

Жасанды интеллект технологиясын қолдану

Банкте Басқарма мақұлдаған және Банктің Директорлар кеңесі бекіткен Жасанды интеллект технологиясын қолдану саясаты (бұдан әрі – Саясат) қолданылады. Саясат банктік қызметтерді көрсету процестерінде жасанды интеллект (бұдан әрі – ЖИ) технологиясын қолданудың мақсаттарын, міндеттері мен қағидаттарын, сондай-ақ Банктің қызметінде ЖИ жүйелерін енгізу, пайдалану және бақылау тәртібін айқындайды.

Саясат Қазақстан Республикасының заңнамасының талаптарына, оның ішінде «Қазақстан Республикасындағы банктер және банк қызметі туралы», «Дербес деректер және оларды қорғау туралы», «Ақпараттандыру туралы» Қазақстан Республикасы заңдарына, Қазақстан Республикасы Қаржы нарығын реттеу және дамыту агенттігінің нормативтік құқықтық актілеріне сәйкес әзірленген, сондай-ақ NIST Artificial Intelligence Risk Management Framework және Еуропалық Одақтың «AI Act» регламентіне негізделген.

Саясат Банктің барлық қызметкерлері үшін, сондай-ақ ЖИ технологиясын қолдануға байланысты қызметті жоспарлау және жүзеге асыру кезінде, оның ішінде ЖИ жүйелерін әзірлеу, енгізу, пайдалану және бақылау барысында үшінші тұлғалар үшін міндетті болып табылады.

1. ЖИ қолданудың негізгі қағидаттары

Банкте ЖИ қолдану келесі қағидаттарға негізделеді:

Заңдылық – ЖИ-ді жобалау, әзірлеу, пайдалану және дамыту кезінде Қазақстан Республикасының заңнамалық актілерін сақтай отырып, этикалық және моральдық нормаларды қатаң ұстану;

Ашықтық – ЖИ шешім қабылдау алгоритмдерінің түсініктілігін және осы процестегі айқындаушы факторлардың түсіндірмелілігін қамтамасыз ету;

Әділдік – әрбір адамның теңдігін, қадір-қасиетін, бірдей құндылығы мен құқықтарын қамтамасыз ету, кез келген кемсітушілікті болдырмау;

Сенімділік – ақауға төзімді есептеу және инфрақұрылымдық шешімдерді пайдалану, бұл ретте ЖИ технологиялары мен жүйелерінің әзірлеушілері мен иелері олардың тек жарияланған мақсаттарда жұмыс істеуіне кепілдік береді, жасырын алгоритмдер мен жарияланбаған мүмкіндіктерді пайдалануға жол берілмейді;

Ақпараттық қауіпсіздікті қамтамасыз ету – Банктің ЖИ ақпараттандыру объектілерінің құпиялылығы, тұтастығы және қолжетімділігі күйін қолдауға бағытталған процесс;

Құпиялылықты қамтамасыз ету – ЖИ қолдану кезінде деректерді жинау, өңдеу және сақтау барысында Қазақстан Республикасы заңнамасының талаптарын сақтау, деректердің тиісті қорғалуын қамтамасыз ету (оның ішінде рұқсатсыз қол жеткізуден немесе заңсыз өңдеуден/беруден/таратудан/сақтаудан қорғау);

Кибертұрақтылық – деректерді бұрмалау, араласу және манипуляциялау сияқты сыртқы және ішкі қауіптерден қорғалу;

Тәуекелге бағдарлану – бизнес-процестерде ЖИ қолдануға байланысты ықтимал тәуекелдерді анықтау және оларды басқару саясатын енгізу;

Бақыланушылық – шешім қабылдау процесін бақылау және басқаруда адамның белсенді қатысуын қамтамасыз ету, ЖИ жүйелерінің жұмысын тұрақты мониторингтеу және сыни бағалау.

Аталған қағидаттар Саясат негізделген ЕО-ның «AI Act» регламентінің талаптарын ескере отырып іске асырылады: ЖИ жүйелерінің жұмыс істеуі тек жарияланған мақсаттар шеңберінде қамтамасыз етіледі, жасырын алгоритмдерге, жарияланбаған мүмкіндіктерге және кез келген кемсітушілікке жол берілмейді, оның ішінде «AI Act» регламентімен тыйым салынған тәжірибелерге жататын манипуляциялық ықпал ету, адамның осал тұстарын пайдалану, әлеуметтік скоринг және рұқсатсыз биометриялық бақылау.

2. Клиенттердің құқықтары

Банк клиенттердің келесі құқықтарын қамтамасыз етеді:

Білу құқығы. Клиент Қазақстан Республикасының заңнамасына сәйкес оның Банктегі қаржылық активтеріне қатысты шешімдер қабылдауға ЖИ қатысатынын білуге құқылы;

Шағымдану құқығы. ЖИ қатысуымен қабылданған барлық шешімдер белгіленген тәртіппен шағымдануға жатады, оның ішінде Банк қызметкерін және/немесе ЖИ жүйесін әзірлеушілерді/жеткізушілерді тарту кезеңі қарастырылады (егер ЖИ жүйесі Банк үшін үшінші тұлғалармен әзірленген болса);

Бас тарту құқығы. Клиент Қазақстан Республикасының заңнамасына қайшы келмеген жағдайда автоматтандырылған процестерге қатысудан бас тартуға, сондай-ақ деректерді жинауға және өндеуге берген келісімін қайтарып алуға құқылы;

ЖИ қолданылуы туралы ақпарат алу құқығы. Клиенттің сұрауы бойынша Банк Қазақстан Республикасының заңнамасы шеңберінде оның деректерін өңдеу кезінде ЖИ қолданылуы туралы қажетті ақпаратты ұсынуға міндеттенеді;

Жеке деректердің үшінші тұлғаларға берілмеуін қамтамасыз ету құқығы. Банк клиенттер туралы деректерді, оның ішінде иесіздендірілген деректерді, үшінші тұлғаларға, ортақ деректер кеңістіктеріне және т.б. бермейді, егер мұндай беру Қазақстан Республикасы заңнамасының талабы болмаса.

3. Тәуекелдерді ішкі бағалау

Енгізу алдында әрбір ЖИ жүйесі келесі өлшемшарттар бойынша ішкі тәуекелдерді бағалауға жатады: клиентке немесе контрагентке, қызметкерге, бизнес-процестерге және Банктің беделіне ықпалы; дербес және сезімтал деректерді, сондай-ақ Банктің қорғалатын ақпаратын өңдеу/сақтау; егер ЖИ жүйесі Банк үшін үшінші тұлғалармен әзірленген болса, дербес деректерді қорғау және қорғалатын ақпаратқа қойылатын талаптарды, оның ішінде клиенттің дербес деректерін трансшекаралық беру талаптарын сақтау; Қазақстан Республикасының заңнамасына және Банктің ақпараттық қауіпсіздік стандарттарына сәйкес қабылданған ақпараттық қауіпсіздік талаптарын сақтау; шешім қабылдаудың автономдылығы; кемсітушілік ықтималдығы; деректер сапасы; әрекеттердің даусыздығы; Банктің қызметкерлері тарапынан шешімдердің қайтарымдылығы.

Тәуекелдерді бағалау тәуекелдер картасы түрінде ресімделеді: әрбір тәуекел сипатталады (ықтимал туындау орындары, тәуекел көздері, тәуекелге алып келетін оқиғалар) және бағаланады (қаржылық және қаржылық емес салдарлар), әрбір тәуекел бойынша оны

төмендету жөніндегі іс-шаралар әзірленеді. Тәуекелдер картасына этикалық, техникалық, операциялық және реттеушілік тәуекелдер міндетті түрде енгізіледі. Тәуекелдерден қорғау ҚР ҚНРДА нормативтік актілері мен Банктің тәуекелдерді басқару саласындағы ішкі нормативтік құжаттарына сәйкес үш қорғаныс желісі қағидаты негізінде жүзеге асырылады.

4. ЖИ жүйелерінің өмірлік циклі

Банк ЖИ жүйесінің толық өмірлік циклін басқаруды жүзеге асырады, оған қарастыру, жобалау, әзірлеу немесе енгізу, тестілеу, пайдалануға енгізу, пайдалану, сүйемелдеу, мониторинг және тиімділікті тұрақты бағалау (оның ішінде ЖИ жүйесін үздіксіз жетілдіру процесі), сондай-ақ пайдаланудан шығару кіреді. Әрбір ЖИ жүйесі үшін Банктің қызметкерлері арасынан оның Бизнес-иесі, Деректер иесі, операторы және IT-менеджері (әкімшісі), сондай-ақ ЖИ жүйесіне тартылған және/немесе оны қолдау үшін қажетті ақпараттық активтер айқындалады.

5. Басқару және бақылау

ЖИ қолдану процесін басқару ЖИ жөніндегі комитетке жүктеледі. Бұл алқалы орган ЖИ жүйелерін қолдану міндеттері бойынша шешімдер қабылдауға уәкілетті және ЖИ басқаруды орталықтандыруды, сондай-ақ ЖИ қолдану қағидаттарын сақтауды қамтамасыз етеді. ЖИ жөніндегі комитет құрамына міндетті түрде, бірақ онымен шектелмей, Банктің тәуекелдерді басқару, ақпараттық технологиялар, ақпараттық қауіпсіздік және деректерді басқару бөлімшелерінің өкілдері енгізіледі. ЖИ жөніндегі комитет ЖИ қолданудың мақсатты салаларын айқындайды. Банкте ЖИ саласындағы кез келген зерттеу жұмысы ЖИ жөніндегі комитетті міндетті түрде хабардар ете отырып жүргізіледі.

Банк ЖИ қолдану процестерін регламенттейтін ішкі рәсімдерді әзірлейді және іске асырады, оның ішінде пайдаланылатын ЖИ жүйелерінің тізілімін қалыптастыру және жүргізу, ЖИ тәуекелдік профилі бойынша жыл сайынғы есептілікті ұсыну, ЖИ әзірлеу және қолдану регламенті, үлгілік тәуекелдер картасы және оларды басқару тәсілдері, сондай-ақ ЖИ қолданудың мақсатты салаларын айқындау тәртібі.

6. Мониторинг және есептілік

Саясат қағидаттарын іске асыру бөлігінде Банктің қызметін және қол жеткізілген прогресті бағалау мақсатында ЖИ жобаларын іске асыруға, Банктің ЖИ саласындағы қызметінің Саясат ережелеріне және Қазақстан Республикасының заңнамасына сәйкестігіне бақылау және мониторинг жүргізіледі. ЖИ жөніндегі комитет Банктің Директорлар кеңесіне ұсынылатын есептіліктің тізбесін, нысанын және мерзімділігін айқындайды. Саясаттың иесі және оны іске асыруға жауапты тұлға ретінде деректерді басқару және ЖИ мәселелеріне жауапты Банктің бөлімшесі белгіленеді. Банктің қызметкерлері, оның ішінде лауазымды тұлғалар, Саясат ережелерін орындамағаны және (немесе) тиісінше орындамағаны үшін жауапты болады.