Банк ВТБ (Қазақстан) Акционерлік қоғамының Еншілес ұйымы ақпараттық қауіпсіздік саясаты

Банк ВТБ (Қазақстан) Акционерлік қоғамының Еншілес ұйымында (бұдан әрі – Банк) Банктің Директорлар кеңесімен Ақпараттық қауіпсіздік саясаты (бұдан әрі – Саясат) әзірленіп, бекітілген, ол Банкте ақпараттық қауіпсіздікті (бұдан әрі – АҚ) басқарудың тиімді жүйесін құрудағы тәсілдерді, қағидаттар мен қағидаларды айқындайды, сондай-ақ Саясат ережелерін іске асыруға жауапты Банктің органдары мен бөлімшелерін айқындайды.

Саясат Қазақстан Республикасының қолданыстағы заңнамасына, Қазақстан Республикасының Қаржы нарығын реттеу және дамыту агенттігінің және Қазақстан Республикасы Ұлттық Банкінің талаптарына, сондай-ақ Банктің ішкі құжаттарына сәйкес әзірленген.

Саясат мыналарды айқындайды:

1. АҚ басқару жүйесін құрудың мақсаттарын, міндеттерін және негізгі қағидаттарын;
2. АҚ басқару жүйесінің қолданылу саласын;
3. Банктің ақпараттық активтерінде құрылатын, сақталатын және өңделетін ақпаратқа қолжетімділікті басқаруға қойылатын талаптарды;
4. АҚ қамтамасыз ету жөніндегі қызмет мониторингін және қауіптерді анықтау мен талдау, шабуылдарға қарсы іс-қимыл жасау және АҚ инциденттерін тергеп-тексеру жөніндегі іс-шараларды жүзеге асыруға қойылатын талаптарды;
5. АҚ инциденттері туралы ақпаратты жинауды, шоғырландыруды және сақтауды жүзеге асыруға қойылатын талаптарды;
6. АҚ инциденттері туралы ақпаратқа талдау жүргізуге қойылатын талаптарды;
7. Банк жұмыскерлерінің өздеріне жүктелген функционалдық міндеттерді орындау кезінде АҚ қамтамасыз ету үшін жауапкершілігін.

АҚ басқару жүйесін құрудың мақсаттары, міндеттері және негізгі принциптері

Банктегі АҚ басқарудың негізгі мақсаттары сыртқы операциялық ортаға, Банктің стратегиясына, Банктің ұйымдық құрылымына, активтер көлеміне, Банктің операцияларының сипаты мен күрделілік деңгейіне сәйкес келетін, АҚ тәуекелдерін барынша азайтуға бағытталған, сондай-ақ Саясатта көзделген мақсаттарға сәйкес тиімді АҚ басқару жүйесін (бұдан әрі – АҚБЖ) құру болып табылады.

АҚБЖ-ның негізгі міндеті Банктің бизнес-мақсаттарына қол жеткізу үшін пайдаланылатын технологиялар мен автоматтандырылған ақпараттық жүйеге (бұдан әрі – ААЖ) әсер ететін АҚ тәуекелдерін барынша азайту, сондай-ақ АҚ қауіптерін іске асырудың және ықтимал инциденттердің қолайсыз салдарын жою жөніндегі іс-шаралардың тиімділігін қамтамасыз ету болып табылады.

АҚБЖ-ның тиісті деңгейін, оны дамыту мен жетілдіруді қамтамасыз ету мақсатында Банк келесі негізгі мақсаттарға қол жеткізеді:

1) ақпараттық активтерді АҚ қауіптерінен қорғау жөніндегі шараларды іске асыру;

2) ақпаратты қорғау құралдарын иелену құнын оңтайландыру;

3) АҚ өзекті қауіптерін іске асырудан келтірілетін залалдың алдын алу және/немесе оны қолайлы деңгейге дейін төмендету;

4) АҚ саласындағы заңнамалық, нормативтік және шарттық талаптарды сақтау;

5) АҚ қауіптерінің ықтимал іске асырылуы жағдайында Банктің жұмыс істеу тұрақтылығын арттыру;

6) Банктің АҚБЖ жай-күйін бақылау және оны тұрақты жетілдіру;

7) кибербарлау процесін қоса алғанда, АҚ инциденттеріне үздіксіз мониторинг жүргізу және ден қою;

8) АҚ инциденттеріне жедел ден қою үшін жұмыскерлерді оқыту және олардың біліктілігін арттыру;

9) АҚ бөлігінде ВТБ Тобына қатысушылардың бірыңғай даму стратегиясын жүргізуге қатысу, АҚ бақылаудың, қамтамасыз етудің және басқарудың ашық біріздендірілген процестерін енгізу;

10) АҚ мәселелері бойынша Бас банкпен өзара іс-қимылдың тиімділігі мен сапасын арттыру.

АҚ басқару жүйесін құрудың негізгі принциптері

АҚБЖ-ның барынша жоғары тиімділігіне қол жеткізу мақсатында Банк келесі негізгі қағидаттарды басшылыққа алады:

1) **Бөлінбестік** – ААЖ қауіпсіздігі олардың ажырамас қасиеті (сипаттамасы) болып табылады, қосымша сервис емес;
2) **Кешенділік** – қауіпсіздікті қамтамасыз етудің тұтас жүйесін құру кезінде ақпаратты қорғаудың барлық арналарын жабатын және оның жекелеген компоненттерінің түйісу жерлерінде әлсіз тұстары жоқ, әртекті құралдарды келісілген түрде қолдану қажет;
3) **Жүйелілік** – ақпаратты қорғау жөніндегі қызмет қатаң әрі жан-жақты регламенттелуге тиіс;
4) **Үздіксіздік** – ақпаратты қорғау бір реттік іс-шара немесе жүргізілген іс-шаралар мен орнатылған қорғау құралдарының жай ғана жиынтығы емес, Банктің ақпараттық жүйелерінің өмірлік циклінің барлық кезеңдерінде, олардың жобалануының ең ерте сатыларынан бастап, тек пайдалану кезеңінде ғана емес, тиісті шараларды қабылдауды көздейтін үздіксіз мақсатты процесс;
5) **Барабарлық** – қолданылатын ақпаратты қорғау әдістері мен құралдары оның жойылуы, ағып кетуі немесе бұрмалануы қауіптеріне барабар болуы тиіс;
6) **Активтерді сәйкестендіру және бағалау** – «Барабарлық» қағидатын іске асыру барлық ақпараттық активтерді сәйкестендіруге және олардың Банк мақсаттары мен міндеттері үшін құндылығын айқындауға негізделуге тиіс;
7) **Икемділік және басқарылушылық** – қорғау жүйелері ААЖ қорғалу деңгейін өзгерту мүмкіндігін қамтамасыз етуі тиіс;
8) **Уақтылылық** – АҚ ішкі жүйелерін әзірлеу қорғалатын жүйені әзірлеумен бір мезгілде жүргізілуі тиіс;

9) **Алдын алу** – АҚ қамтамасыз ету жүйесінің жұмысында ақпараттың тұтастығына, қолжетімділігіне және құпиялылығына әсер етуі мүмкін АҚ оқиғаларын болдырмауға (алдын алу шараларына) басымдық берілуі тиіс;
10) **Бақыланушылық** – ақпараттық қауіпсіздікті қамтамасыз ету ережелерін бұзу әрекеттерін анықтау және жолын кесу міндетті әрі уақтылы болуы тиіс;
11) **Заңдылық** – ақпаратты қорғау жөніндегі қызмет қолданыстағы заңнамаға, қадағалау және бақылау органдарының талаптарына, ақпаратты қорғау саласындағы нормативтік актілерге қатаң сәйкестікте жүзеге асырылуы тиіс;
12) **Үздік тәжірибелерді ұстану** – АҚ қамтамасыз ету шараларын іске асыру кезінде ВТБ Тобының талаптарын, отандық және халықаралық стандарттарды ақпараттық қауіпсіздік саласындағы үздік тәжірибелер ретінде ескеру ұсынылады;
13) **Талдау және жетілдіру** – ақпараттық жүйелердің жұмыс істеуін, ақпаратты ұстап қалу және жүйе компоненттеріне әсер ету әдістері мен құралдарының өзгеруін, қорғау саласындағы нормативтік талаптардың өзгеруін, сондай-ақ ақпаратты қорғау саласындағы отандық және шетелдік тәжірибені талдау негізінде ақпаратты қорғау құралдары мен шараларының тиімділігін бағалау және оларды үнемі жетілдіру бойынша тұрақты жұмыс қажет;
14) **Өкілеттіктерді барынша шектеу** – пайдаланушыларға қолжетімділік құқықтарын беру тек өндірістік қажеттілікпен айқындалады. Ақпаратқа қолжетімділік тек қызметкерге және үшінші тұлғаларға олардың лауазымдық/шарттық міндеттерін орындауы үшін қажетті көлемде және жағдайда ғана берілуі тиіс;
15) **Функцияларды бөлу** – рөлдер құрамын айқындау кезінде бір рөл шеңберінде бір қызметкерге сыни операцияларды жеке орындауға немесе Банктің кез келген жүйесіне толық әрі бақыланбайтын қолжетімділік алуға мүмкіндік беретін функцияларды біріктіруге (өкілеттіктерді шоғырландыруға) тыйым салынады;
16) **Персонификация** – Банктің барлық жұмыскерлерінің әрекеттері дербестендірілген есептік жазба арқылы жүзеге асырылуы тиіс. Нақты бір қызметкерге бекітілмеген есептік жазбалардың болуы рұқсат етілмейді;
17) **«Рұқсат етілмегеннің барлығы тыйым салынады» қағидаты** – ақпараттық жүйенің кез келген объектісіне қолжетімділік тек жобалық құжаттамада, бизнес-процесс регламентінде және ақпаратты қорғау құралдарының баптауларында тіркелген тиісті рұқсат (ереже) болған жағдайда ғана берілуі тиіс. Кез келген тікелей рұқсат етілмеген қолжетімділікке тыйым салынады;
18) **Қорғаныс шаралары мен құралдарын қолданудың қарапайымдылығы** – қолданылатын қорғау құралдары интуитивті түрде түсінікті және пайдалануға оңай болуы тиіс. Оларды қолдану ақпараттық жүйелер пайдаланушыларының (жұмыскерлер мен клиенттер) күнделікті жұмысында айтарлықтай қосымша еңбек шығындарымен байланысты болмауы тиіс;
19) **Қорғау құралдарының төзімділігі** – қолданылатын құралдардың төзімділік деңгейі мен ақпаратты қорғау шараларының тиімділігі қорғалатын объектінің құндылығына сәйкес айқындалып, зиянкес тарапынан оларды

еңсеру үшін уақыт пен есептеу ресурстарының орынсыз жоғары шығындарын талап етуі тиіс;

20) **Қорғаудың эшелондануы** – бір ғана қорғаныс шегіне сүйенуге болмайды, ол қаншалықты сенімді деп есептелсе де. Периметрді қорғау құралдарынан бөлек ішкі желіні, серверлерді, жұмыс станцияларын, дерекқорларды және т.б. қорғау жүйелері қолданылуы тиіс;
21) **Қорғау құралдарының әртүрлілігі** – жалпы қауіпсіздік деңгейінің жеткізушілерге, провайдерлерге, серіктес компанияларға тәуелділігін және жекелеген жүйелердің істен шығу тәуекелдерін азайту мақсатында әртүрлі өндірушілердің құралдарын қолдану орынды. Жұмыс станцияларында, серверлерде және желілік экрандау құралдарында әртүрлі өндірушілердің антивирустық құралдарын пайдалану міндетті болып табылады;
22) **Мамандану және кәсібилік** – ақпаратты қорғау құралдарын әзірлеу, енгізу, сүйемелдеу және қорғау шараларын іске асыру жұмыстарына нақты қызмет түрі бойынша ақпараттық ресурстардың қауіпсіздігін қамтамасыз ету саласында тәжірибесі бар, қажетті лицензиялары бар, енгізілетін шешімдер өндірушілерінің серіктестік мәртебелеріне ие және білікті қызметкерлері бар мамандандырылған ұйымдар тартылуы тиіс;
23) **Хабардар болу** – жұмыскерлер мен клиенттердің АҚ мәселелері бойынша хабардар болуы жүйелердің қауіпсіз жұмыс істеуінің міндетті шарты болып табылады;
24) **Жеке жауапкершілік** – ақпараттың және оны өңдеу жүйелерінің қауіпсіздігін қамтамасыз ету үшін жауапкершілік тек ақпараттық қауіпсіздік бөлімшесіне ғана емес, әрбір Банктің жұмыскеріне оның өкілеттіктері шегінде жүктеледі;
25) **Персоналдың адалдығы** – Банктің барлық бөлімшелер ұжымдарында жұмыс ортасы осылай қалыптастырылуы тиіс: АҚ талаптарын орындау жұмыскерлер үшін қосымша жүктеме ретінде емес, саналы қажеттілік және корпоративтік этиканың ажырамас бөлігі ретінде қабылдануы тиіс;
26) **Басшылықтың қатысуы** – Банктің басшылығының АҚ қамтамасыз ету қажеттілігін түсінуі, АҚ жүйесінің жұмыс істеуіне қатысты стратегиялық шешімдер қабылдауға, соның ішінде АҚ тәуекелдерін қабылдау мәселелеріне тікелей қатысуы;
27) **Өзара іс-қимыл және үйлестіру** – АҚ тиімді қамтамасыз етілуі Банктің барлық мүдделі бөлімшелерімен, Бас Банктің АҚ бөлімшесімен, сондай-ақ басқа да бейінді министрліктермен, ведомстволармен, ұйымдармен және бірлестіктермен өзара іс-қимыл және үйлестіру негізінде жүзеге асырылады;
28) **Технологиялық тәуелсіздік** – бағдарламалық және бағдарламалық-аппараттық құралдарды, оның ішінде ақпаратты қорғау құралдарын таңдау кезінде оларды әзірлеушілер (өндірушілер) немесе өзге тұлғалар тарапынан қолдануға қойылған шектеулер ескеріледі. Ақпаратты қорғау құралдары оларды пайдалану кезеңінің барлық мерзіміне кепілдік және/немесе техникалық қолдаумен.

Саясат Банктің барлық жұмыскерлеріне қолданылады және АҚ қамтамасыз ету жөніндегі қызметті ұйымдастырудың тұжырымдамалық негіздері мен талаптарын сипаттайды, сондай-ақ оларды іске асырудың негізгі бағыттарын айқындайды:

1) ақпараттық активтерді сәйкестендіру, қорғалатын ақпаратты санаттау;
2) шабуылдарға қарсы іс-қимылды қоса алғанда, желілік қауіпсіздікті құру;
3) антифрод тетіктерін құру;
4) Банктің ААЖ-іне және ақпараттық ресурстарына қолжетімділікті бақылауды қамтамасыз ету;
5) серверлерді, деректерді өңдеу орталықтарын, серверлік үй-жайларды қорғауды қамтамасыз ету;
6) Банкте айқындалған тәртіпке сәйкес ақпараттық инфрақұрылымды антивирустық қорғауды қамтамасыз ету;
7) автоматтандырылған жұмыс орындарын қорғауды қамтамасыз ету;
8) қолданбалы бағдарламалық қамтамасыз ету/ Банктің ААЖ өмірлік циклінің кезеңдерінде АҚ қамтамасыз ету;
9) виртуалды ортада қызметті жүзеге асыру кезінде АҚ қамтамасыз ету;
10) дерекқорларды басқару жүйелерін қорғауды қамтамасыз ету;
11) интернет пен электрондық поштаны пайдалану кезінде контенттік бақылауды қамтамасыз ету/ жүзеге асыру;
12) зиянды кодтың әсерінен қорғауды қамтамасыз ету;
13) ақпаратты криптографиялық қорғауды қамтамасыз ету;
14) резервтік көшіруді және резервтік көшірмелерді сақтауды жүзеге асыру;
15) жұмыскерлердің АҚ мәселелері бойынша хабардарлығын арттыру;
16) АҚ мониторингін жүргізу және АҚ оқиғалары мен инциденттерін басқару;
17) АҚ басқару.

АҚБЖ-ның қолданылу саласы қамтиды:

1) Банктің барлық бизнес-процестері;
2) Банктің барлық құрылымдық бөлімшелері;
3) Банктің бас кеңсесі мен филиалдарының барлық ғимараттары.

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

Банктің ақпараттық активтерінде құрылатын, сақталатын және өңделетін ақпаратқа қолжетімділікті басқаруға қойылатын талаптар пайдаланушы қолжетімділігінің өмірлік циклінің барлық кезеңдерін қамтиды, жаңа пайдаланушыларды бастапқы тіркеуден бастап, ААЖ-ге және сервистерге қолжетімділік қажет болмай қалған пайдаланушыларды соңғы тіркеуден шығаруына дейін.

Жұмыскер Банктің құрылымдық бөлімшесі басшысы қол қойған және бизнес-процесс иесімен келісілген ресімделген өтінім негізінде рөлмен (рөлдер тізбесімен) қамтамасыз етіледі.

Пайдаланушыға функционалдық міндеттерін орындау үшін ең аз қажетті өкілеттіктер ғана берілуі тиіс және қызметтік міндеттері өзгерген немесе Банктің жұмыскері жұмыстан босатылған жағдайда барлық құқықтар кері қайтарылуы тиіс.

Банктің ААЖ-не шарттың/келісімнің талаптарына сәйкес қолжетімділік беруді талап ететін үшінші тұлғалармен (жабдықты техникалық сүйемелдеу, ақпараттық жүйелерді енгізуді сүйемелдеу) құпиялылық туралы келісім жасалуы тиіс (оның ішінде серіктестермен).

Ақпараттық активтерді үшінші тұлғаларға беру жағдайында (Банктің серверлік қуаттарын үшінші тараптың деректерді өңдеу орталықтарында орналастыру, деректерді өңдеу және/немесе сақтау бойынша сыртқы сервистерді пайдалану) Банк АҚ қамтамасыз ету бойынша келесі шараларды қабылдайды:

1) Банктің ақпараттық активтерін қорғауға қойылатын талаптарды және Банктің осындай талаптардың орындалуын тексеру құқығын, сондай-ақ АҚ және ААЖ-нің жұмыс қабілеттілігінің бұзылуы салдарынан туындаған залалды өтеу шарттарын үшінші тұлғамен тиісті келісімде/шартта көрсету;
2) Қазақстан Республикасының азаматтық, банк заңнамасына, Қазақстан Республикасының дербес деректер және оларды қорғау туралы заңнамасына сәйкес үшінші тұлғаларға берілуіне жол берілмейтін ақпаратқа үшінші тұлғалардың қол жеткізу мүмкіндігін болдырмау.

АҚ қамтамасыз ету жөніндегі қызметке мониторинг жүргізуге және қауіптерді анықтау мен талдау, шабуылдарға қарсы іс-қимыл жасау және АҚ инциденттерін тергеп-тексеру жөніндегі іс-шараларды жүзеге асыруға қойылатын талаптар

АҚ инциденттеріне ден қою тәртібі мынадай кезеңдерден тұрады, бірақ олармен шектелмейді:

1) АҚ оқиғаларына мониторинг жүргізу және АҚ инциденттерін анықтау (бұдан әрі – мониторинг және анықтау кезеңі);
2) АҚ инцидентін оқшаулау және оған қарсы іс-қимыл жасау (бұдан әрі – әрекет ету кезеңі);
3) АҚ инцидентін ішкі тергеп-тексеру (бұдан әрі – ішкі тергеп-тексеру кезеңі).

АҚ қамтамасыз ету жөніндегі қызметке мониторинг жүргізу кезеңінде АҚ бойынша бөлімше тарапынан келесі іс-шаралар жүзеге асырылады:

1) АҚ оқиғаларына мониторинг жүргізу және талдау;
2) АҚ оқиғаларын АҚ инциденттеріне жатқызудың әзірленген тәртібіне сәйкес АҚ оқиғаларын АҚ инциденттеріне жатқызу;
3) АҚ инциденттерін жіктеу және басымдылығын айқындау;
4) АҚ инциденті туралы ақпаратты әрекет ету кезеңіне беру.

АҚ инциденттеріне әрекет ету кезеңінде стандартты әрекет ету рәсімдері қолданылады, ал стандартты әрекет ету рәсімдерін қолданудың тиімділігі төмен болған жағдайларда АҚ инциденттеріне жедел әрекет ету шаралары қабылданады, олар келесі шараларды қамтиды, бірақ олармен шектелмейді:

1) АҚ инцидентіне тиімді қарсы іс-қимыл жасау процесін қамтамасыз ету мақсатында Банктің жұмыскерлерін, сондай-ақ қажет болған жағдайда үшінші тұлғаларды хабардар ету және әрекет ету процесіне тарту;
2) бизнес-процесс иелерімен келісу бойынша Банкте бизнес-процесті ішінара немесе толық тоқтату бойынша қосымша бақылау шараларын қолдану;
3) АҚ инцидентіне тартылған бағдарламалық-техникалық құралдардан деректер жинау;
4) АҚ инцидентін талдау, оны оқшаулау және оның салдарын жою;
5) АҚ оқиғаларына ретроспективті талдау жүргізу;
6) АҚ инциденттеріне әрекет ету барысында анықталған компрометация индикаторларын және осалдықтарды айқындау және кейіннен осындай АҚ инциденттерінің қайталануына жол бермеуге бағытталған түзету шараларын іске асыру;
7) АҚ инцидентіне ішкі тергеп-тексеру жүргізу қажеттілігі туралы шешім қабылдау.

Инцидентті ішкі тергеп-тексеру кезеңінде Банк АҚ-мен қамтамасыз етеді:

1) АҚ инцидентін ішкі тергеп-тексеруге АҚ инциденттеріне әрекет ету процесіне тартылған жауапты жұмыскерлерді және (немесе) Банктің бөлімшелерін, сондай-ақ үшінші тұлғаларды тарту;
2) АҚ инцидентін ішкі тергеп-тексеруді жүргізу үшін қажетті материалдарды жинау және талдау;
3) АҚ инцидентінің туындау себептерін және инциденттің іске асырылу тәртібін анықтау;
4) АҚ инцидентінің іске асырылуынан келтірілген әсер ауқымын және залалды бағалау;
5) тергеліп жатқан АҚ инцидентіне қатысты қабылданған әрекет ету шараларының тиімділігін талдау;
6) АҚ инцидентін тергеп-тексеру нәтижелері бойынша АҚ инциденті туралы ақпаратты қамтитын, сондай-ақ АҚ инцидентінің қайта іске асу ықтималдығын және ықтимал залалды азайту мақсатында түзету шараларын қабылдау жөніндегі ұсынымдар берілетін қорытындыны дайындау.

АҚ инциденттері туралы ақпаратқа талдау жүргізуге қойылатын талаптар

АҚ инциденттері туралы ақпаратты талдаудың негізгі мақсаттары болып табылады:
1) АҚ инциденті туралы ақпараттың толықтығы мен дәлдігін қамтамасыз ету;
2) салдарларды және келтірілген залалды айқындау;
3) қайталанатын АҚ инциденттерінің алдын алуға қабілетті шабуыл әдістері мен бақылау құралдарын айқындау;
4) АҚ қатерін толық жою үшін қабылдануы мүмкін іс-әрекеттерді айқындау;
5) АҚ инцидентінің негізгі себебін анықтау.

Саясат Банктің барлық жұмыскерлері, үшінші тұлғалар үшін міндетті түрде орындалуға жатады, сондай-ақ Банктің ақпараттық активтері мен ішкі құжаттарына қолжетімділігі бар сервистер жеткізушілеріне де, Банкпен және олардың қызметімен тікелей өзара байланысты бөлігінде, танысу үшін жеткізіледі.

Саясат Қазақстан Республикасының заңнамасы және/немесе Банктің ішкі құжаттары өзгерген/толықтырылған жағдайда қайта қаралуға жатады.