ІШКІ ҚҰЖАТ	
Атауы:	«Фридом Банк Қазақстан» АҚ Ақпараттық қауіпсіздік саясаты
Иесі:	Ақпараттық қауіпсіздік департаменті
Бекітілді:	Банктің Директорлар Кеңесінің шешімімен (Банктің ДК 29.03.2024 ж. №03-29(з) хаттамасы, тіркеу №А0-23-04/16/ПТ/29032024 (27.02.2025))
Қолданысқа енгізу мерзімі:	Бекітілген күннен бастап
Соңғы өзгерістерді/ толықтыруларды енгізу	ДК 31.03.2025 ж. №03-31(з) шешімімен бекітілген «Фридом Банк Қазақстан» АҚ АҚ Саясатына өзгертулер мен толықтырулар, ДК 22.07.2025 ж. №07-22(з)
Күші жойылған/күші жойылған деп танылған құжаттар (бар болса):	
Құпиялылық дәрежесі:	***жалпыға қолжетімді***

Ақпараттық қауіпсіздік саясатына
бекітілген өзгерістер мен толықтырулардың
ТІЗІЛІМІ

№	Құжаттың нөмірі	Банк органының өзгерістер мен толықтыруларды бекіту туралы шешімінің деректемелері	Бекітілген өзгерістер мен толықтыруларды қолданысқа енгізу мерзімі	Өзгерістерді/толықтыруларды енгізу негіздемесі
1	№А0-23-04/16/ПТ/29032024 (27.02.2025)	ДК 31.03.2025 ж. №03-31(з) шешімі	Бекітілген күннен бастап	Холдингтің АҚ киберқауіпсіздігі бойынша АҚШ бағалы қағаздар және биржалар комиссиясының жаңа талаптарына, сондай-ақ құжатты ресімдеу бойынша пайдаланылатын халықаралық стандарттар бөлігінде нақтылауға және Банк талаптарына сәйкестендіруге байланысты.
2	№А0-23-04/16/ПТ/29032024 (27.02.2025)	ДК 22.07.2026 ж. №07-22(з) шешімі	Бекітілген күннен бастап	ҚР ҚНРДА Басқармасының 2026 жылғы 3 сәуірдегі №53 қаулысына байланысты нормативтік базаны өзектендіру мақсатындағы өзгерістер, сондай-ақ АҚК функцияларын өзгерту.
3				
4				
5				
6				

Мазмұны

1-тарау. Жалпы ережелер 4

2-тарау. Саясатта қолданылатын ұғымдар 4

3-тарау. АҚБЖ құрудың мақсаттары, міндеттері мен негізгі қағидаттары 5

4-тарау. АҚБЖ қолданылу аясы мен қатысушылары 8

5-тарау. Ақпараттық қауіпсіздікті қамтамасыз ету бойынша рөлдер мен жауапкершілікті бөлу 9

5.1 АҚК 9

5.2 Банк Басқармасының Төрағасы 9

5.3 АҚД 10

5.4 АҚБ 12

5.5 Қауіпсіздік департаменті 13

5.6 HR департаменті 13

5.7 Заң департаменті 14

5.8 Комплаенс-бақылау департаменті 14

5.9 Ішкі аудит департаменті 14

5.10 Операциялық, АТ/АҚ тәуекелдері мен ішкі бақылау департаменті 14

5.11 Бизнес-процестер мен АЖ иелері 14

6-тарау. Банктің АҚ қатерлерін жіктеу 16

7-тарау. Банктің ақпараттық инфрақұрылымы және қорғау объектілері 17

8-тарау. Банктің ақпараттық жүйелерінде жасалатын, сақталатын және өңделетін ақпаратқа қол жеткізуге қойылатын талаптар және ақпарат пен оған қолжетімділікке мониторинг жүргізу 17

9-тарау. АҚ қамтамасыз ету қызметіне мониторинг жүргізуге және қатерлерді анықтау мен талдау, шабуылдарға қарсы әрекет ету және АҚ оқыс оқиғаларын тергеп-тексеру бойынша іс-шараларға қойылатын талаптар 18

10-тарау. АҚ оқыс оқиғалары туралы ақпаратты жинауды, шоғырландыруды және сақтауды жүзеге асыруға қойылатын талаптар 19

11-тарау. АҚ оқыс оқиғалары туралы ақпаратты талдауға қойылатын талаптар 19

12-тарау. АҚ қамтамасыз ету процестері 20

13-тарау. Банк қызметкерлерінің өздеріне жүктелген функционалдық міндеттерін орындау кезінде АҚ қамтамасыз ету үшін жауапкершілігі 20

14-тарау. Қорытынды ережелер 21

1-тарау. Жалпы ережелер

1. «Фридом Банк Қазақстан» АҚ (бұдан әрі – Банк) Ақпараттық қауіпсіздік саясаты (бұдан әрі – Саясат) ақпараттық қауіпсіздік саласындағы шаралар кешеніне қойылатын стратегиялық мақсаттарды, міндеттер мен негізгі талаптарды айқындау, ақпараттық жүйелердің жұмыс істеу тұрақтылығы мен ақпараттың сақталуын қамтамасыз ету, Банктің мүдделерін ақпараттық технологиялар саласындағы қатерлерден жан-жақты қорғауды қамтамасыз ету мақсатында әзірленді.

2. Саясат Банктің Бас офисі мен филиалдарында кез келген түрдегі қорғалатын ақпараттың: ауызша, жазбаша, физикалық тасымалдағыштарындағы ақпараттың, сондай-ақ жаһандық және жергілікті желілер арқылы берілетін деректердің сақталуы және жария етілмеуі саласындағы негізгі талаптар мен ұстанымын айқындайды.

3. Саясат Қазақстан Республикасының заңнамасына, *Қазақстан Республикасы Қаржы нарығын реттеу және дамыту агенттігі Басқармасының 2026 жылғы 3 сәуірдегі № 53 «Банктердің, Қазақстан Республикасының резидент емес банктері филиалдарының және банктік операциялардың жекелеген түрлерін жүзеге асыратын ұйымдардың ақпараттық қауіпсіздігін қамтамасыз ету талаптарын бекіту туралы» қаулысына (бұдан әрі – Қаулы), Қазақстан Республикасы заңнамасының киберқауіпсіздікті қамтамасыз ету саласындағы талаптарына*, *Freedom Holding Corp Ақпараттық қауіпсіздік саясатына, ISO/IEC 27001:2022 және PCI DSS (Payment Card Industry Data Security Standard) халықаралық стандарттарына* сәйкес әзірленді.

2-тарау. Саясатта қолданылатын ұғымдар

4. Саясатта келесі ұғымдар қолданылады:

1) **Автоматтандырылған жүйе** – ақпараттық технологиялық процестерді жүзеге асыратын техникалық және бағдарламалық құралдардың, деректердің (құжаттар массивтерінің) ұйымдастырылған түрде реттелген жиынтығы болып табылатын жүйе;

2) **Аутентификация** – жүйеде ұсынылған қолжетімділік деректемелерінің сәйкестігін анықтау арқылы қолжетімділік субъектісінің немесе объектісінің түпнұсқалығын растау;

2-1) ***Ішкі құжат (бұдан әрі – ІҚ)*** *– Банктің жұмысын ұйымдастыру және Банктің ішкі қызметін/процестерін регламенттеу/ретке келтіру үшін Банкте әзірленген, бекітілген және тіркелген, сондай-ақ Банктің бөлімшелері мен қызметкерлері үшін міндетті талаптарды немесе функцияларды, өзара іс-қимылдарды, жұмыс процестерін, соның ішінде бөлімшелердің/қызметкерлердің келісілген қатысуын талап ететін процестерді орындау кезіндегі әрекеттердің/іс-шаралардың тәртібін белгілейтін, өзгертетін және/немесе тоқтататын электрондық (қағаз) тасымалдағыштағы құжат;*

3) **Ақпараттық қауіпсіздік департаменті (бұдан әрі – АҚД)** – электрондық ақпараттық ресурстардың, ақпараттық жүйелердің және ақпараттық-коммуникациялық инфрақұрылымның сыртқы және ішкі қатерлерден қорғалу жай-күйіне бақылауды қамтамасыз ететін Банктің құрылымдық бөлімшесі (ҚБ);

4) **Сәйкестендіру** – жүйеге және/немесе жүйе ресурсына кіруге рұқсат алу үшін ұсынылған сәйкестендіргіштің жүйеде бар сәйкестендіргіштер тізбесіне сәйкестігін белгілеу немесе анықтау;

5) **Ақпараттық қауіпсіздік (бұдан әрі – АҚ)** – электрондық ақпараттық ресурстардың, ақпараттық жүйелердің және ақпараттық-коммуникациялық инфрақұрылымның сыртқы және ішкі қатерлерден қорғалу жай-күйі;

6) **Ақпараттық жүйе (бұдан әрі – АЖ)** – аппараттық-бағдарламалық кешенді қолдана отырып, ақпаратты сақтауға, өңдеуге, іздеуге, таратуға, беруге және ұсынуға арналған жүйе;

7) **Ақпараттық-коммуникациялық инфрақұрылым** (бұдан әрі – ақпараттық инфрақұрылым) – электрондық ақпараттық ресурстарды қалыптастыру және оларға қолжетімділікті қамтамасыз ету мақсатында технологиялық ортаның жұмыс істеуін қамтамасыз етуге арналған ақпараттық-коммуникациялық инфрақұрылым объектілерінің жиынтығы;

8) **Ақпараттық ресурстар** – ақпараттық жүйелердегі (кітапханаларда, мұрағаттарда, қорларда, деректер базаларындағы) жекелеген құжаттар мен жекелеген құжаттар массивтері, деректер мен ақпарат массивтері;

9) **Ақпарат** – әр түрлі ақпарат тасымалдағыштарда бекітілген және белгілі бір мағынаны білдіретін белгілердің, символдардың, цифрлардың, дыбыстық сигналдардың, басқа деректердің реттелген тізбегі;

10) **Ақпараттық қауіпсіздік комитеті (бұдан әрі – АҚК)** – Басқарма Төрағасы басқаратын және Банктің АҚ қамтамасыз ету міндеттері бойынша шешімдер қабылдауға уәкілеттік берілген, *құрамы мен функциялары АҚК туралы Ережемен айқындалатын* Банктің алқалы органы;

11) **Рұқсат етілмеген қолжетімділік** – осы ақпаратқа қол жеткізуге құқығы жоқ тұлғалардың қорғалатын ақпаратқа қолжетімділігі;

12) **Ақпараттық технологиялар үшін жауапты бөлімшелер** (бұдан әрі – АТБ) – Банктің ақпараттық технологияларының жұмыс істеуі, дамуы, әзірленуі және енгізілуі үшін, сондай-ақ бірінші қорғаныс желісі ретінде тәуекелдерді уақтылы анықтау, бағалау және басқару үшін жауапты Банктің бөлімшесі (бөлімшелері);

13) **Артықшылықты есептік жазба** – ақпараттық жүйедегі есептік жазбаларының қолжетімділік құқықтарын жасау, жою және өзгерту артықшылықтарына ие есептік жазбасы;

14) **Ақпараттық қауіпсіздікті басқару жүйесі** (бұдан әрі – АҚБЖ) – ақпараттық қауіпсіздікті құратын, іске асыратын, пайдаланатын, мониторингті, тексеруді, сүйемелдеуді және жетілдіруді жүзеге асыратын Банктің жалпы басқару жүйесінің бөлігі және ол Банктің ішкі құжаттарының жиынтығын, Банк қызметкерлеріне жүктелген лауазымдық міндеттерге сәйкес олардың ұйымдастырушылық іс-шараларын, ақпаратты қорғаудың барлық бағыттары бойынша әзірленетін, енгізілетін және қолданыста болатын технологиялық, техникалық әдістер мен құралдарды қамтиды;

15) **ҚБ** – құрылымдық бөлімше;

16) **ОЖ** – операциялық жүйе;

17) **ДҚБЖ** – деректер базасын басқару жүйесі.

3-тарау. АҚБЖ құрудың мақсаттары, міндеттері мен негізгі қағидаттары

5. АҚБЖ-ның негізгі мақсаты АЖ қауіпсіздігіне қатысты қатерлерге жол бермеу арқылы Банктің ақпараттық жүйелерінің тұрақты жұмыс істеуін қамтамасыз ету, қорғалатын ақпараттың жария болуына, жоғалуына, жылыстауына, бұрмалануына және жойылуына жол бермеу, сондай-ақ Банктің беделіне кері әсер ету қатерін болдырмау болып табылады.

6. Осы Саясатта Банктің АҚ қатерлерінің негізгі түрлері, осы қатерлер бағытталған Банктің корпоративтік АЖ объектілері, сондай-ақ қатерлерден қорғау шараларына қойылатын талаптар ашып көрсетіледі.

7. Осы Саясаттың талаптарын іске асыру бойынша негізгі тұжырымдамалық міндеттер:

1) төмендегілерді қамтамасыз етуге бағытталған ақпараттық технологиялар саласындағы Банктің тәуекелдерін бағалау негізінде АҚ қамтамасыз ету бойынша ұйымдастырушылық және техникалық шаралар кешенінің орындалуын жоспарлау, іске асыру және бақылау:

– Банктің бизнес-процесетерін қолдау үшін оның ақпараттық активтерінің үздіксіз қолжетімділігін;

– бизнес-процестердің жоғары сапасын қолдау мақсатында Банктің ақпараттық активтерінің тұтастығын;

– Банктің және өзге тараптардың ақпаратының құпиялылығын;

– Банкте қолданылатын АҚ бойынша қабылданатын шаралардың Қазақстан Республикасы заңнамасының, сондай-ақ реттеуші және қадағалау органдары талаптарының сәйкестігін;

2) төмендегілерді қоса алғанда, Банктің жалпы басқару жүйесінің ажырамас бөлігі ретінде АҚБЖ-ны жетілдіру:

– Қазақстан Республикасы реттеуші және қадағалау органдарының талаптарына сәйкес Банктің ұйымдастырушылық құрылымын жетілдіру;

– АҚ қамтамасыз ету бойынша таңдалған шаралар кешенінің іске асырылуын қамтамасыз ететін АҚБЖ процестерін жетілдіру;

– Банк басшылығы тарапынан АҚБЖ процестерінің және осы процестер шеңберінде қабылданатын АҚ қамтамасыз ету шараларының нәтижелері мен тиімділігін, сондай-ақ олардың осы Саясаттың, реттеуші және қадағалау органдарының және Қазақстан Республикасы қолданыстағы заңнамасының белгіленген талаптарына сәйкестігін бақылауды, бағалауды қамтамасыз ету;

3) таңдалған ұйымдастырушылық және техникалық шаралар кешенін ескере отырып, АҚ бойынша талаптарды құжаттау;

4) қызметкерлердің Банктің АҚ саласындағы саясаты, АҚ қамтамасыз ету бойынша қабылданатын шаралар мен талаптар, қызметкерлерге жүктелетін міндеттер мен мінез-құлық ережелері туралы хабардар болуын қамтамасыз ету, сондай-ақ олардың тиісті түрде орындалуына бақылауды қамтамасыз ету;

5) Банктің АҚ қамтамасыз ету жөніндегі қызметі барысында Қазақстан Республикасы заңнамасының талаптарының сақталуын қамтамасыз ету.

8. Осы Саясаттың негізіне келесі базалық қағидаттар алынған:

1) Банктің мақсаттарына әсер ететін қолайсыз факторларды уақтылы анықтау – АҚБЖ Банктің жұмысының тұрақтылығы мен сенімділігіне теріс әсер етуге қабілетті ақпараттық технологиялардағы қатерлердің дамуын жедел анықтауды, талдауды және болжауды көздейді;

2) қолайсыз факторлардың мақсаттарға әсерін бағалау – ақпараттық технологияларда туындайтын немесе болжанатын кез келген қатерлер Банктің мақсаттарына және бизнес-процестерінің орындалу табыстылығына әсер ету бөлігінде бағаланады және Банктің тәуекелдерін бағалауда көрсетіледі;

3) басымдық – АҚ бойынша талаптар АЖ мен Банк активтеріне қойылатын кез келген өзге талаптар алдында басымдыққа ие болады;

4) барабарлық – ұйымдастырушылық және техникалық сипаттағы шаралар тәуекелдерге сәйкес келуге тиіс – осы шараларды іске асыруға жұмсалатын шығындар ақпараттық технологиялардағы қатерлерді іске асырудан болжанатын залалға барабар болуға тиіс;

5) мақсаттардың айқындылығы – шараларды жоспарлау кезінде нақты және

қолжетімді мақсаттар белгіленеді. Талаптарды құжаттау кезінде Банк осы талаптарды орындау кезінде қол жеткізуге ұмтылатын нақты әрі түсінікті мақсаттар көрсетіледі;

6) нәтижелілік – АҚ бойынша кез келген шаралар Банк тиісті шараларды іске асыру кезінде қол жеткізуге ұмтылатын нәтижені ескере отырып жоспарлануға тиіс;

7) тәжірибе мен үздік тәжірибені пайдалану – АҚ қамтамасыз ету жөніндегі қызмет Банктің де, басқа ұйымдардың да жинақталатын және талданатын тәжірибесін, сондай-ақ халықаралық стандарттар мен озық әлемдік тәжірибенің ұсынымдарын ескере отырып орындалуға тиіс;

8) үздіксіздік – Банктің АҚ қамтамасыз ету жөніндегі қызметі негізінде барлық бизнес-процестерді, басқарудың барлық деңгейлерін және Банктің барлық қызметкерлерін қамтитын АҚБЖ негізі болып табылатын үнемі жетілдіріліп отыратын процесс ретінде үздіксіз негізде құрылады;

9) шаралардың бақылануы мен тиімділігі – Банк басшылығы кез келген шараларды бағаланатын тәуекелдерге сәйкестігі, іске асырудың толықтығы мен сапасы тұрғысынан бақылайды. Банк қойылған мақсаттар мен нәтижелерге қол жеткізу дәрежесін негізге ала отырып, шаралардың тиімділігін бағалайды;

10) заңдылық – қорғау іс-шараларын жүзеге асыруды және Банктің АҚБЖ әзірлеуді Қазақстан Республикасының заңнамасына сәйкес жүзеге асыруды білдіреді;

11) жүйелілік – АҚБЖ құруға жүйелі тәсіл және ақпарат қауіпсіздігін қамтамасыз ету мәселесін түсіну мен шешу үшін елеулі маңызы бар барлық өзара байланысты, өзара әрекеттесетін және уақыт өте келе өзгеретін элементтерді, жағдайлар мен факторларды есепке алу;

12) кешенділік – компьютерлік жүйелерді қорғау әдістері мен құралдарын кешенді пайдалану қатерлерді іске асырудың барлық елеулі (маңызды) арналарын жабатын және оның жекелеген компоненттерінің түйіскен жерлерінде әлсіз орындары жоқ тұтас қорғау жүйесін құру кезінде әртекті құралдарды келісілген түрде қолдануды болжайды. Қорғаныс эшелондалып құрылады;

13) персоналды ынталандыру – Банк басшылығы мен қызметкерлері белгіленген талаптарды орындауға және ақпараттық қауіпсіздікті қамтамасыз ету мақсаттарына қол жеткізуге тиісті деңгейде ынталандыруға ие болуға тиіс;

14) тәуекел-бағдарланған тәсіл – АҚ саласындағы негізгі шешімдер өзекті тәуекелдерді, олардың бизнес-процестерге әлеуетті әсерін талдау негізінде, сондай-ақ Банк үшін тәуекелдің рұқсат етілген деңгейлеріне сәйкес қабылданады;

15) өкілеттіктерді минимизациялау – ақпараттық ресурстарға артық қолжетімділікті болдырмау мақсатында әрбір қызметкерге тек оның лауазымдық міндеттерін орындауға қажетті құқықтар мен өкілеттіктер ғана беріледі;

16) міндеттерді бөлу – ешбір пайдаланушыға ақпараттық жүйені немесе критикалық маңызды бизнес-операцияларды өз бетінше бұзуға мүмкіндік беретін жеткілікті құқықтар берілмеуге тиіс;

17) корпоративтік жауапкершілік – Банктің барлық қызметкерлері өздерінің лауазымдық міндеттері шегінде АҚ қамтамасыз етуге жауапты болады және болжанатын оқсы оқиғалар мен қатерлердің алдын алу үшін ақылға қонымды күш-жігер жұмсайды;

18) қауіпсіз архитектура – АҚ қағидаттары бизнес-процестерді, ақпараттық жүйелерді және инфрақұрылымды жобалаудың барлық кезеңдерінде ескеріледі, бұл әлеуетті осалдықтарды олардың жасалу кезеңінде барынша азайтуға мүмкіндік береді;

19) хабардар болу және оқыту – АҚБЖ барлық қатысушылары ақпараттық қауіпсіздік саласындағы міндеттері туралы хабардар және өзекті қатерлер, қорғау әдістері

мен ішкі регламенттер бойынша тұрақты оқытудан өтеді.

4-тарау. АҚБЖ қолданылу аясы мен қатысушылары

9. АҚБЖ қолданылу аясына Банктің Интернет желісі, пошта, пайдаланушылардың Банктің ақпараттық ресурстарына қол жеткізуі арқылы көрсетілетін барлық клиенттік, қаржылық қызметтер бойынша барлық бизнес-процестері кіреді.

10. АҚБЖ қолданылу аясы Банктің барлық ҚБ қамтиды.

11. АҚБЖ қолданылу аясына барлық ақпараттық активтер, соның ішінде Банкке тиесілі және (немесе) Банк өңдейтін құпия және ашық (жалпыға қолжетімді) ақпарат, ақпараттық ресурстар, аппараттық-бағдарламалық құралдар, желілік қамтамасыз ету, ақпарат тасымалдағыштар, Банк кеңселері, Банктің, клирингілік қызмет көрсетудің және заңды және жеке тұлғаларға сервис ұсыну жұмысын қамтамасыз ететін Банктің негізгі құрылымдық бөлімшелері кіреді.

12. Банктің қорғауға жататын негізгі АҚБЖ объектілері:

1) түрі мен ұсынылу формасына қарамастан, Банктің жұмысына қажетті ақпараттық активтер;

2) АТ-инфрақұрылым элементтері, соның ішінде ақпаратты қалыптастыру, өңдеу, беру, сақтау және пайдалану бойынша техникалық және бағдарламалық құралдар, соның ішінде кітапханалар, мұрағаттар, деректер қоры, ақпарат алмасу арналары мен телекоммуникациялар, АЖ мен ақпаратты қорғау құралдары, Банктің қорғалатын АТ-инфрқұрылым элементтері орналастырылған нысандар мен үй-жайлар;

3) Банкте ақпаратты өңдеу процестері, регламенттері мен рәсімдері.

13. Банк қызметкерлері АҚБЖ субъектілері болып табылады.

14. Банктің АҚБЖ қатысушылары:

1) Банктің Директорлар кеңесі;
2) Банк Басқармасы;
3) АҚК;
4) АҚД;
5) АТБ;
6) Қауіпсіздік департаменті;
7) HR департаменті;
8) Заң департаменті;
9) Комплаенс-бақылау департаменті;
10) Ішкі аудит департаменті;
11) Операциялық, АТ/АҚ тәуекелдері мен ішкі бақылау департаменті;
12) Бизнес-процестер мен АЖ иелері.

15. Директорлар кеңесі бюджетті қалыптастыру кезінде Банктің АҚ қамтамасыз етуне арналған ресурс қажеттіліктерін ескереді.

16. Банк Директорлар кеңесі Банктің АҚ саясатын, қызметтік, коммерциялық немесе заңмен қорғалатын өзге құпияны құрайтын мәліметтер туралы ақпаратты қоса алғанда, қорғалатын ақпарат тізбесін және қорғалатын ақпаратпен жұмыс істеу тәртібін бекітеді.

17. Банк Басқармасы АҚ басқару процесін регламенттейтін ІҚ бекітеді.

5-тарау. Ақпараттық қауіпсіздікті қамтамасыз ету бойынша рөлдер мен жауапкершілікті бөлу

18. Банкте АҚ мақсаттарын іске асыруға қажетті басшылық пен АҚ қамтамасыз ету қызметін басқару сапасы АҚБЖ тиімді ұйымдастырылуымен және АҚ қамтамасыз ету процестері мен шараларын немесе жекелеген міндеттерді орындауға қажетті рөлдер мен жауапкершілікті бөлу арқылы қамтамасыз етіледі.

19. АҚБЖ шеңберінде осы Саясаттың 14-тармағында сипатталған, АҚБЖ барлық процестерінің орындалуын қамтамасыз ететін және төмендегілерге ықпал ететін процеске бағдарланған ұйымдық құрылым құрылады:

1) Банктің барлық ҚБ, сондай-ақ Банкте АҚ қамтамасыз етуге мүдделі үшінші тарап ұйымдары мен тұлғалардың АҚ саласына қатысты мәселелерді шешуге үйлестірілген түрде қатысуын қамтамасыз ету;

2) Банк басшылығын ақпараттық қауіпсіздік мәселелері бойынша талап етілетін және уақтылы хабарлауды қамтамасыз ету, соған байланысты шешімдерді қабылдау, орындау және бақылау процестерін нақты ұйымдастыру.

20. Банкте АҚ тиімді басқару, менеджмент және қамтамасыз ету мақсатында рөлдер мен жауапкершілік айқындалған және оңтайлы түрде бөлінген.

21. Рөлдер мен жауапкершілікті бөлу кезінде АҚБЖ шеңберінде бірде-бір рөл қолдамайтын және ешкімнің жауапкершілік аймағы кірмейтін процестер мен шаралардың болу мүмкіндігіне жол берілмейді.

22. Осы Саясат шеңберінде Банктегі АҚБЖ шеңберіндегі негізгі рөлдер айқындалады. Рөлдер мен жауапкершілікті жан-жақты айқындау Банктің ҚБ туралы ережелерде, қызметкерлердің лауазымдық нұсқаулықтарында және Банктің өзге құжаттарында белгіленеді.

5.1 АҚК

23. АҚК келесі функцияларды орындайды:

1) АҚ қамтамасыз етудің жаңа әдістерін енгізу кезінде Банктің ақпараттық қауіпсіздігін қолдау саясатын және Банктің АҚБЖ қалыптастыру мен дамытуды қамтамасыз ету;

2) мерзімінде жойылмаған осалдықтарды көрсете отырып (жойылмау себептерін көрсете отырып), ішкі және сыртқы сканерлеу нәтижелері бойынша есептерді қарау;

3) Банктің АҚБЖ жай-күйі туралы жыл сайынғы есепті қарау;

4) өткен жылғы АҚ оқыс оқиғаларын талдау нәтижелерін қарау;

5) АҚ қамтамасыз ету шараларын іске асыруға қатысты басқа мәселелерді қарау.

5.2 Банк Басқармасының Төрағасы

24. Банк Басқармасының Төрағасы АҚ қамтамасыз ету процесін басқаруға арналған Банктің жалпы басқару жүйесінің бөлігі болып табылатын АҚБЖ құруды, оның жұмыс істеуін және жақсартуды қамтамасыз етеді.

5.3 АҚД

25. АҚД Банк ақпаратының құпиялылығын, тұтастығын және қолжетімділігін қамтамасыз ету мақсатында келесі функцияларды жүзеге асырады:

1) АҚБЖ ұйымдастырады, Банктің ҚБ АҚ қамтамасыз ету және қатерлерді анықтау мен талдау, шабуылдарға қарсы тұру және АҚ оқыс оқиғаларын тергеп-тексеру жөніндегі іс-шараларды үйлестіруді және бақылауды жүзеге асырады;

2) Банктің АҚ саясатын әзірлейді, соның ішінде қажет болған жағдайда оған өзгерістер енгізеді;

3) Банктің АҚ қамтамасыз ету процесіне әдістемелік қолдау көрсетеді;

4) өз өкілеттіктері шеңберінде Банктің АҚ басқару, қамтамасыз ету және бақылау әдістерін, құралдары мен механизмдерін таңдауды, енгізуді және қолдануды жүзеге асырады;

5) АҚ оқыс оқиғалары бойынша ақпаратты жинайды, шоғырландырады, сақтайды және өңдейді;

6) АҚ оқыс оқиғалары туралы ақпаратты талдайды;

7) *АҚК-ның* АҚ мәселелері бойынша *шешім* қабылдауы үшін ұсыныстар дайындайды;

8) Банктің АҚ қамтамасыз ету процесін автоматтандыратын бағдарламалық-техникалық құралдардың енгізілуін, тиісті түрде жұмыс істеуін, сондай-ақ оларға қолжетімділік берілуін қамтамасыз етеді;

9) қолжетімдігі шектеулі ақпаратты техникалық қорғауды жүзеге асыру бойынша іс-шараларды ұйымдастырады, үйлестіреді және бақылайды;

10) ақпаратты, *соның ішінде дербес деректерді* қорғау жүйесін жетілдіру бойынша ұсыныстар әзірлейді;

11) сыртқы тексерулердің нәтижелеріне талдау жасайды, тексерулер барысында анықталған бұзушылықтарды жою бойынша іс-шаралар жоспарын әзірлейді, олардың іске асырылуын бақылайды;

12) ақпараттық объектілерде оны өңдеу процесінде ақпаратты оқуға (ұрлауға), бұзуға, бұрмалауға немесе бұғаттауға бағытталған құқыққа қайшы (оның ішінде қасақана) техникалық, бағдарламалық және өзге ықпалдар мен процестерге жол бермеу немесе оларды елеулі түрде қиындату жөніндегі міндеттерді шешеді;

13) Банк қызметкерлерінің АҚ мәселелері бойынша хабардар болуын қамтамасыз ету бойынша іс-шараларды ұйымдастырады және өткізеді;

14) Банктің АҚБЖ жай-күйіне мониторинг жүргізеді;

15) Банк басшылығына Банктің АҚБЖ жай-күйі туралы хабарлайды;

16) артықшылықты есептік жазбаларын пайдалану бойынша АҚ талаптарын айқындайды;

17) АҚ қатерлерін бағалауды жүзеге асырады;

18) АҚ тәуекелдерін өңдеу шараларын әзірлейді және оларды іске асыру туралы есептілікті Операциялық, АТ/АҚ тәуекелдері мен ішкі бақылау департаментіне ұсынады;

19) Операциялық, АТ/АҚ тәуекелдері мен ішкі бақылау департаментіне АҚ маңызды тәуекелдерін іске асыру, сондай-ақ олардың салдарын жою туралы есептілікті әзірлейді және ұсынады;

20) Банктің АҚ қамтамасыз ету бөлігіндегі стратегиясын іске асыру бойынша іс-шаралар жоспарын әзірлейді, онымен шектелмей, төмендегілерді ашады:

а. ресурс қажеттіліктерін айқындау, соның ішінде АҚ тәуекелдерін басқаруға бағытталған шараларды іске асыруға байланысты бюджетті айқындау;

b. АҚ саласында талап етілетін іс-шараларды мерзімдері мен оларды іске асыруға жауапты орындаушыларды көрсете отырып сипаттау.

26. АҚД директоры:

1) Банкте АҚБЖ ұйымдастырады;

2) Банктің АҚ қамтамасыз етуге байланысты барлық процестерді басқарады және бақылайды;

3) Банк басшылығының АҚ қамтамасыз ету бойынша мақсаттары мен міндеттеріне қол жеткізу үшін жауапкершілік алады;

4) Банктің АҚ қамтамасыз ету мәселелері бойынша Банктің ҚБ өзара әрекеттесуді қамтамасыз етеді;

5) Банктің құрылымдық бөлімшелерінің АҚ қамтамасыз ету және қатерлерді анықтау мен талдау, шабуылдарға қарсы тұру және АҚ оқыс оқиғаларын тергеп-тексеру бойынша іс-шаралар қызметін үйлестіреді және бақылайды;

6) АҚБЖ процестері шеңберінде жұмыс жоспарларын, соның ішінде Банктің АҚ архитектурасын әзірлейді;

7) ақпараттың ықтимал жылыстау арналарын анықтау процесін ұйымдастырады;

8) АҚ бағыты бойынша қатерлер модельдерін жасау және қорғау әдістерін айқындау процесін ұйымдастырады;

9) Банк басшылығына Банктің АҚБЖ жай-күйі туралы хабарлайды;

10) *АҚ құралдарын енгізу және әкімшілендіру процесін ұйымдастырады;*

11) ҚБ-дің АҚБЖ талаптарына сәйкестігіне аудит жүргізуге жауапты болады.

27. АҚД қызметкерлері төмендегілер үшін жауапты:

1) АҚ тәуекелдерін басқару жұмыстарын ұйымдастыру және әдістемелік басшылық ету, ақпараттық активтерді, АЖ жіктеу;

2) Банктің әзірленетін, сатып алынатын және пайдаланылатын АЖ-нің АҚ талаптарына сәйкестігін бағалау, талаптарды іске асыру тәсілдері бойынша ұсыныстар әзірлеу;

3) жүйелерге өзгерістер мен олардың релиздерін енгізу кезінде АҚ талаптарының орындалуын бақылау;

4) АЖ қауіпсіздік сервистерінің функционалдық мүмкіндіктері мен баптауларына қойылатын талаптарды және талаптарды іске асыру тәсілдері бойынша ұсыныстарды әзірлеу;

5) пайдаланушылардың, жүйелерді енгізу және қолдау персоналының Банктің АЖ мен ресурстарына қолжетімділікті басқару процесіне (өкілеттіктерді беру, өзгерту, кері қайтару) қойылатын талаптарды әзірлеу;

6) АҚ, пайдаланылатын қосымшалардың, желінің, ОС және ДҚБЖ жай-күйіне мониторинг жүргізу;

7) АҚ мәселелері бойынша хабардар болуды арттыру шараларын енгізу;

8) АҚ оқыс оқиғаларын шешуді басқару және бақылау;

9) төтенше жағдайлар орын алғанда маңызды бизнес-процестердің үздіксіздігін қамтамасыз ету кезінде АҚ талаптарының орындалуына мониторинг жасау;

10) АТ қызметтерін жеткізушілермен жасалатын шарттарға АҚ талаптарының енгізілуін бақылау, АТ қызметтерін қолдауды жеткізуші ұйымдардың АҚ талаптарын орындауына мониторинг жүргізу;

11) *дербес деректерді қоса алғанда,* маңызды ақпараттық активтерді қорғау;

12) Қазақстан Республикасының заңнамасымен айқындалған АҚ шараларының тиімділігіне мониторинг жүргізу және оларды бағалау;

13) АҚ қамтамасыз ету шаралары мен құралдарын енгізу және олардың орындалуын бақылау;

14) Банктің қорғалатын ақпаратымен жұмыс істеу тәртібінің (қолжетімділік, беру, сақтау, уәкілетті органдарға ұсыну) орындалуына мониторинг жасау;

15) Банк қызметкерлерінің, сондай-ақ сыртқы ұйымдар қызметкерлерінің АТ және қамтамасыз ету инфрақұрылымы орналасқан орындарға қолжетімділігін басқару шаралары мен *бақылау* құралдарын енгізу;

16) белгіленген АҚ талаптарының бұзылу фактілері бойынша қызметтік тексерулер жүргізу, осындай тексерулерді жүргізу кезінде құқық қорғау органдарымен өзара әрекеттесуді ұйымдастыру.

28. АҚ келесі негізгі бағыттарын АҚД қызметкерлері орталықтандырылған түрде басқарады:

1) Банк желісінің АҚ, маңызды қосымшаларды қолдайтын инфрақұрылым элементтерінің (ДҚБЖ, ОЖ) жай-күйіне мониторинг құралдарын енгізу, сондай-ақ Банк желісінің АҚ, ДҚБЖ, ОЖ – маңызды жүйелер компоненттерінің жай-күйіне мониторинг жасау және бағалау;

2) әзірленетін (сатып алынатын) және пайдаланылатын жүйелер мен олардың компоненттеріне (ОЖ, ДҚБЖ), ақпараттық инфрақұрылым компоненттеріне АҚ бойынша бірыңғай талаптарды әзірлеу;

3) жүйелердің жаңарту релиздерін дайындау және өткізу кезінде АҚ жай-күйіне мониторинг жасау және бағалау, аталған жүйелердің қауіпсіздік сервистерінің функционалдық мүмкіндіктері мен баптауларына қойылатын талаптарды және талаптарды іске асыру тәсілдері бойынша ұсыныстарды айқындау;

4) *Директорлар кеңесінің № [күні] шешімімен алынып тасталды.*

29. АҚД қызметкерлері авариялар мен апаттар кезінде Банктің АТ-сервистерін қалпына келтіру процесіне қатысады және АТ-сервистеріне төнетін қатерлерді бағалау, АТ-сервистерін қалпына келтіру бойынша талаптарды қалыптастыру және оларды қалпына келтіру процестері мен шараларын жоспарлау, іске асыру және қолдау бөлігінде Банктің басқа құрылымдық бөлімшелерімен өзара әрекеттеседі.

5.4 АТБ

30. АТБ келесі функцияларды жүзеге асырады:

1) Банктің ақпараттық инфрақұрылымының сызбасын әзірлейді және оның өзектілігін қолдайды;

2) АТБ-ға жатпайтын АЖ АТ-менеджерлері қолжетімділікті қамтамасыз ететін мамандандырылған ақпараттық активтерді қоспағанда, пайдаланушыларға Банктің ақпараттық активтеріне қолжетімділікті қамтамасыз етеді;

3) АҚ талаптарын ескере отырып, Банктің жүйелік және қолданбалы бағдарламалық жасақтамасының үлгілік баптауларын қалыптастыруды және конфигурациялауды қамтамасыз етеді;

4) Банктің ІҚ сәйкес ақпараттық инфрақұрылымы жұмысының үздіксіздігінің, Банк АЖ деректерінің құпиялылығының, тұтастығының және қолжетімділігінің белгіленген талаптарының орындалуын қамтамасыз етеді (ақпаратты резервтеу және (немесе) мұрағаттау және сақтық көшірмесін жасауды қоса алғанда);

5) АЖ таңдау, енгізу, әзірлеу және тестілеу кезінде АҚ талаптарының сақталуын қамтамасыз етеді.

31. Жаңа АЖ сатып алу және қолданыстағы АЖ пысықтау талаптарын енгізуді және әзірлеуді жүзеге асыратын АТБ төмендегілер үшін жауап береді:

1) АЖ әзірлеуге (жобалауға) арналған тапсырмаларды, Банкте белгіленген АҚ талаптарынан ауытқуларды АҚД-мен келісу;

2) өнімді, тестілік орталарды және әзірлеу орталарын бөлу;

3) АЖ әзірлеу және тестілеу персоналының міндеттерін бөлу;

4) АЖ-да тестілеу барысында анықталған АҚ осалдықтарын жою.

32. Міндеттеріне АЖ мониторингі мен пайдалану кіретін АТБ төмендегілер үшін жауапты:

1) АҚД-мен келісуді және АЖ қауіпсіз пайдалану талаптарының, АҚ сервистерінің баптауларының (сәйкестендіру және аутентификация, қолжетімділікті басқару, хаттамалау, шифрлау, туннельдеу) орындалуын бақылауды, анықталған АҚ осалдықтарын уақтылы жою;

2) өнімді орталарды тестілік және әзірлеу орталарынан бөлуді, жүйелерді (өнімдерді) енгізу және қолдау персоналының міндеттерін бөлуді және оларды қолдауды жүзеге асыратын персоналдың жүйелерге қолжетімділік жөніндегі өкілеттіктерін минимизациялау;

3) зиянды БЖ пен спамнан қорғау құралдарын енгізуді және қолдауды;

4) *пайдаланушылар мен әкімшілердің* Банктің ақпараттық ресурстарына қолжетімділігін басқару;

5) АТ/АҚ оқыс оқиғаларын АҚД-ға жеткізуді, оларды шешуді, АҚД-мен бірлесіп олардың туындау себептерін жою;

6) Банктің *ІҚ сәйкес* келісілген АТ қызметтерін жеткізушілермен жасалатын шарттарда қажетті АҚ шаралары мен тараптардың АҚ бойынша міндеттемелерін айқындайтын талаптарды белгілеу;

7) Қазақстан Республикасының заңнамасымен және *Банктің ІҚ* айқындалған АҚ талаптарының орындалуы;

8) ақпараттық және технологиялық инфрақұрылымның маңызды объектілеріне әсер ететін төтенше жағдайлар орын алғанда негізгі бизнес-процестердің істен шығуынан қорғау бойынша АҚД-мен келісілген шараларды енгізу.

5.5 Қауіпсіздік департаменті

33. Қауіпсіздік департаменті келесі функцияларды жүзеге асырады:

1) Банкте физикалық және техникалық қауіпсіздік шараларын іске асырады, соның ішінде өткізу және объектішілік режимдерді ұйымдастырады;

2) Банк қызметкерлерін жұмысқа қабылдау және жұмыстан шығару кезінде АҚ қатерлерінің туындау тәуекелдерін барынша азайтуға бағытталған алдын алу іс-шараларын жүргізеді;

3) өрт қауіпсіздігі мен қауіпсіздік техникасының қамтамасыз етілуін бақылау және мониторинг жүргізу;

4) Банктің қаржылық, ақпараттық және материалдық ресурстарына төнетін ішкі және сыртқы қатерлерді, сондай-ақ олардың туындауына ықпал ететін себептер мен жағдайларды болжайды, ескертеді, анықтайды, жояды;

5) Банктің коммерциялық, қызметтік және банктік құпияны құрайтын құпия ақпаратының ықтимал жылыстау арналарын анықтайды.

5.6 HR департаменті

34. HR департаменті келесі функцияларды жүзеге асырады:

1) Банк қызметкерлерінің, сондай-ақ қызмет көрсету шарты бойынша жұмысқа тартылған тұлғалардың, стажерлардың, практиканттардың АҚ талаптарын сақтау міндеттемесіне және құпия Ақпаратты жария етпеу туралы келісімге қол қоюын қамтамасыз етеді;

2) Банк қызметкерлерінің АҚ саласында хабардар болуын арттыру процесін ұйымдастыруға қатысады;

3) қаржы нарығын реттеу және дамыту бойыншаі уәкілетті органға АҚД қызметкерлерін тағайындау және жұмыстан шығару туралы үш жұмыс күні ішінде хабарлайды;

4) АҚД-мен бірлесіп қызметкерлерді АҚ саласында оқытуды және тренингтерді, Банк қызметкерлерінің білімі мен дағдыларын жыл сайынғы тексеруді жүргізеді.

5.7 Заң департаменті

35. Заң департаменті:

1) Банктің ішкі құжаттарына АҚ қамтамасыз ету мәселелері бойынша құқықтық сараптама жүргізеді;

2) АҚ оқыс оқиғаларын талқылау кезінде АҚД-ға заңгерлік қолдау көрсетеді;

3) Комплаенс-бақылау департаментімен бірлесіп қорғалатын ақпарат тізбесіне енгізуге жататын ақпарат түрлерін айқындайды.

5.8 Комплаенс-бақылау департаменті

36. Комплаенс-бақылау департаменті Заң департаментімен бірлесіп қорғалатын ақпарат тізбесіне енгізуге жататын ақпарат түрлерін айқындайды.

5.9 Ішкі аудит департаменті

37. Ішкі аудит департаменті Банктің Директорлар кеңесінің тиісті тапсырмасы және/немесе мақұлдауы кезінде белгіленген рәсімдерге сәйкес іске асырылып жатқан процестердің және АҚ қамтамасыз ету бойынша шаралардың Банктің АҚ жөніндегі ішкі құжаттарында көрсетілген талаптарға сәйкестігіне шынайы, объективті және тәуелсіз баға береді.

38. Ішкі аудит департаментінің міндеттеріне Банктің ішкі аудит жүйесін ұйымдастыруды регламенттейтін Банктің ішкі құжаттарына сәйкес Банктің АҚБЖ жай-күйін бағалауды жоспарлау және жүргізу кіреді.

5.10 Операциялық, АТ/АҚ тәуекелдері мен ішкі бақылау департаменті

39. Операциялық, АТ/АҚ тәуекелдері мен ішкі бақылау департаменті Банктің ішкі құжаттарында, ҚР заңнамасының талаптарында көзделген және өз құзыреті шеңберінде АҚ тәуекелдерін басқару жөніндегі функцияларды жүзеге асырады.

5.11 Бизнес-процестер мен АЖ иелері

40. Банктің ҚБ басшылары Банктің тиісті бизнес-процестерінің иелері болып табылады және бизнес-процестердің маңыздылық дәрежесін және Банк қызметіндегі олармен

байланысты ақпараттық активтерді, бизнес-процестердің бұзылу немесе ақпараттық активтер мен ақпараттың құпиялылығы, тұтастығы немесе қолжетімділігі бұзылу қатерлерінен туындайтын Банк тәуекелдерін жоғары дәрежеде түсінеді.

41. Бизнес-процестердің иелері ретінде Банктің ҚБ басшылары:

1) бизнес-процестер мен ақпараттық активтердің маңыздылығына объективті баға беру арқылы оларды бағалауға және жіктеуге қатысады;

2) ақпараттық ресурстардың құпиялылығына, тұтастығы мен қолжетімділігіне қойылатын талаптарды, сондай-ақ Банктің бизнес-процестері мен ақпараттық ресурстарына қатысты АҚ бойынша өзге талаптарды айқындайды;

3) Банктің ақпараттық саладағы тәуекелдерін басқару процесінің негізгі қатысушылары болып табылады;

4) Банктің тәуекелдерін құрайтын әлеуетті негативті факторларды және орын алуы мүмкін әлеуетті залалды айқындайды;

5) мониторинг, аудиттер және АҚ оқыс оқиғаларының нәтижелері бойынша тәуекелдерді қайта бағалауға қатысады;

6) олардың бизнес-процестерін қолдауды қамтамасыз ететін Банктің ақпараттық активтерінің иелері ретінде әрекет етеді. Олардың міндеттеріне пайдаланылатын ақпараттық ресурстарға қолжетімділік құқықтарын айқындау және тұрақты түрде қайта қарау, қолжетімділік пен тиісті өкілеттіктерді беру туралы шешім қабылдау кіреді;

7) АҚД-ға бизнес-процестер, пайдаланылатын ақпараттық ресурстар және оларды бағалау туралы толық әрі объективті ақпарат беру үшін жауапкершілік алады;

8) Банктің АЖ және ресурстарын оларды пайдалану талаптары мен нұсқаулықтарына сәйкес дұрыс пайдалану үшін жауапкершілік алады;

9) қызметкерлерді АҚ талаптарын қамтитын Банктің ішкі құжаттарымен танысуын қамтамасыз етеді;

10) өздері басқаратын құрылымдық бөлімшелерде АҚ қамтамасыз ету үшін дербес жауапкершілік алады;

11) Банктің ҚБ осындай келісімдерді, шарттарды жасаудың бастамашысы болатын жағдайларда, құпия ақпаратты жария етпеу туралы келісімдердің жасалуын және қызметтер көрсетуге/жұмыстарды орындауға арналған келісімдерге, шарттарға АҚ қамтамасыз ету талаптарының енгізілуін қамтамасыз етеді.

42. АЖ немесе қосымша жүйелердің бизнес-иелері:

1) АЖ құру, енгізу, модификациялау, пайдалану кезінде және клиенттер мен Банктің ҚБ-не өнімдер мен қызметтерді ұсыну кезінде, сондай-ақ АЖ-ны сыртқы АЖ-мен, соның ішінде мемлекеттік органдардың АЖ-мен біріктіру кезінде АҚ талаптарының сақталуы үшін жауап береді;

2) АЖ-ға қолжетімділік матрицаларын қалыптастырады және олардың өзектілігін қолдайды.

43. ҚБ қызметкерлері:

1) Банкте қабылданған АҚ талаптарының сақталуына жауап береді;

2) өздерінің функционалдық міндеттері шеңберінде өзара әрекеттесетін үшінші тұлғалардың АҚ талаптарын орындауын, соның ішінде аталған талаптарды үшінші тұлғалармен жасалатын келісімдерге, шарттарға енгізу арқылы бақылайды;

3) Банктің ақпараттық активтерімен жұмыс барысында туындаған барлық күдікті жағдайлар мен бұзушылықтар туралы өздерінің тікелей басшысына және АҚД-ға хабарлайды.

6-тарау. Банктің АҚ қатерлерін жіктеу

44. Банктің АҚБЖ ұйымдастыру кешенді сипатқа ие және қатер көздерін, олардың анықталуына ықпал ететін факторларды және олардың алдын алу тәсілдерін міндетті түрде сәйкестендіруді көздейтін ықтимал жағымсыз салдарды талдауға негізделеді.

45. АҚ қатерлерінің түрлері:

1) **Антропогендік** – қатерлердің антропогендік көзі ретінде қорғалатын объектінің штаттық құралдарымен жұмыс істеуге қолжетімділігі (рұқсат берілген немесе рұқсат берілмеген) бар субъектілерді қарастырған жөн.

Ақпарат қауіпсіздігінің бұзылуына себеп болуы мүмкін антропогендік қатерлер субъектілерінің әрекеттері екіге бөлінеді: сыртқы және ішкі.

Кездейсоқ немесе қасақана әрекет ететін сыртқы субъектілер жіктеудің әр түрлі деңгейіне ие. Оларға мыналар жатады:

- криминалдық құрылымдар;
- хакерлер;
- жосықсыз серіктестер;
- коммуникациялық қызметтерді жеткізушілердің техникалық персоналы;
- қадағалау ұйымдары мен апаттық қызметтердің өкілдері;
- ғимаратқа кіруге рұқсаты бар кез келген басқа субъектілер.

Ішкі субъектілер бағдарламалық жасақтама мен техникалық құралдарды әзірлеу және пайдалану саласындағы Банк персоналын, сондай-ақ техникалық және қосалқы сипаттағы жұмыстарды орындайтын персоналды білдіреді. Жоғарыда аталған персонал штаттық жабдықты, желінің техникалық құралдарын пайдалануға және олардың тікелей орналасқан үй-жайларына қол жеткізуге мүмкіндігі бар. Оларға мыналар жатады:

- негізгі персонал (пайдаланушылар, әкімшілер, әзірлеушілер);
- қосалқы персонал (жинаушылар, күзет);
- техникалық персонал (жұмысын қамтамасыз ету, пайдалану).

2) **Техногендік** – адамның технократиялық қызметінен және өркениеттің дамуынан туындайтын қатерлер.

3) **Табиғи** – еңсерілмейтін күшті құрайтын қатерлер, яғни объективті және абсолютті сипатқа ие, барлығына ықпал ететін, даму процесін Банк басқара алмайтын мән-жайлар. Осындай қатерлерді болжау мүмкін емес, сондықтан олардан қорғану шаралары тұрақты түрде қолданылады.

Әлеуетті АҚ қатерлерінің табиғи көздері әдетте қорғалатын объектіге қатысты сыртқы болып табылады және Банк келесі көздерді айқындады:

- өрттер;
- жер сілкіністері;
- су тасқындары;
- дауылдар;
- басқа ұқсас табиғи құбылыстар.

4) Әлеуетті АҚ қатерлерінің көзі болып табылатын **техникалық құралдарға** мыналар жатады:

сыртқы:

- байланыс құралдары;
- инженерлік коммуникация желілері (сумен жабдықтау, кәріз);

ішкі:

- ақпаратты өңдеудің сапасыз техникалық құралдары;
- ақпаратты өңдеудің сапасыз бағдарламалық құралдары;
- қосалқы құралдар (күзет, дабыл жүйесі, телефония);
- Банкте қолданылатын басқа техникалық құралдар.

7-тарау. Банктің ақпараттық инфрақұрылымы және қорғау объектілері

46. Банктің ақпараттық инфрақұрылымы ақпараттық ресурстарды, автоматтандырылған жүйелерді, есептеу техникасы құралдарын, олардың жұмысын қамтамасыз ететін инженерлік жүйелерді, сондай-ақ автоматтандырылған жүйелер жұмыс істейтін және ақпарат өңделетін үй-жайларды қамтиды. Банк персоналы ақпараттық инфрақұрылыммен тығыз байланысты.

47. Банктің ақпараттық ресурстары бастапқы ақпараттан, деректер базасынан, жүйелік, желілік, операциялық және аспаптық бағдарламалық жасақтамадан, құжаттық түрде, сол сияқты өзге түрде ұсынылған физикалық тасымалдағыштарда сақталатын ақпараттан құралады.

48. Банк ақпаратының бір бөлігі оргтехника, құжаттау, жалпы пайдаланудағы құжаттық және сөйлесу байланысы құралдарында (дербес компьютерлер, лазерлік және матрицалық принтерлер, факсимильді аппараттар, ішкі және қалалық автоматты телефон станцияларының телефондары және басқалары) өңделеді.

49. Банк инфрақұрылымының жекелеген элементтері (электрмен жабдықтау, өрт және күзет дабылы, сымды радиохабар тарату жүйелері және басқалар) ақпараттық жүйелермен жанасуы салдарынан қорғалатын ақпараттың қайталама тасымалдаушылары немесе оның жылыстау арналары болып табылады.

50. Банк ақпараттық инфрақұрылымының басқару буынына жататын және маңызды басқару шешімдерін қабылдауды қамтамасыз ететін бөлігі қорғалуға тиіс ең көп жинақталған, аналитикалық, статистикалық және болжанатын мәліметтердің осы деңгейде жоғары шоғырлануына байланысты ерекше назар аударуды талап етеді.

51. Банктің ақпараттандырудың келесі объектілері қорғалуға тиіс:

1) таратылуы шектеулі мәліметтерді, банктік, коммерциялық және құпияның басқа түрлерін құрайтын мәліметтерді, сондай-ақ Банктің ІҚ-мен құпия сипаттағы қорғалатын ақпаратқа жатқызылған өзге мәліметтерді қамтитын ақпараттық ресурстар;

2) Банктің ақпараттандыру құралдары мен жүйелері (автоматтандырылған жүйелер, әр түрлі деңгейдегі және мақсаттағы есептеу желілері, сондай-ақ оларды орналастыру сызбалары, ақпарат берудің техникалық құралдары, ақпаратты көбейту және көрсету құралдары, қосалқы техникалық құралдар мен жүйелер);

3) Банктің ақпараттық ресурстарын қорғаудың техникалық құралдары мен жүйелері.

52. Заңнамамен мемлекеттік құпияларға жатқызылған ақпараттық ресурстар Саясатта қарастырылмайды.

8-тарау. Банктің ақпараттық жүйелерінде жасалатын, сақталатын және өңделетін ақпаратқа қол жеткізуге қойылатын талаптар және ақпарат пен оған қолжетімділікке мониторинг жүргізу

53. Банктің АЖ-ға қолжетімділік пайдаланушыларды сәйкестендіру және аутентификация арқылы жүзеге асырылады.

54. Банк АЖ пайдаланушыларын сәйкестендіру және аутентификациялау «есептік жазба (идентификатор) – құпия сөз» жұбын енгізу арқылы немесе екі факторлы аутентификация тәсілдерін қолдана отырып жүргізіледі.

55. Банктің АЖ-да тек дербестендірілген пайдаланушылық есептік жазбалары қолданылады.

56. Технологиялық есептік жазбаларды пайдалануға *АТБ кураторы болып табылатын* Банк басшысы бекітетін, оларды пайдалану мен өзектілігі үшін дербес жауапты тұлғаларды көрсете отырып, әрбір АЖ үшін осындай есептік жазбалардың тізбесіне сәйкес жол беріледі.

57. Банктің АЖ-да *Банктің электрондық ақпараттық ресурстарына қолжетімділік құқықтарын шектеу талаптарымен және Банктің құпия сөзбен қорғау талаптарымен* айқындалатын есептік жазбалар мен құпия сөздерді басқару функциялары қолданылады.

58. Банк қызметкерлеріне қорғалатын, құпия ақпаратқа қолжетімділік олардың функционалдық міндеттерін орындауға қажетті көлемде беріледі.

59. Банк қызметкерлері *АҚ талаптарын сақтау жөніндегі міндеттememен және Құпия ақпаратты жария етпеу туралы келісіммен* танысқаннан кейін АЖ-ға қолжетімділік алады.

60. Пайдаланушы атқаратын функцияларды автоматтандыратын бағдарламалық жасақтаманың жұмыс істеуі үшін мұндай құқықтар қажет болатын жағдайларды қоспағанда, пайдаланушыларға жұмыс станцияларында локалды әкімшінің құқықтарын немесе соған ұқсас құқықтарды беруге тыйым салынады.

61. Қызметкердің функционалдық міндеттері өзгерген кезде барлық қолда бар қолжетімділік құқықтары ажыратылады және оның жаңа функционалдық міндеттеріне сәйкес келетін жаңа қолжетімділік құқықтары беріледі.

62. Қызметкермен еңбек қатынастары тоқтатылған кезде оның АЖ-ға барлық қолжетімділік құқықтарының күші жойылады.

63. Қызметкер жұмыс орнында ұзақ уақыт болмаған кезде, оның АЖ-ға қосылуы *Банктің электрондық ақпараттық ресурстарына қолжетімділік құқықтарын шектеу жөніндегі талаптармен* белгіленген тәртіппен бұғатталады.

64. АҚД пайдаланушылардың қолжетімділік құқықтарының функционалдық міндеттеріне сәйкестігіне тексеру жүргізеді, сондай-ақ еңбек қатынастары тоқтатылған қызметкерлердің қолжетімділік құқықтарының тоқтатылуына және ұзақ уақыт болмаған қызметкерлердің қосылуының бұғатталуына бақылау жүргізеді.

65. Банктің АЖ-ға сыртқы тараптың / үшінші тұлғалардың қолжетімділігі шарттық қатынастар шеңберінде беріледі және *Банктің электрондық ақпараттық ресурстарына қолжетімділік құқықтарын шектеу жөніндегі талаптармен* регламенттеледі.

9-тарау. АҚ қамтамасыз ету қызметіне мониторинг жүргізуге және қатерлерді анықтау мен талдау, шабуылдарға қарсы әрекет ету және АҚ оқыс оқиғаларын тергеп-тексеру бойынша іс-шараларға қойылатын талаптар

66. Банк АҚ қамтамасыз ету жөніндегі қызметке мониторинг және қатерлерді анықтау мен талдау, шабуылдарға қарсы әрекет ету және АҚ оқыс оқиғаларын тергеп-тексеруді жүргізеді.

67. Банк АҚ оқиғаларына мониторинг жүргізеді және АҚ оқыс оқиғаларын басқарады.

68. Банк мониторинг жүргізілетін АҚ оқиғаларының тізбесін, оқиғалардың себептерін, олардың пайда болу кезеңділігін, мониторинг ережелері мен мониторинг әдістерін айқындайды.

69. АҚД АҚ оқыс оқиғасы орын алған кезде қажет болған жағдайда қосымша бақылауды енгізеді, бизнес-процесті ішінара немесе толық тоқтатады.

70. Мониторинг объектілерін жедел және тұрақты бақылау мақсатында мамандандырылған бағдарламалық құралдар, сонымен қатар пайдаланушылардың, процестердің және т.б. әрекеттерін тіркеудің штаттық (коммерциялық өнімдер мен жүйелерге кіретін) құралдары пайдаланылуы мүмкін.

71. Банк АҚ оқиғаларын АҚ оқыс оқиғаларына жатқызу тәртібін айқындайды

72. АҚ оқыс оқиғаларын басқару тәртібі Банктің АҚ оқыс оқиғаларына қатасты әрекет ету *мәселелерін регламенттейтін* ішкі құжаттармен айқындалады.

10-тарау. АҚ оқыс оқиғалары туралы ақпаратты жинауды, шоғырландыруды және сақтауды жүзеге асыруға қойылатын талаптар

73. Банк АҚ оқыс оқиғасын, оның себептері мен салдарын жою бойынша шұғыл шаралар қабылдау тәртібін айқындайды.

74. Банк орын алған АҚ оқыс оқиғасы туралы Банктің Басшылығына, *уәкілетті органына* және құрылымдық бөлімшелеріне хабарлау тәртібін айқындайды.

75. Банк АҚ оқыс оқиғасының туындау себептерін, оның механизмі мен салдарын жан-жақты талдайды

76. Туындау ықтималдығы жоғары және жақын болашақта оны төмендету мүмкіндігі жоқ АҚ оқыс оқиғалары үшін осындай сипаттағы оқыс оқиғаны өңдеу алгоритмін, оқыс оқиғаны және оның салдарын оқшаулау жөніндегі үлгілік шұғыл шараларды, оқыс оқиғаны өңдеу әдістерін сипаттайтын жеке құжаттар жасалады.

77. АҚ оқыс оқиғасын талдау негізінде оқыс оқиға туралы барлық ақпаратты, сондай-ақ *оның қайталану* ықтималдығын төмендету мақсатында түзету шараларын жүргізу жөніндегі ұсыныстарды көрсететін қорытынды дайындалады.

78. Банк оқыс оқиға туралы барлық ақпаратты, қабылданған шаралар мен ұсынылатын түзету шараларын көрсете отырып, АҚ оқыс оқиғаларын есепке алу журналын жүргізеді.

79. АҚ қамтамасыз ету қызметіне мониторинг жүргізу барысында алынған АҚ оқыс оқиғалары туралы ақпарат шоғырландыруға, жүйелеуге және сақтауға жатады.

80. АҚ оқыс оқиғалары туралы ақпаратты сақтау мерзімі кемінде 5 (бес) жылды құрайды.

81. Банкте АҚ оқыс оқиғалары туралы *ақпаратты жинау, шоғырландыру және сақтау процесі* АҚ оқыс оқиғаларына қатысты әрекет ету *мәселелерін регламенттейтін* ІҚ-мен регламенттеледі.

11-тарау. АҚ оқыс оқиғалары туралы ақпаратты талдауға қойылатын талаптар

82. АҚД АҚ оқыс оқиғасын өңдеу нәтижелері бойынша оқыс оқиғаның туындау себептерін, оның механизмі мен салдарын жан-жақты талдау жүргізеді. Оқыс оқиғаға тартылған бағдарламалық-техникалық құралдардан деректер жинау кезінде жиналған деректердің сақталуы мен өзгермейтіндігі қамтамасыз етіледі.

83. АҚ оқыс оқиғасын талдау нәтижелері бойынша АҚД еркін нысанда қорытынды дайындайды, онда оқыс оқиға туралы барлық ақпарат, сондай-ақ қайталанатын оқыс оқиғаның ықтималдығы мен ықтимал зиянын төмендету мақсатында түзету шараларын қабылдау бойынша ұсыныстар көрсетіледі.

84. Туындау ықтималдығы жоғары және қысқа мерзімде төмендетілмейтін АҚ оқыс оқиғалары үшін АҚД осындай оқыс оқиғаларды өңдеу алгоритмін, оқыс оқиғаны және оның

салдарын оқшаулау жөніндегі үлгілік шұғыл шараларды сипаттайтын жеке құжаттарды әзірлейді.

85. АҚ оқыс оқиғаларын талдау нәтижелері, сондай-ақ олардың *қайталану* ықтималдығын минимизациялау жөніндегі ұсынымдар АҚД тарапынан жыл сайын АҚ Комитетінің қарауына енгізіледі және кейіннен АҚ тәуекелдерін бағалау, АҚ қамтамасыз ету әдістері мен құралдарын түзету, бизнес-процестерді өзгерту үшін пайдаланылады.

12-тарау. АҚ қамтамасыз ету процестері

86. Осы Саясат Банктің АҚ қамтамасыз етудің келесі процестерін регламенттейді:

1) Осалдықтарды басқару – бұл мамандандырылған бағдарламалық жасақтаманы қолдана отырып, осалдықтардың болуына сканерлеуді көздейтін АЖ қорғанысына техникалық талдау жасау процесі. АҚД Банктің ақпараттық жүйелерінің осалдықтарын басқару ережелеріне сәйкес кемінде тоқсанына бір рет осалдықтарға сканерлеу жүргізеді;

2) Операциялық жүйелер мен бағдарламалық жасақтаманың жаңартуларын басқару – бұл АЖ жаңартуларының шығуына мониторинг жасау, оларды тестілеу және соңғы құрылғыларға орнату процесі, ол Банктің операциялық жүйелері мен бағдарламалық жасақтаманың жаңартуларын басқару ережелерімен регламенттеледі. Маңызды осалдықтарды жоятын қауіпсіздік жаңартулары, АҚД-мен келісілген жағдайларды қоспағанда, олар жарияланған және өндіруші таратқан күннен бастап бір айдан кешіктірілмей орнатылады;

3) Вирусқа қарсы қорғауды қамтамасыз ету – бұл Банктің корпоративтік есептеу желісінің ақпараттық ресурстарын компьютерлік вирустар мен зиянды бағдарламалық жасақтаманың жойғыш әсерінен вирусқа қарсы қорғауды ұйымдастыру процесі, ол Банктің вирусқа қарсы қорғау ережелерімен регламенттеледі;

4) Желілік қауіпсіздікті басқару – бұл желілік инфрақұрылымды жобалау, енгізу және пайдалану кезінде АҚ талаптарын айқындайтын процесс, ол Банктің желілік қауіпсіздік саясатымен реттеледі;

5) Мониторинг және оқыс оқиғаларды басқару;

6) Банк қызметкерлерінің АҚ мәселелері бойынша хабардар болуын қамтамасыз ету;

7) Банктің ақпараттық ресурстарына қол жеткізуге рұқсат беру.

13-тарау. Банк қызметкерлерінің өздеріне жүктелген функционалдық міндеттерін орындау кезінде АҚ қамтамасыз ету үшін жауапкершілігі

87. *Банк қызметкерлерінің* осы Саясат талаптарын сақтамауы Қазақстан Республикасының заңнамасына және Банктің ІҚ сәйкес жауапкершілікті көздейді.

88. Осы Саясат талаптарының сақталуын бақылау Банктің Басқармасына және Атқарушы директорларға жүктеледі.

89. АҚБЖ қатысушылары болып табылатын Банктің ҚБ өз құзыреттері шегінде осы Саясат талаптарының орындалуына жауапты болады.

90. Директорлар Кеңесінің –жылғы № шешімімен алынып тасталды.

91. Директорлар Кеңесінің –жылғы № шешімімен алынып тасталды.

92. Әрбір пайдаланушы ақпаратпен жұмыс істеу кезінде және Банктің АЖ мен ресурстарымен жұмыс істеген кезде өз әрекеттері үшін дербес жауап береді.

93. Банк қызметкерлері міндетті:

1) АЖ қауіпсіздігін қамтамасыз ету бойынша Банкте белгіленген ішкі талаптарды білуге және сақтауға;

2) АЖ мен ресурстарды осы Саясатқа, нақты АЖ мен қосымшаларға қойылатын қауіпсіздік талаптарына сәйкес пайдалануға;

3) тікелей басшысына немесе АҚД қызметкерлеріне АҚ талаптарын бұзушылықтар, өзге күдікті жағдайлар мен оқыс оқиғалар туралы ақпарат беруге;

4) Банктің АЖ-да бөтен бағдарламалық жасақтаманы пайдаланбауға және таратпауға;

5) ақпараттық желіде дұрыс әрекет етуді қамтамасыз етуге, АҚ механизмдерін айналып өту немесе бұғаттау бойынша, ақпаратты қасақана өзгерту, жою, оқу немесе рұқсат етілмеген тәсілмен беру бойынша қандай да бір әрекеттер жасамауға;

6) бағдарламалық жасақтамадан табылған осалдықтар немесе қателер туралы АЖ әкімшілеріне және АҚД қызметкерлеріне дереу хабарлауға, сондай-ақ белгіленген АҚ ережелерін бұзатын басқа пайдаланушылардың құқыққа қайшы әрекеттері туралы хабарлауға.

94. Банк қызметкерлеріне тыйым салынады:

1) Банктің құпия ақпаратын кез келген қолжетімді тәсілдермен бөгде тұлғаларға беруге;

2) электрондық поштаны жеке мақсаттарда пайдалануға. Электрондық пошта қызметтік міндеттерін орындауға ғана беріледі;

3) жұмыс станциясына Банктің қызметіне байланысты емес ақпаратты жүктеуге;

4) Банктің корпоративтік желісінде бөтен бағдарламалық жасақтаманы пайдалануға және таратуға;

5) құпия сөздер мен өзге аутентификациялық деректерді жұмыс компьютерлерінде, мобильді құрылғыларда және электрондық ақпарат тасымалдағыштарда, сондай-ақ қағаз тасымалдағыштарда шифрланбаған түрде сақтауға.

95. Банк қызметкерлердің кіріс/шығыс корреспонденциясын бақылау құқығын өзіне қалдырады.

96. Интернет желісіндегі әрбір пайдаланушының әрекеттері хаттамаланады, бұзушылықтар анықталған жағдайда қызметкерге тәртіптік жаза қолданылады.

14-тарау. Қорытынды ережелер

97. Осы Саясатқа өзгерістер мен толықтырулар енгізу Банктің *ІҚ* әзірлеу, бекіту, өзгерту және/немесе толықтыру және қолданысын тоқтату жөніндегі *ІҚ* талаптарына сәйкес жүзеге асырылады.

98. Саясатқа өзгерістер және/немесе толықтырулар енгізу үшін жауапкершілік АҚД-ға жүктеледі.

99. Осы Саясатты және АҚ бойынша *ІҚ* қайта қарау ҚР қолданыстағы заңнамасындағы немесе Банктің ҚБ жұмыс технологиясындағы өзгерістерге, аудиторлардың ұсыныстары мен ескертулеріне, сыртқы сарапшылардың ұсынымдарына байланысты жоспарлы, сол сияқты жоспардан тыс болуы мүмкін. Саясат пен АҚ бойынша *ІҚ*-да баяндалған ақпаратты талдау және өзектендіру мақсатында аталған құжаттарды міндетті түрде қайта қарау кемінде екі жылда 1 (бір) рет жүзеге асырылуы тиіс.

100. Сыртқы мүдделі тараптарды (Банк клиенттерін, контрагенттерді және т.б.) Саясаттағы оларға қатысты бөлігіндегі өзгерістер туралы хабардар етуге олармен өзара әрекеттесетін Банктің ҚБ басшылары жауапты. Хабардар ету жөніндегі жұмыстарды жалпы үйлестіру мәселелері, сондай-ақ оларды бақылау АҚД-ға жүктеледі.

101. Банктің барлық қызметкерлері осы Саясат орындауға және онымен танысуға міндетті.