және объектішілік режимді ұйымдастырады, сондай-ақ Банк қызметкерлерін жұмысқа қабылдаған және босатқан кезде АҚ қатерлерінің туындау тәуекелін азайтуға бағытталған, профилактикалық (алдын алу) шараларын өткізеді.

24. Қызметкерлермен жұмыс жүргізу бөлімшесі банк қызметкерлерінің, сондай-ақ қызмет көрсету туралы шарт бойынша жұмысқа тартылған тұлғалардың, тағылымдамадан өтушілердің, практиканттардың құпия ақпаратты жария етпеу туралы міндеттемелерге қол қоюын қамтамасыз етеді, сондай-ақ Банк қызметкерлерінің АҚ саласында хабардар болуларын арттыру процесін ұйымдастыруға қатысады.

25. Заң бөлімшесі Банктің АҚ қамтамасыз ету мәселелері бойынша ІНҚ мен ішкі құжаттарына Ішкі нормативтік құжаттарды басқару жөніндегі нұсқаулыққа сәйкестік тұрғысына құқықтық сараптама жүргізеді.

26. Комплаенс- бақылау бөлімшесі Банктің заң бөлімшесімен бірлесіп, қорғалатын ақпараттар тізбесіне кіруі тиіс ақпараттың түрлерін анықтайды.

27. Ішкі аудит бөлімшесі аудиторлық тексерулер жүргізу кезінде Банктің АҚБЖ жай-күйіне бағалау жүргізеді.

28. Банк Басқармасы ақпараттық қауіпсіздіктің тиісті деңгейін ұйымдастыру және ұстап тұру үшін Банктің барлық бөлімшелерінің қызметтерін үйлестіруді жүзеге асырады және Саясаттың ережелерін іске асыруда жауапкершілікте болады.

29. Банк Басқармасы ақпараттық технологиялар бөлімшесімен және ақпараттық қауіпсіздік бөлімшесімен бірлесіп, нақты нұсқаулар, көрсетілген міндеттемелер, нақты міндеттер қою арқылы және АҚ қамтамасыз ету жөніндегі міндеттері туралы қызметкерлерді хабардар ету арқылы АЖ және Банктің электрондық ақпараттық ресурстарын (бұдан әрі - ЭАР) қолдау жөніндегі іс-шаралар кешенін белсенді түрде іске асыруы тиіс.

30. АҚ үйлестіру пайдаланушылардың, әкімшілердің, қолданбалы бағдарламалық жасақтаманы әзірлеушілердің және кадрлық ресурстар, ақпараттық технологиялар және тәуекелдерді басқару сияқты салалардағы білікті мамандардың өзара байланысы мен ынтымақтастығын қамтуы тиіс.

Бұл қызмет:

1) АҚ қамтамасыз ету жөніндегі шаралардың орындалу сәйкестігін қамтамасыз етуі;

2) Саясатқа сәйкес болмаған жағдайда, АҚ қамтамасыз ету жөніндегі іс- шараларды анықтау;

3) АҚ қамтамасыз етудің әдіснамасын және процестерін, мысалы ақпараттың тәуекелін, жіктелуін бағалауды бекітуі;

4) АҚ қатерлерінің барлық өзгерістерін және ақпараттың осалдылық дәрежесін және ақпаратты АҚ қатерлеріне өңдеу құралдарын сәйкестендіруі;

5) қабылданатын шешімдердің барабарлығын бағалау және АҚ бақылау шараларын іске асыруды үйлестіруі;

6) пайдаланушылардың АҚ саласындағы дайындық деңгейін және ол туралы хабардар болуын (білуді) арттыруы;

7) мониторингтен және АҚ бойынша оқыс оқиғаларды қараудан алынған ақпаратты бағалау және анықталған АҚ оқыс оқиғаларына жауап ретінде тиісті іс-шаралар ұсынуды.

31. Банк Басқармасы нақты басқаруды және АҚБЖ жетілдіру бойынша бастамаларға қолдау көрсетуді қамтамасыз етуі тиіс.

32. Банк Басқармасы АҚ бақылау шараларын үйлестіруді қамтамасыз етуі және АҚ қамтамасыз ету үшін ресурстар беруі тиіс.

33. Банк Басқармасы АҚ бойынша нақты рөлдер мен міндеттерді бөлуді бекітуі тиіс.

34. Банк Басқармасы АЖ-ның ақпараттық қауіпсіздікке байланысты қолданыстағы талаптарға, заңнама талаптарына, оның ішінде зияткерлік меншік құқықтарын сақтау жөніндегі талаптарға сәйкес екендігі туралы өзіне міндеттеме алады.

35. АҚ мәселелері бойынша оқытуға және хабардар болуға қойылатын талаптар:

1) пайдаланушылар, ақпараттық технологиялар бөлімшелерінің қызметкерлері Саясатпен танысулары тиіс;

2) Банктің АҚ үшін жауапты қызметкері АҚ жөнінде бастапқы нұсқаулық өткізуі тиіс;

3) АЖ және ЭАР жұмысын қамтамасыз етуші ақпараттық технологиялар бөлімшелерінің қызметкерлері АҚ талаптарын сақтау жөнінде жүйелі түрде нұсқаулықтан өтулері тиіс;

4) АҚ үшін жауапты тұлға қажеттілігіне қарай, 3 (үш) жылда 1 (бір) рет ақпараттық қауіпсіздік бойынша біліктілікті арттыру курсынан өтуі тиіс;

36. Банк ақпараттық қауіпсіздік бөлімшелерінің, ақпараттық қауіпсіздік тәуекелдерін басқару және ішкі аудит жөніндегі бөлімшелердің қызметкерлерінің біліктілігін арттыруды сырттан оқыту жүргізу арқылы қамтамасыз етеді (курстарға, семинарларға қатысу - әрбір қызметкер үшін 3 (үш) жылда кемінде 1 (бір) рет).

37. Саясатта қамтылған талаптардың орындалуын қамтамасыз ету мақсатында оны үшінші тараптардың сақтауын қамтамасыз ету қажет. Сондықтан, тиісті жағдайларда, сырттағы заңды және жеке тұлғалармен жасалатын барлық шарттар, Саясаттың талаптарын сақтау және АҚ қамтамасыз ету туралы талаптарды қамтуы тиіс. Банктің АЖ және ЭАР-да қамтылған деректерімен контрагенттердің байланысын көздейтін барлық қызмет, Саясатта баяндалған нормативтік талаптарға сәйкес жүзеге асырылуы тиіс. Аталған талап барлық контрагенттерге қатысты қолданылады.

4-Тарау АҚ басқару бойынша талаптар

38. Банктің ақпараттық активтерінің құпиялылығын, тұтастығын және қолжетімділігін қорғаудың негізгі шаралары болып табылатындар:

– желілік қауіпсіздікті басқару;
- осалдылықты және қауіпсіздік саясатын басқару;
– түпкілікті құрылғылардың қауіпсіздігін басқару;
– сәйкестендіруді және қолжетімділікті басқару;
– АҚ оқыс оқиғаларын басқару;
– криптографиялық қорғау құралдарын басқару;
– вирусқа қарсы қорғау құралдарын басқару;
– ақпараттық активтердің физикалық қауіпсіздігін қамтамасыз ету;
– контрагенттермен өзара әрекет кезінде қауіпсіздікті қамтамасыз ету;
– қызметкерлерді АҚ мәселесінде оқыту және білімдерін арттыру;
– интернет-ресурстардың қауіпсіздігін қамтамасыз ету.

39. Банктің АҚ ұйымдастыру іс-шараларына қатысты талап етілетіндер:

1) АҚ басқаруға және АҚ қамтамасыз ету бойынша шараларды әзірлеуге жауапты АҚ бойынша бөлімше құру және оның жұмыс істеуі;

2) АҚ үшін жауапты жұмысшылар мен қызметкерлердің саны мен оларға жүктелген тапсырмалардың деңгейіне олардың біліктіліктерінің сәйкес болуы;

3) АҚ-ға қатысты қолданыстағы құжаттамаларды бекіту және жүйелі түрде қайта қарау (құжатталған ережелердің, рәсімдердің, практикалық әдістердің немесе нұсқаулықтардың төрт деңгейлі жүйесі), сондай-ақ олармен Банктің жұмысшылары мен қызметкерлерін, олардың міндеттемелеріне қатысты бөлігімен жылына кем дегенде бір рет таныстыру.

4) АҚ тәуекелдерді бағалау негізінде АҚ қамтамасыз ету бойынша шараларды жоспарлау.

40. Ақпараттық ресурстардың қауіпсіздігін қамтамасыз ету міндеттері келесі әдістермен шешіледі:

– минималды жеткіліктілік қағидаттарына негізделген деректер мен артықшылықтарды азайту;
– өкілеттіктерді бөлу және бақылауды қайталау;

– құпия ақпаратты сақтау және өңдеудің бірыңғай тәртібін бекіту;

– АҚ-ға қатысы бар ақпараттық жүйелерді жұмысқа қабілетті күйде ұстау;

– АҚ режимін бұзушылыққа жауапты тұлғалардың көңіл бөлуі (жауап беруі);

– Банктің және контрагенттің қызметкерлерінен АҚ талаптарын сақтау және құпия ақпаратты сақтауды қамтамасыз ету міндеттемелерін алу;

Банктің қызметкерлерін АҚ саласында кезеңімен оқыту және біліктіліктерін арттыру.

41. Банк ақпаратты Банктің ақпараттық жүйесінде құру, жинау, сақтау және өңдеу бойынша ішкі рәсімдерді әзірлейді. Банк ақпарат құру, сақтау және өңдеу және оған қолжетімділік процестеріне мониторингті АЖ тетіктерінің және қауіпсіздікті қамтамасыз ету техникалық құралдарының көмегімен жүзеге асырады. Банктің АЖ-да құрылған, сақталған және өңделген ақпаратқа қолжетімділік қызметкерлерге артықшылықтың ең төменгі деңгейі қағидатына сәйкес олардың қызметтік міндеттеріне сәйкес беріледі.

42. Мониторинг жүргізілуі тиіс АҚ оқиғаларының тізбесі, оқиғаның шығу көзі, мониторинг кезеңділігі, ережелері мен олардың әдістерін АҚ бөлімшесі қолда бар статистика мен мониторинг тиімділігін ескере отырып, жылына кем дегенде бір рет қайта қарайды.

43. АҚ оқыс оқиғаларын басқару тәртібі Банктің тиісті ІНҚ-мен анықталады және ол АҚ оқыс оқиғалары туралы ақпаратты шоғырландыру, жүйелеу және сақтау жөніндегі ережелерді, АҚ оқиғаларын АҚ оқыс оқиғаларына жатқызу тәртібін, кейіннен АҚ оқиғаларына талдау жасауды және болған АҚ оқыс оқиға туралы ақпараттандыруды қамтиды.

44. АҚ оқыс оқиғалары туралы ақпаратты шоғырландыру, жүйелеу және сақтау процесі №48 Қаулыда көзделген оқыс оқиғаға талдауды жүзеге асыру, қызметтік тексерулер жүргізу және есептілікті қалыптастыру үшін оқыс оқиға туралы жеткілікті деректердің тұтастығын, қолжетімділігін және құпиялылығын, сондай-ақ толықтығын қамтамасыз етуге тиіс.

45. АЖ бизнес- иеленушілері өнімдер мен қызметтерді құру, енгізу, өзгерту, клиенттерге ұсыну кезінде АҚ-ға қойылатын талаптардың сақталуына жауап береді, сондай-ақ АЖ-ға қол жеткізу матрицаларын қалыптастырады және өзектілігін (маңыздылығын) сақтайды.

46. Банктің құрылымдық бөлімшелерінің басшылары қызметкерлерді АҚ-ға қойылатын талаптарды қамтитын Банктің ІНҚ-мен таныстыруды қамтамасыз етеді, сондай-ақ бағыныста бөлімшелерде АҚ талаптарының орындалуын қамтамасыз етуге, жаңа өнімдерді, қызметтерді, бизнес-қосымшаларды, бизнес-процестер мен технологияларды әзірлеу кезінде қорғау шараларын енгізуге жауапты.

3-Бөлім ҚОРЫТЫНДЫ ЕРЕЖЕЛЕР

47. Саясаттың талаптарын орындамағаны/тиісті орындамағаны үшін, сондай-ақ өздеріне жүктелген қызметтік міндеттемелерін орындау кезінде АҚ қамтамасыз ету жауапкершілігі Банктің барлық қызметкерлеріне жүктеледі.

48. Саясатта белгіленген талаптардың орындалуын бақылау УАО-ға жүктеледі.

49. Саясат ІНҚ Дерекқорына өзгерістер енгізілгеннен соң келесі жұмыс күні күшіне енеді және Банктің барлық қызметкерлерінің қолдануына және басшылыққа алуына жалпы міндет болып табылады, сондай-ақ Банктің ақпараттық активтеріне қолжетімділігі бар үшінші тұлғалардың мәліметіне жеткізіледі.

50. Саясатта реттелмеген мәселелер Қазақстан Республикасының заңнамасына және Банктің ІНҚ-ға сәйкес шешіледі.

АТ- қауіпсіздігі қызметі директоры
Э.А. Рустамов

ӨЗГЕРІСТЕР МЕН ТОЛЫҚТЫРУЛАР ПАРАҒЫ

№ р/с	Хаттама нөмірі	Хаттама жасалған күн	Күшіне енген күні	Өзгерістердің бастамашысы
1.				
2.				