«KMF Банк» АҚ
Ақпараттық қауіпсіздік саясаты

Бизнес-иегері:	Қауіпсіздік департаменті
Бекітілді:	Директорлар кеңесінің 12.11.2025 ж. № 3(9) хаттамасымен
Қолданысқа енгізілді:	12.11.2025 ж. бастап
Күші жойылды деп танылды:	«KMF(ҚМФ)» МҚҰ» АҚ Директорлар кеңесінің 15.07.2026 ж. № 6 Хаттамасымен бекітілген «KMF Банк» АҚ Ақпараттық қауіпсіздік саясаты
ІНҚ-ға қол жеткізу деңгейі:	Қолжетімділігі шектелмеген

Алматы қ.,
2025 ж.

Мазмұны

1-тарау. Жалпы ережелер

1. Осы «KMF Банк» АҚ Ақпараттық қауіпсіздік саясаты (бұдан әрі – Саясат) «KMF Банк» АҚ-ның (бұдан әрі – Банк) ішкі нормативтік құжаты және ақпараттық қауіпсіздігін басқару жүйесінің негізі болып табылады.
2. Осы Саясат Қазақстан Республикасының заңнамасына, оның ішінде Қазақстан Республикасының Ұлттық Банкі Басқармасының 2018 жылғы 27 наурыздағы № 48 қаулысымен бекітілген Банктердің, Қазақстан Республикасының бейрезидент-банктері филиалдарының және банк операцияларының жекелеген түрлерін жүзеге асыратын ұйымдардың ақпараттық қауіпсіздігін қамтамасыз етуге қойылатын талаптарға, ISO/IEC 27000 ақпараттық қауіпсіздік жөніндегі халықаралық стандарттар сериясына және Банктің ішкі нормативтік құжаттарына сәйкес әзірленді;
3. Осы Саясаттың мақсаты Банктің ақпараттық қауіпсіздікті қамтамасыз ету саласындағы оның басшылығы бекіткен ресми ұстанымын декларациялау, сондай-ақ ақпараттық қауіпсіздікті басқару жүйесін құрудың мақсаттарын, міндеттерін, қағидаттарын және даму бағыттарын айқындау болып табылады.
4. Банк Басқармасы ақпараттық қауіпсіздік тәуекелдерінің жол берілетін деңгейімен бизнесті орнықты дамыту үшін жағдай жасауға, бәсекелестік артықшылықтарды қалыптастыруға, қаржылық тұрақтылықты, рентабельділікті қамтамасыз етуге және Банктің рейтингін көтеруге ықпал ететін ақпараттық қауіпсіздікті басқару жүйесінің процестеріне бастама жасайды, қолдау көрсетеді, талдау жүргізеді және орындалуын бақылайды.
5. Банктің Директорлар кеңесі Банктің стратегиясына және операциялық қызметіне ақпараттық қауіпсіздік мәселелерін интеграциялауды қамтамасыз ете отырып, ақпараттық қауіпсіздік саласындағы стратегиялық басшылықты жүзеге асырады. Бюджетті қалыптастыру кезінде Директорлар кеңесі Банктің стратегиялық мақсаттарын, заңнама мен реттеуші органдардың талаптарын, ағымдағы және болжамды қауіп ортасын, сондай-ақ мүдделі тараптар алдындағы міндеттемелерді ескере отырып, ақпараттық қауіпсіздікті қамтамасыз етуге арналған ресурстарға деген қажеттілікті ескереді.
6. Осы Саясатта белгіленетін ақпараттық қауіпсіздік талаптары Банктің даму стратегиясымен келісілген, оның бизнес-процестеріне интеграцияланған және ақпараттық қауіпсіздік тәуекелдерін барынша азайтуға бағытталған. Ақпараттық қауіпсіздік тәуекелдері Банктің операциялық тәуекелдерінің бір бөлігі ретінде қарастырылады және оның қаржылық орнықтылығы мен жұмыс істеу тұрақтылығына елеулі әсер етеді.
7. Осы Саясаттың талаптары осы Саясатта белгіленген ақпараттық қауіпсіздікті басқару жүйесінің әрекет ету саласына кіретін барлық процестерге, ресурстарға және субъектілерге қолданылады.
8. Осы Саясат жалпыға қолжетімді құжат болып табылады және барлық мүдделі тараптар қол жеткізе алуы үшін Банктің корпоративтік сайтында орналастырылады.
9. Осы Саясатта мынадай терминдер мен анықтамалар қолданылады:
    1) қолжетімділік – Банктің ақпараттық активтерін пайдалану мүмкіндігі;

2) ақпараттық қауіпсіздіктің оқыс оқиғасы – ақпараттық-коммуникациялық инфрақұрылымның немесе оның жекелеген объектілерінің жұмысында жекелей немесе сериялы түрде туындайтын, олардың тиісінше жұмыс істеуіне қауіп төндіретін және (немесе) электрондық ақпараттық ресурстарды заңсыз алу, көшірмесін түсіріп алу, тарату, түрлендіру, жою немесе бұғаттау үшін жағдай жасайтын іркілістер;

3) ақпараттық актив – ақпараттың және оны сақтауға және (немесе) өңдеуге пайдаланылатын ақпараттық-коммуникациялық инфрақұрылым объектісінің жиынтығы;

4) ақпараттық-коммуникациялық инфрақұрылым (бұдан әрі – ақпараттық инфрақұрылым) – электрондық ақпараттық ресурстарды қалыптастыру және оларға қолжетімділік беру мақсатында технологиялық ортаның жұмыс істеуін қамтамасыз етуге арналған ақпараттық-коммуникациялық инфрақұрылым объектілерінің жиынтығы;

5) ақпараттық қауіпсіздік тәуекелі – Банктің ақпараттық активтері құпиялылығының бұзылуы, тұтастығының немесе қолжетімділігінің қасақана бұзылуы салдарынан залалдың пайда болу ықтималдығы.

2-тарау. Ақпараттық қауіпсіздік

10. Ақпараттық қауіпсіздік деп Банктің электрондық ақпараттық ресурстарының, ақпараттық жүйелерінің және ақпараттық инфрақұрылымының Банкке, оның клиенттеріне, қызметкерлеріне, акционерлеріне материалдық залал әкелуі, іскерлік беделіне зиян келтіруі немесе мүдделеріне өзге де нұқсан келтіруі мүмкін сыртқы және ішкі қауіптерден қорғалу жай-күйі түсініледі.

11. Ақпараттық қауіпсіздікті қамтамасыз ету деп Банктің ақпараттық активтерінің құпиялылығы, тұтастығы және қолжетімділігі күйін сақтауға бағытталған процесс түсініледі.

12. Ақпараттық қауіпсіздікті қамтамасыз ету шеңберінде ақпарат қауіпсіздігінің басты атрибуттары сақталады:

1) құпиялылық - ақпараттың ашылмайтын және авторизацияланбаған субъектілерге қолжетімді болмайтын қасиеті. Құпиялылықты қамтамасыз ету ақпараттың рұқсатсыз ашылуының алдын алуға бағытталған шаралардың қолданылуын қамтиды;

2) тұтастық - сақтау, өңдеу және беру процесінде ақпараттың толықтығы, қайшылықсыздығы және дәлдігі сақталатын қасиеті. Тұтастықты қамтамасыз ету ақпаратты рұқсатсыз құруды, өзгертуді немесе жоюды алдын алуға және анықтауға бағытталған шараларды қолдануды қамтиды;

3) қолжетімділік - ақпараттың уәкілетті субъектінің сұрауы бойынша қолжетімді және пайдалануға жарамды болу қасиеті. Қолжетімділікті қамтамасыз ету ықтимал кедергілерге, соның ішінде жүйелердің істен шығуына және қолжетімділікті қасақана бұзу әрекеттеріне қарамастан ақпаратқа қолжетімділікті қолдауға бағытталған шараларды қолдануды қамтиды.

13. Ақпараттық қауіпсіздікті қамтамасыз ету бойынша қызметтің негізгі мақсаты Банктің бизнес-процестері үшін ықтимал залалдың ең төменгі деңгейін

қамтамасыз ететін Банктің ақпараттық активтерін қорғау болып табылады. Осы мақсатқа жету үшін Банкте ақпараттық қауіпсіздікті басқару жүйесі құрылады, жұмыс істейді және үздіксіз жетілдіріледі.

3-тарау. Ақпараттық қауіпсіздікті басқару жүйесін ұйымдастыру

§1. Ақпараттық қауіпсіздікті басқару жүйесінің анықтамасы

14. Ақпараттық қауіпсіздікті басқару жүйесі ақпараттық қауіпсіздікті қамтамасыз ету процесін басқаруға арналған Банктің жалпы басқару жүйесінің бір бөлігі болып табылады.
15. Ақпараттық қауіпсіздікті басқару жүйесі тәуекелдерді басқару тетіктері арқылы ақпараттық қауіпсіздік саласында шешімдер қабылдаудың жүйелі, негізделген және басқарылатын тәсілдемесін қамтамасыз етеді.
16. Ақпараттық қауіпсіздікті басқару жүйесі ақпараттық қауіпсіздікті тиімді басқаруды қамтамасыз ететін Саясатты, ұйымдық құрылымды, процестерді, ресурстарды және құжатталған ақпаратты қамтиды.
17. Банк ақпараттық қауіпсіздікті басқару жүйесінің жұмыс істеуін, тиісті жетілу деңгейін, дамуын және үнемі жақсартылуын қамтамасыз етеді.

§2. Ақпараттық қауіпсіздікті басқару жүйесінің мақсаттары

18. Ақпараттық қауіпсіздікті басқару жүйесінің негізгі мақсаттары:
    1) Банкте ақпараттық активтердің қауіпсіздігіне байланысты тәуекелдер бақылауда болатын және басқарылатын жағдайлар жасау және оларды тұрақты қолдау;
    2) заңнаманың, реттеуші органдардың, салалық стандарттардың және ақпараттық қауіпсіздік саласындағы үздік тәжірибелердің талаптарына сәйкестігін қамтамасыз ету;
    3) бизнес-процестердің үздіксіздігін, Банктің орнықты жұмыс істеуі мен дамуын қамтамасыз ету;
    4) клиенттер, контрагенттер, серіктестер, инвесторлар және жалпы, қоғам тарапынан Банкке деген сенімді нығайту, оның рейтингі мен инвестициялық тартымдылығын арттыру.

§3. Ақпараттық қауіпсіздікті басқару жүйесінің міндеттері

19. Ақпараттық қауіпсіздікті басқару жүйесінің қойылған мақсаттарына жету үшін Банк мынадай міндеттердің тиімді орындалуын қамтамасыз етеді:
    1) ақпараттық активтерді сәйкестендіру және жіктеу;
    2) ақпараттық қауіпсіздік тәуекелдерін бағалау, өңдеу және оларға мониторинг жүргізу;
    3) ақпараттық қауіпсіздікке қолданылатын талаптарды және оларды қамтамасыз ету рәсімдерін айқындау және құжаттау;
    4) Банк қызметкерлерін ақпараттық қауіпсіздікті қамтамасыз ету рәсімдеріне оқытып-үйрету, олардың хабардар болуын арттыру және ақпараттық қауіпсіздік мәселелері бойынша жауапкершілікті белгілеу;
    5) Банк басшылығы тарапынан ішкі аудиттер мен талдау жүргізу арқылы ақпараттық қауіпсіздікті басқару жүйесінің қолданылатын ішкі және сыртқы талаптарға сәйкестігін тұрақты бағалау;

6) мүдделі тараптарды Банктің ақпараттық қауіпсіздікті қамтамасыз ету, оқыс оқиғаларды басқару тәсілдемесі туралы, сондай-ақ Банктің ақпараттық қауіпсіздігіне жүргізілген тәуелсіз аудиттердің нәтижелері туралы хабардар ету.

§4. Ақпараттық қауіпсіздікті басқару жүйесін құру қағидаттары

20. Банкте ақпараттық қауіпсіздікті басқару жүйесін құру және оның жұмыс істеуі мынадай негізгі қағидаттарға сәйкес жүзеге асырылады:
    1) заңдылық - Банктің ақпараттық қауіпсіздігін қамтамасыз ету үшін қабылданатын барлық іс-әрекет ақпараттық қауіпсіздікті басқарудың, қамтамасыз етудің және бақылаудың рұқсат етілген әдістерін, құралдары мен тетіктерін қолдана отырып, қолданыстағы заңнама негізінде жүзеге асырылады;
    2) барабарлық - қабылданатын ақпараттық қауіпсіздік шаралары бизнестің қажеттіліктері мен қауіп деңгейін ескере отырып, тәуекелдерді талдау негізінде анықталады;
    3) үздіксіз жұмыс істеу - ақпараттық қауіпсіздікті басқарудың ұйымдық және техникалық шараларының орнықты, сенімді және қолжетімді жұмысы қамтамасыз етіледі;
    4) дербес жауапкершілік - Банктің әрбір қызметкері ақпараттық қауіпсіздікті басқару жүйесінің жұмысы шеңберінде өзіне жүктелген міндеттердің орындалуына және талаптардың сақталуына жауапты болады;
    5) өкілеттіктерді барынша азайту - ақпаратқа қолжетімділік Банк қызметкерлеріне олардың лауазымдық функцияларымен және міндеттерімен айқындалатын көлемде беріледі;
    6) мүдделер қақтығысын жою - қызметкерлердің міндеттері мүдделер қақтығысы орын алмайтындай етіп бөлінеді. Атап айтқанда, бірде-бір қызметкер аса маңызды операцияларды жеке-дара орындауға мүмкіндік беретін өкілеттіктерге ие болмауы керек;
    7) кешенділік - ақпараттық қауіпсіздікті басқару жүйесін құру қауіп жүзеге асатын барлық негізгі арналарды қамтитын және компоненттердің түйіспелеріндегі осалдықтарды болдырмайтын ақпараттық қауіпсіздікті басқарудың әртүрлі шараларын келісіп қолдануға негізделеді.

§5. Ақпараттық қауіпсіздікті басқару жүйесінің әрекет ету аумағы

21. Ақпараттық қауіпсіздікті басқару жүйесінің әрекет ету аумағы Банк қызметі шеңберінде ақпараттық қауіпсіздікті қамтамасыз ету бойынша талаптар қолданылатын процестердің, ресурстардың және субъектілердің жиынтығы ретінде айқындалады.
22. Ақпараттық қауіпсіздікті басқару жүйесінің әрекет ету аумағы мынадай элементтерді қамтиды:
    1) Банктің орнықты жұмыс істеуін және стратегиялық мақсаттарына жетуін қамтамасыз ететін бизнес-процестер;
    2) электрондық ақпараттық ресурстарды, деректер базасын, құжаттарды, бағдарламалық жасақтаманы қоса алғанда, ақпараттық активтер;

3) деректерді өңдеу орталықтарын, серверлерді, желілерді, сақтау құрылғыларын, пайдаланушы құрылғыларын, байланыс арналарын және ақпаратты өңдеуді, сақтауды және беруді қамтамасыз ететін өзге де техникалық құралдарды қоса алғанда, ақпараттық инфрақұрылым;
4) тағылымдамадан өтушілер мен тәжірибеден өтушілерді қоса алғанда, ақпараттық активтерге қол жеткізе алатын Банк қызметкерлері;
5) ақпаратты өңдеуді, қолжетімділікті басқаруды, оқыс оқиғаларға ден қоюды, аудитті және тиімділікті бағалауды регламенттейтін ішкі процестер мен рәсімдер;
6) егер Банк ақпаратын өңдеуге, беруге немесе сақтауға қатысса, контрагенттер, жеткізушілер және сыртқы АТ-сервистер.

23. Әрекет ету аумағы тұрақты түрде қайта қаралуға жатады және қажет болған жағдайда нақтыланады.

§6. Ақпараттық қауіпсіздікті басқару жүйесін жүзеге асыру

24. Ақпараттық қауіпсіздікті басқару жүйесін құру және дамыту Деминг-Шухарттың үздіксіз жетілдіру моделіне негізделген циклдік процесс ретінде жүзеге асырылады (PDCA: Plan – Do – Check – Act) және мынадай кезеңдерді қамтиды:
1) жоспарлау («Plan») - ақпараттық қауіпсіздікті басқару жүйесінің әрекет ету саласын айқындау, ақпараттық қауіпсіздік тәуекелдерін басқару тәсілдемесін формалдау, ресурстарды айқындау және бөлу, ақпараттық қауіпсіздікті басқару шараларын әзірлеу;
2) орындау («Do») - жоспарлау кезеңінде әзірленген шараларды іске асыру, сондай-ақ алдыңғы циклдердің нәтижелері бойынша қабылданған шешімдерді орындау; ақпараттық қауіпсіздік тәуекелдерін бағалау мен өңдеу;
3) тексеру («Check») - ақпараттық қауіпсіздікті басқару жүйесінің жұмыс істеу нәтижелерін оның тиімділігіне, қауіптерге барабарлығына және Банк қызметіне әсер ететін ішкі және сыртқы факторларға сәйкестігіне сенімді болу мақсатында бағалау;
4) түзету («Act») – «тексеру» кезеңінің нәтижелері негізінде ақпараттық қауіпсіздікті басқару жүйесін үнемі жақсартуға бағытталған, жақсарту үшін анықталған мүмкіндіктерді іске асыру бойынша іс-қимылдар мен түзетуші іс-қимылдар туралы шешімдер қабылдау.

§7. Ақпараттық қауіпсіздікті басқару жүйесін дамыту және жақсарту бағыттары

25. Осы Саясат ақпараттық қауіпсіздікті басқару жүйесін тұрақты дамытудың және жақсартудың мынадай негізгі бағыттарын айқындайды:
1) ақпараттық қауіпсіздікті қамтамасыз ету бойынша қызметті ұйымдастыру - Банктегі ақпараттық қауіпсіздікті қамтамасыз ету бойынша рөлдерді, міндеттер мен уәкілеттіктерді айқындау және бөлу, сондай-ақ бұл ақпаратты барлық мүдделі тараптарға жеткізу;
2) құжатталған ақпаратты басқару - ақпараттық қауіпсіздікті басқару жүйесіне жататын құжаттарды әзірлеу, келісу, бекіту, сақтау, беру және жою;

3) ақпараттық қауіпсіздік тәуекелдерін басқару - ақпараттық қауіпсіздік тәуекелдерін сәйкестендіру, бағалау, өңдеу және мониторинг жүргізу;

4) тиімділікті бағалау - ішкі аудитті және басшылық тарапынан талдау жүргізуді қоса алғанда, ақпараттық қауіпсіздікті басқару жүйесінің тиімділігін өлшеу, талдау, бағалау және мониторинг жүргізу;

5) қызметкерлердің қауіпсіздігін қамтамасыз ету - жұмысқа қабылдау кезінде, еңбек қызметі барысында, ауыстыру және жұмыстан шығару кезінде ақпараттық қауіпсіздік талаптарын сақтау шараларын жүзеге асыру;

6) ақпараттық активтерді басқару - ақпараттық активтерді сәйкестендіру, жіктеу, жол берілген пайдалану қағидаларын және қорғау бойынша міндеттерді белгілеу;

7) қолжетімділікті басқару – ақпараттық активтерге тек авторизацияланған пайдаланушылардың ғана қол жеткізуін қамтамасыз ету, санкцияланбаған қолжетімділіктің алдын алу;

8) криптографиялық қорғауды қолдану - ақпараттың құпиялылығын, тұтастығын және шынайылығын қамтамасыз ету үшін криптографиялық әдістерді қолдану;

9) физикалық қауіпсіздік және қоршаған ортаның әсерінен қорғау - санкцияланбаған физикалық қол жеткізудің, зақымданудың, ұрлаудың алдын алу, сондай-ақ Банктің бизнес-процестерін бұзуға қабілетті факторлардан қорғау;

10) ақпараттық инфрақұрылымды қауіпсіз пайдалану - ақпаратты өңдеу құралдарын дұрыс және қауіпсіз пайдалануды қамтамасыз ету, зиянды бағдарламалардан қорғау, резервтік көшіру, аудиторлық із журналдарын жүргізу және қорғау, осалдықтарды және бағдарламалық жасақтаманы басқару;

11) желілік қауіпсіздікті басқару - ақпаратты Банк ішінде және одан тыс жерлерде беру кезінде оның қауіпсіздігін қамтамасыз ету;

12) ақпараттық жүйелердің өмірлік циклінің барлық кезеңінде ақпараттық қауіпсіздікті қамтамасыз ету - тестілік деректерді қорғауды қоса алғанда, оларды жобалау, әзірлеу, енгізу, пайдалану, модификациялау және пайдаланудан шығару кезінде ақпараттық қауіпсіздікке қойылатын талаптардың сақталуын қамтамасыз ету;

13) жеткізушілермен өзара қарым-қатынас - Банктің ақпараттық активтеріне қол жеткізе алатын жеткізушілермен жасалған келісімдерде және шарттарда ақпараттық қауіпсіздікке қойылатын талаптарды белгілеу және бақылау;

14) ақпараттық қауіпсіздіктің оқыс оқиғаларын басқару - ақпараттық қауіпсіздіктің оқыс оқиғаларына мониторинг жүргізудің, оларды анықтаудың, ден қоюдың және тексерудің жүйелі және тиімді тәсілдемесін қамтамасыз ету;

15) бизнестің үздіксіздігін басқарудағы ақпараттық қауіпсіздік - қызметтің үздіксіздігін қамтамасыз ету және қалпына келтіру бойынша

жоспарларды іске асыру кезінде ақпараттың және оны өңдеу құралдарының тұтастығы мен қолжетімділігін қамтамасыз ету;

16) заңнаманың, реттеуші органдардың талаптарын, салалық стандарттарды, шарттық міндеттемелерді, сондай-ақ осы Саясаттың және Банктің ақпараттық қауіпсіздік бойынша өзге де ішкі нормативтік құжаттарының ережелерін сақтау.

26. Ақпараттық қауіпсіздік талаптары осы Саясаттың негізінде ақпараттық қауіпсіздікті басқару жүйесінің шеңберінде әзірленетін Банктің ішкі нормативтік құжаттарында нақтыланады және егжей-тегжейі ашылады.

§8. Банктің ақпараттық активтерінде құрылатын, сақталатын және өңделетін ақпаратқа қолжетімділікті басқаруға қойылатын талаптар

27. Ақпаратқа қолжетімділікті басқару Банктің ақпараттық активтерінің құпиялылығын, тұтастығын және қолжетімділігін қамтамасыз етуге, ақпаратқа рұқсатсыз қол жеткізуді, өзгертуді немесе жоюды болдырмауға бағытталған.

28. Қолжетімділікті басқарудың жалпы тәсілдемесі мынадай қағидаттарға негізделеді:

1) ең аз артықшылықтар - тек лауазымдық міндеттерді орындау үшін қажетті көлемде ғана қолжетімділікті қамтамасыз ету;
2) қол жеткізу құқықтарын шектеу - лауазымдық және функционалдық міндеттерге, пайдаланушылардың санаттарына және ақпараттың құпиялылық деңгейлеріне негізделген қолжетімділіктің рөлдік моделдерін пайдалану;
3) үздіксіз бақылау және қайта қарау - қол жеткізу құқықтарының өзектілігін үнемі қайта қарау және оларды уақтылы өзгерту немесе кері қайтарып алу;
4) дербестендірілген қолжетімділік - ақпараттық жүйелердегі барлық іс-әрекет тек дербестендірілген есептік жазбаларды пайдалану арқылы жүзеге асырылады;
5) қол жеткізу оқиғаларын тіркеу – оқыс оқиғаларды әрі қарай талдау және тексеру үшін қол жеткізу және пайдаланушылардың іс-қимылы журналдарын жүргізу;

29. Қолжетімділікті басқару процестеріне қойылатын талаптар мыналарды қамтиды:

1) ақпараттық активтің иесімен келісуді қоса алғанда, қол жеткізу құқықтарын беру, өзгерту және кері қайтарып алу рәсімдерін формалдау және құжаттау;
2) сәйкестендіруді және аутентификацияны басқару жүйелерімен мүмкіндігінше біріктірілген қолжетімділікті автоматтандырылған басқару құралдарын пайдалану;
3) нақты қолжетімділіктің пайдаланушылардың бекітілген құқықтары мен рөлдеріне сәйкестігін міндетті түрде уақтын-уақтын тексеру;
4) күндерді, негіздемелерді және жауапты тұлғаларды қоса алғанда, қолжетімділікті басқару бойынша барлық іс-әрекетті тіркеу;

5) оқыс оқиғаларға, авариялар немесе шұғыл қол жеткізу қажеттілігіне байланысты жағдайлар үшін арнайы қолжетімділік рәсімдерін қамтамасыз ету (оның ішінде артықшылықты қолжетімділік).

30. Қолжетімділікті басқару осы Саясаттың, Банктің ішкі нормативтік құжаттарының және ақпараттық қауіпсіздік саласындағы қолданылатын халықаралық стандарттардың талаптарына сәйкес жүзеге асырылады.

§9. Ақпараттық қауіпсіздікті қамтамасыз ету бойынша қызметке мониторингті жүзеге асыруға және қауіптерді анықтау және талдау, шабуылдарға қарсы іс-қимыл және ақпараттық қауіпсіздіктің оқыс оқиғаларын тексеру бойынша іс-шараларға қойылатын талаптар

31. Ақпараттық қауіпсіздікті қамтамасыз ету бойынша қызметке мониторинг жүргізу ақпараттық қауіпсіздікті басқару жүйесінің белгіленген талаптарының орындалуын бақылауға, ақпараттық қауіпсіздіктің мақсаттарына (міндеттеріне) қол жеткізуге және ақпараттық қауіпсіздікті басқарудың ауытқуларын, оқыс оқиғаларын немесе тиімсіз шараларын уақтылы анықтауға бағытталған.

32. Мониторингтің жалпы тәсілдемесі мынадай қағидаттарға негізделеді:

1) тұрақтылық пен жүйелілік - мониторинг бекітілген процестер мен рәсімдер шеңберінде тұрақты негізде жүзеге асырылады;
2) дәлелділік – мониторинг нәтижелерінің барлығы тіркелуі, расталуы және талдау үшін қолжетімді болуы тиіс;
3) объективтілік және тәуелсіздік - деректерді талдау бейтарап, қажет болған жағдайда, Банктің тәуелсіз мамандарының немесе құрылымдық бөлімшелерінің қатысуымен жүргізіледі;
4) жақсартуға бағдарлану – мониторинг нәтижелері түзету және алдын алу әрекеттеріне бастама жасау үшін пайдаланылады.
5) Мониторинг процестеріне қойылатын талаптар мыналарды қамтиды:
6) Банктің басқа да мүдделі құрылымдық бөлімшелерінің қатысуымен Қауіпсіздік департаменті Ақпараттық қауіпсіздік басқармасының күштерімен мониторинг ұйымдастыру және жүргізу;
7) ақпараттық қауіпсіздікті басқару шараларын іске асыру, оқыс оқиғалар, ауытқулар және сәйкессіздіктер туралы деректерді жинау, сақтау және талдау;
8) мониторинг нәтижелерін басшылық пен реттеуші органдар үшін есептер және талдамалық материалдар түрінде ұсыну;
9) автоматтандырылған бақылау құралдарын, соның ішінде қауіпсіздік оқиғаларын орталықтан жинау және байланыстыру жүйелерін (SIEM) пайдалану;
10) қолданылған әдістерді, анықталған проблемаларды және қабылданған түзету шараларын қоса алғанда, мониторингтің барлық кезеңін құжаттау.

33. Қауіптерді анықтау және талдау, шабуылдарға қарсы іс-қимыл және оқыс оқиғаларды тексеру бойынша іс-шаралар ден қоюға дайын болуды қамтамасыз етуге, нұқсанды барынша азайтуға және ақпараттық қауіпсіздіктің қайталанған оқыс оқиғаларының алдын алуға бағытталған.

34. Қауіптерді анықтаудың және талдаудың, шабуылдарға қарсы іс-қимылдың және ақпараттық қауіпсіздіктің оқыс оқиғаларын тексерудің жалпы тәсілдемесі мынадай қағидаттарға негізделеді:
    1) проактивтілік - шабуылдарды жүзеге асыруға жол бермеу үшін алдын алу шараларын және қауіптерді ерте анықтауды қолдану;
    2) уақтылы ден қою – оқыс оқиғалар туындаған кезде қажетті әрекеттерді жедел орындау;
    3) кешенділік - барлық ықтимал факторлар мен осалдықтарды ескере отырып, оқыс оқиғаларды қарау;
    4) дәлелдеу және қадағалау - талдау, есеп беру және әрі қарай жақсарту үшін оқыс оқиғалар туралы барлық ақпаратты тіркеу;
    5) үздіксіз жетілдіру - алынған тәжірибені Банктің ақпараттық қауіпсіздіктің қауіптеріне орнықтылығын арттыру үшін пайдалану.
35. Қауіптерді анықтау және талдау, шабуылдарға қарсы іс-қимыл және ақпараттық қауіпсіздіктің оқыс оқиғаларын тексеру бойынша іс-шараларға қойылатын талаптар мыналарды қамтиды:
    1) қауіптерді сәйкестендіру және талдау - техникалық және талдамалық құралдарды, соның ішінде басып кіруді анықтау жүйелерін, SIEM, сыртқы және ішкі белсенділік туралы есептерді пайдалана отырып, ықтимал және нақты қауіптер туралы ақпаратты жинау және өңдеу;
    2) шабуылдардың алдын алу және оларға қарсы іс-қимыл - ақпараттық қауіпсіздікті басқарудың алдын алу шараларын іске асыру, қорғаныс құралдарын (желіаралық экрандар, антивирустар, басып кіруді анықтау және алдын алу құралдары және т.б.) баптау және пайдалану, сондай-ақ жедел әрекет ету рәсімдерін қолдану;
    3) Оқыс оқиғаларды тексеру – оқыс оқиғалардың себептерін, ауқымын, салдарын анықтау, сондай-ақ түзету шараларын әзірлеу;
    4) оқыс оқиғаларды есепке алу журналын жүргізу - ақпараттық қауіпсіздіктің барлық оқыс оқиғаларын анықтау уақытын, сипаттамаларын, себептерін, қабылданған шараларды, қатысушы тұлғаларды және әрекет ету нәтижелерін міндетті түрде көрсете отырып тіркеу;
    5) үрдістер мен қайталанатын оқыс оқиғаларды талдау - заңдылықтарды анықтау, қауіптер динамикасын талдау, ақпараттық қауіпсіздікті басқару шараларын өзекті ету және қолданылатын тәсілдемелерді түзету үшін жинақталған ақпаратты пайдалану.
36. Ақпараттық қауіпсіздікті қамтамасыз ету бойынша қызметтің мониторингі, сондай-ақ қауіптерді анықтау және талдау, шабуылдарға қарсы іс-қимыл және ақпараттық қауіпсіздіктің оқыс оқиғаларын тексеру осы Саясаттың, Банктің ішкі нормативтік құжаттарының және ақпараттық қауіпсіздік саласындағы қолданылатын халықаралық стандарттардың талаптарына сәйкес жүзеге асырылады.

§10. Ақпараттық қауіпсіздіктің оқыс оқиғалары туралы ақпаратты жинауды, шоғырландыруды және сақтауды жүзеге асыруға қойылатын талаптар

37. Ақпараттық қауіпсіздіктің оқыс оқиғалары туралы ақпаратты жинау, шоғырландыру және сақтау себептерді талдау, залалды бағалау, ден қою тиімділігін арттыру және қайталанатын оқыс оқиғалардың алдын алу үшін қажетті мәліметтердің толықтығы мен дұрыстығын қамтамасыз етуге бағытталған.

38. Ақпараттық қауіпсіздіктің оқыс оқиғалары туралы ақпаратты жинаудың, шоғырландырудың және сақтаудың жалпы тәсілдемесі мынадай қағидаттарға негізделеді:

1) шынайылық – оқыс оқиғалар туралы мәліметтер дәл, толық және есепке алу жүйесінде тіркелген дереккөздермен расталған болуы тиіс;
2) жеделдік – ақпарат оқыс оқиғаның маңыздылығына сәйкес белгіленген мерзімдер шегінде кідіріссіз жиналуы, өңделуі және шоғырландырылуы тиіс;
3) қорғалу – оқыс оқиғалар туралы ақпарат санкцияланбаған қолжетімділіктен, өзгертуден және жоюдан, оның ішінде техникалық және ұйымдық шараларды пайдалана отырып қорғалуға жатады;
4) бақылану – оқыс оқиғалар туралы деректермен барлық өзгерістер мен әрекеттер тіркеліп, әрі қарай талдау үшін қолжетімді болуы тиіс;
5) құрылымдалу - ақпаратты жинаудың және сақтаудың пайдаланылатын нысандары мен форматтары стандартталған және есепке алудың біркелкілігін қамтамасыз етеді.

39. Оқыс оқиғалар туралы ақпаратты жинау, шоғырландыру және сақтау процестеріне қойылатын талаптар:

1) деректерді орталықтан сақтауды және талдау мүмкіндігін қамтамасыз ететін оқыс оқиғаларды тіркеу мен есепке алудың автоматтандырылған жүйелерін пайдалану;
2) жауапты тұлғаларды тағайындауды, мәліметтерді ұсыну мерзімдерін және міндетті параметрлер тізбесін (түрі, бастау көзі, анықтау уақыты, сипаттамасы, маңыздылығы бойынша жіктелуі, қабылданған шаралар және т.б.) қоса алғанда, бастапқы ақпаратты жинау рәсімін формалдау;
3) әрі қарай іздеу және талдау мүмкіндігімен, барлық тіркелген оқыс оқиғалар туралы мәліметтерді қамтитын ақпараттық қауіпсіздіктің оқыс оқиғаларын есепке алатын бірыңғай журнал жүргізу;
4) Банктің ішкі нормативтік құжаттарына және Қазақстан Республикасы заңнамасының талаптарына сәйкес белгіленген мерзім ішінде оқыс оқиғалар туралы ақпаратты сақтау;
5) құқықтарды шектеу тетіктерін қолданып және аудиторлық із журналдарын жүргізіп, лауазымдық және функционалдық міндеттер шегінде ғана оқыс оқиғалар туралы ақпаратқа қолжетімділікті қамтамасыз ету.

40. Ақпараттық қауіпсіздіктің оқыс оқиғалары туралы ақпарат оқыс оқиғалардың себептері мен салдарын талдау үшін, сондай-ақ ақпараттық қауіпсіздікті қамтамасыз ету процестерін жақсарту туралы шешім қабылдау үшін қолданылады.

41. Ақпараттық қауіпсіздіктің оқыс оқиғалары туралы ақпаратты жинау, шоғырландыру және сақтау осы Саясаттың, Банктің ішкі нормативтік құжаттарының және ақпараттық қауіпсіздік саласындағы қолданылатын халықаралық стандарттардың талаптарына сәйкес жүзеге асырылады.

§11. Ақпараттық қауіпсіздіктің оқыс оқиғалары туралы ақпаратқа талдау жүргізуге қойылатын талаптар

42. Ақпараттық қауіпсіздіктің оқыс оқиғалары туралы ақпаратты талдау себептерді анықтауға, осалдықтарды айқындауға, залалды бағалауға, түзету және алдын алу шараларын қалыптастыруға, сондай-ақ ақпараттық қауіпсіздікті басқару жүйесінің қайталанатын оқыс оқиғаларға орнықтылығын арттыруға бағытталған.

43. Ақпараттық қауіпсіздіктің оқыс оқиғаларын талдаудың жалпы тәсілдемесі мынадай қағидаттарға негізделеді:

1) шынайылық – оқыс оқиғаларды тіркеу және тексеру барысында алынған, расталған және тексерілген деректер ғана пайдаланылады;
2) жүйелілік – оқыс оқиғалар оқшауланбай, ықтимал өзара байланыстарды, қайталанылуын және Банктің жұмыс істеу ортасын ескере отырып қарастырылады;
3) себептерді жоюға бағдарлану – талдаудың негізгі мақсаты салдарды жою ғана емес, сонымен қатар осындай оқыс оқиғалардың қайта туындауын болдырмау болып табылады;
4) құжатталу – талдаудың барлық кезеңі қорытындылар мен қабылданған шешімдерді көрсете отырып тіркелуге жатады.

44. Ақпараттық қауіпсіздіктің оқыс оқиғаларын талдау процесіне қойылатын талаптарға мыналар жатады:

1) оқыс оқиғаның жіктелуі мен басымдылығын ескере отырып, белгіленген мерзімде талдау жүргізу;
2) оқыс оқиғаның туындауына ықпал еткен, оның ішінде адами, ұйымдық, техникалық және сыртқы себептер мен факторларды анықтау;
3) залалды бағалауды, бизнес-процестерге әсерді және ақпараттық қауіпсіздік талаптарының бұзылуын қоса алғанда, оқыс оқиғаның салдарларын анықтау;
4) анықталған осалдықтарды жою, түзету шаралары, сондай-ақ болашақта осындай оқиғалардың алдын алу бойынша ұсыныстар қалыптастыру;
5) Банк басшылығының және өзге де мүдделі тараптардың қарауы үшін оқыс оқиғаларды талдау нәтижелерін ұсыну;
6) тәуекелдерді басқару жүйесін өзекті ету және ақпараттық қауіпсіздікті басқару жүйесін жақсарту үшін жинақталған талдамалы материалдарды пайдалану.

45. Оқыс оқиғалар туралы ақпаратты талдау осы Саясаттың, Банктің ішкі нормативтік құжаттарының және ақпараттық қауіпсіздік саласындағы халықаралық стандарттардың талаптарына сәйкес жүзеге асырылады.

4-тарау. Қорытынды ережелер

46. Осы Саясат және Банктің ақпараттық қауіпсіздік бойынша ішкі нормативтік құжаттары Банктің барлық қызметкерлерінің, тағылымдамадан өтушілердің, тәжірибеден өтушілердің орындауы үшін міндетті, сондай-ақ клиенттердің және Банктің ақпараттық активтеріне қол жеткізе алатын өзге де үшінші тұлғалардың назарына оларға қатысты бөлігінде жеткізілуі тиіс.
47. Жүктелген лауазымдық функциялары мен міндеттерін орындау кезінде ақпараттық қауіпсіздікті қамтамасыз ету үшін жауапкершілік Банктің барлық қызметкерлеріне жүктеледі.
48. Банктің құрылымдық бөлімшелерінің қызметкерлері ақпараттық қауіпсіздік талаптарын тиісінше орындамағаны және бұзғаны үшін жауапкершілік Банктің тиісті құрылымдық бөлімшелерінің басшыларына жүктеледі.
49. Банк қызметкерлерінің осы Саясатпен танысуы үшін жауапкершілік HR департаментіне жүктеледі.
50. Осы Саясаттың ережелері қажет болған кезде, бірақ Банкте белгіленген тәртіпке сәйкес екі жылда кемінде бір рет қайта қаралады.
51. Осы Саясатты жоспардан тыс қайта қарау:
    1) Қазақстан Республикасының заңнамасында Банктің қызметін, Банктің ұйымдық құрылымын немесе бизнес-процестерін қозғайтын елеулі өзгерістер болған жағдайда;
    2) осы Саясатпен регламенттелген іс-шараларды орындау кезінде елеулі кемшіліктер, сондай-ақ оның ережелерінің Банктің басқа ішкі нормативтік құжаттарымен қайшылықтары айқындалған жағдайда жүзеге асырылады.
52. Осы Ережемен тікелей реттелмеген барлық жағдайда Қазақстан Республикасының қолданыстағы заңнамасының және Банктің ішкі нормативтік құжаттарының талаптарын басшылыққа алу қажет.
53. Осы Саясатқа енгізілген өзгерістер Директорлар кеңесінің шешімімен ғана бекітілуі мүмкін.