Евразийский Банк

кеңінен пайдалану үшін

АҚПАРАТТЫҚ ҚАУІПСІЗДІК САЯСАТЫ

СТ

Ақпараттық қауіпсіздік саясаты (бұдан әрі – Саясат) Қазақстан Республикасы Ұлттық Банк Басқармасының (бұдан әрі – ҚР) «Банктердің, 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) және «Еуразиялық банк» АҚ-ның (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 саласындағы басты қағидаттар мен бағыттарды айқындау мақсатында әзірленген және Банк иеленушісі және пайдаланушы болып табылатын барлық бизнес-процестерді, ақпараттық жүйелер мен құжаттарды қамтиды.

2. Банктің ақпараттық активтерін қорғауды қамтамасыз ету және ақпараттың қауіпсіздігіне қатер төндіретін оқиғалардан болатын залалды азайту Банктегі ақпараттық қауіпсіздікті басқару бойынша қызметтің мақсаты болып табылады.

3. Банктегі ақпараттық қауіпсіздікті басқару бойынша қызметтің 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 ақпараттық қауіпсіздіктің ықтимал қатерлерін және осалдықтарын уақтылы анықтау;

- анықталған қатерлерді болдырмау немесе азайту;

- ақпараттық қауіпсіздік оқиғаларының алдын алу немесе олардың салдарын азайту.

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

– желілік қауіпсіздікті басқару;
- осалдылықты және қауіпсіздік саясатын басқару;
– соңғы (түпкілікті) құрылғылардың қауіпсіздігін басқару;
– сәйкестендіруді және қолжетімділікті басқару;
– ақпараттық қауіпсіздік 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.

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

2-Бөлім ЕРЕКШЕ ЕРЕЖЕЛЕР

5-1. Банк ақпараттық қауіпсіздікті басқару жүйесін құруды және оның жұмыс істеуін қамтамасыз етеді, ол ақпараттық қауіпсіздікті қамтамасыз ету процесін басқаруға арналған банктің жалпы жүйесін басқарудың бір бөлігі болып табылады.

5-2. Ақпараттық қауіпсіздікті басқару жүйесі банктің бизнес-процестері үшін ықтимал залалдың ең төменгі деңгейіне жол беретін банктің ақпараттық активтерін қорғауды қамтамасыз етеді.

6. Банкте ақпараттық қауіпсіздікті басқару жүйесін құру және оның жұмыс істеуі келесі негізгі қағидаттарға сәйкес жүзеге асырылуы тиіс:

– заңдылық – ақпараттық қауіпсіздікті 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 ретінде қарастырылады Ақпараттық қауіпсіздікті 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 (рейтинг);

– 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 ақпараттық қауіпсіздік шараларын іске асыруды Банктің кәсіби даярланған қызметкерлері жүзеге асырулары тиіс;

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

– өзара әрекет және үйлестіру – ақпараттық қауіпсіздік 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 – ақпараттық қауіпсіздік бойынша талаптардың орындалуын және оны ұйымдастыру жүйесінің тиімділігін растаушы құжаттар жедел қолжетімділік және қалпына келтіру мүмкіндігімен құрылуы және сақталуы тиіс.

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

7-1. Банктің ақпараттық қауіпсіздігін басқару жүйесіне қатысушылар болып табылатындар:

1) Директорлар кеңесі;
2) Басқарма;
3) Ақпараттық қауіпсіздік комитеті (бұдан әрі – УАО (Уәкілетті алқалы орган));
4) ақпараттық қауіпсіздік бөлімшесі;
5) ақпараттық технологиялар бөлімшесі;
6) қауіпсіздік жөніндегі бөлімше;
7) қызметкерлермен жұмыс жүргізу жөніндегі бөлімше;
8) банктік қызметті және корпоративтік мәселелерді құқықтық сүйемелдеу бөлімшесі;
9) комплаенс және ішкі бақылау бөлімшесі;
10) ішкі аудит бөлімшесі;
11) АТ және ақпараттық қауіпсіздік тәуекелдерін басқару бөлімшесі.

7-2. 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.

7-3. Басқарма ақпараттық қауіпсіздікті басқару процесін реттейтін, қайта қарау тәртібі мен кезеңділігі Ішкі нормативтік құжаттарды басқару жөніндегі нұсқаулықта айқындалалатын ішкі құжаттарды бекітеді.

8. Банк УАО құрады, оның құрамына ақпараттық қауіпсіздік бөлімшесінің, ақпараттық қауіпсіздік 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 ақпараттық қауіпсіздік бөлімшесінің қызметіне жетекшілік ететін орынбасары тағайындалады.

9. 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. Ақпараттық қауіпсіздікті 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 ақпараттық қауіпсіздік оқиғаларының саны бойынша ақпараттық қауіпсіздік бөлімшесі ұсынған деректер негізінде қауіптерді анықтау, талдау және шабуылдарға қарсы іс-қимыл жөніндегі есепті қамтуы тиіс. Ақпараттық қауіпсіздік оқыс оқиғаларын зерттеу жөніндегі іс-шаралардың мониторингіне оқыс оқиғалардың салдарларын бағалау, себептері мен алдын алу іс-шараларының жоспарларын көрсету, не ақпараттық қауіпсіздік оқыс оқиғаларының әсерін азайту кіреді.

10. Ақпараттық қауіпсіздік бөлімшесі ақпараттық қауіпсіздік оқиғаларына, мониторинг жүргізілуі тиіс ақпараттық қауіпсіздік оқиғаларының тізбесі, оқиғаның шығу көзі, мониторинг кезеңділігі, ережелері мен олардың әдістері анықталатын ақпараттық қауіпсіздік оқыс оқиғаларын басқаруға мониторинг жүргізеді.

Мониторинг жүргізетін ақпараттық қауіпсіздік бөлімшесі ақпараттық қауіпсіздік оқыс оқиғаларын анықтаған жағдайда, қосымша бақылау енгізуге, бизнес-процесті ішінара немесе толық тоқтатуға құқылы.

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

12. Ақпараттық қауіпсіздік оқыс оқиғаларын басқару тәртібі Банктің тиісті ІНҚ-мен анықталады және ақпараттық қауіпсіздік оқыс оқиғалары туралы ақпаратты шоғырландыру, жүйелеу және сақтау жөніндегі ережелерді, ақпараттық қауіпсіздік оқиғаларын ақпараттық қауіпсіздік оқыс оқиғаларына жатқызу тәртібін, ақпараттық қауіпсіздік оқыс оқиғаларына кейіннен талдау жасау және орын алған ақпараттық қауіпсіздіктің оқыс оқиғалары туралы ақпараттандыруды қамтиды.

13. Ақпараттық қауіпсіздік 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.

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

15. Ақпараттық қауіпсіздік бөлімшесінің басшысы ақпараттық қауіпсіздік саласындағы құжатталған стандарттар мен рәсімдерді әзірлеуді, енгізуді және жетілдіруді қамтамасыз етеді.

16. Ақпараттық қауіпсіздік бөлімшесі ақпараттық қауіпсіздік оқыс оқиғалары туралы ақпараттың талдауын уақытында жүргізуді қамтамасыз етеді, оған ақпараттық қауіпсіздік оқыс оқиғалары орын алған жағдайдың мән-жайын ашу, ақпараттық қауіпсіздік тәуекелдерін басқару жөніндегі бөлімшемен өзара әрекетте болу, қажет болған жағдайда, қорғаныш шараларын енгізу жөнінде ұсыныстар қалыптастыру қоса кіреді.

17. 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 талаптарды орындауды қамтамасыз етеді, сондай-ақ ақпараттық жүйелерді таңдау, енгізу, әзірлеу және тестілеуден өткізу кезінде талаптардың сақталуын қамтамасыз етеді.

18. Ақпараттық қауіпсіздік тәуекелдерін басқару бөлімшесі ақпараттық активтерді оларда сақталатын және өңделетін ақпараттың сынилығының ең жоғары деңгейі негізінде оларды сыни және сыни емес деп бөлу арқылы санаттауды жүзеге асырады.

19. 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 ақпараттық қауіпсіздік қатерлерінің туындау тәуекелін азайтуға бағытталған. профилактикалық (алдын алу) шараларын өткізеді.

20. 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 ақпараттық қауіпсіздік саласында хабардар болуларын арттыру процесін ұйымдастыруға қатысады.

21. Заң бөлімшесі Банктің ақпараттық қауіпсіздікті қамтамасыз ету мәселелері бойынша ІНҚ мен ішкі құжаттарына Ішкі нормативтік құжаттарды басқару жөніндегі нұсқаулыққа сәйкестігіне құқықтық сараптама жүргізеді.

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

23. Ішкі аудит бөлімшесі аудиторлық тексерулер жүргізу кезінде Банктің ақпараттық қауіпсіздікті басқару жүйесінің жай-күйіне бағалау жүргізеді.

24. Ақпараттық жүйелердің немесе ішік жүйелердің бизнес- иеленушілері өнімдер мен қызметтерді құру, енгізу, өзгерту, клиенттерге ұсыну кезінде ақпараттық қауіпсіздікке қойылатын талаптардың сақталуына жауап береді, сондай-ақ ақпараттық жүйелерге қол жеткізу матрицаларын қалыптастырады және өзектілігін (маңыздылығын) сақтайды.

25. Банктің құрылымдық бөлімшелерінің басшылары қызметкерлерді ақпараттық қауіпсіздікке қойылатын талаптарды қамтитын Банктің ІНҚ-мен таныстыруды қамтамасыз етеді, сондай-ақ бағынысты бөлімшелерде ақпараттық қауіпсіздік талаптарының орындалуын қамтамасыз етуге жаңа өнімдерді, қызметтерді, бизнес-қосымшаларды, бизнес-процестер мен технологияларды әзірлеу кезінде қорғау шараларын енгізуге жауапты.

3-Бөлім ҚОРЫТЫНДЫ ЕРЕЖЕЛЕР

26. Саясаттың талаптарын орындамағаны/тиісті орындамағаны үшін, сондай-ақ өздеріне жүктелген қызметтік міндеттемелерін орындау кезінде ақпараттық қауіпсіздікті қамтамасыз ету жауапкершілігін Банктің барлық қызметкерлері көтереді.

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

28. Саясат ІНҚ Дерекқорына өзгерістер енгізілгеннен кейінгі 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.

29. Саясатта реттелмеген мәселелер Қазақстан Республикасының заңнамасына және 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.	№ 42	11.06.2019	14.06.2019	АТ қауіпсіздігі қызметі
2.				