

Қазақстан Республикасы
Ұлттық Банкі
Директорлар кеңесінің
2018 жылғы «28» сәуірдегі
№ 75 қаулысымен
бекітілген

Қазақстан Республикасы Ұлттық Банкінің ақпараттық қауіпсіздік саясаты

(Өзгерістер мен толықтырулар: ДҚК ҚРҰБ № 85 2021ж. 28.12.)

1. Жалпы ережелер

1. Қазақстан Республикасы Ұлттық Банкінің ақпараттық қауіпсіздік саясаты (бұдан әрі – Саясат) Қазақстан Республикасы Ұлттық Банкінің (бұдан әрі – Ұлттық Банк) орталық аппаратында, филиалдарында және өкілдігінде ақпараттық қауіпсіздік мақсатын және оны қамтамасыз етуге қойылатын негізгі тәсілдерді айқындайды.

2. Саясат «Қазақстан Республикасының ұлттық қауіпсіздігі туралы» Қазақстан Республикасының Заңына, «Киберқауіпсіздік тұжырымдамасын («Қазақстанның киберқалқаны») бекіту туралы» Қазақстан Республикасы Үкіметінің 2017 жылғы 30 маусымдағы № 407 қаулысына және Қазақстан Республикасының басқа да нормативтік құқықтық актілеріне, сондай-ақ Қазақстан Республикасының ISO/IEC 27001 стандартына¹ сәйкес әзірленді.

3. Ұлттық Банктің басшылығы ақпараттық қауіпсіздіктің қазіргі тәуекелдері және заңнаманы жетілдіру аясында ақпараттық қауіпсіздікті басқару жүйесін (бұдан әрі – АҚБЖ) құру, дамыту және тұрақты түрде жетілдіру маңыздылығын және қажеттілігін түсінеді.

2. Саясаттың қолданылу аясы

4. Саясаттың қолданылу аясы:

1) Ұлттық Банкте электрондық немесе қағаз түрінде өңделгендігіне қарамастан, қызметті жүзеге асырған кезде маңызды ақпараттық актив болып табылатын бүкіл ақпаратты;

2) Ұлттық Банктің қызметін қамтамасыз ету үшін пайдаланылатын ақпаратты өндеудің барлық құралдарын;

¹ ISO/IEC 27001 ҚР СТ Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері. Ақпараттық қауіпсіздіктің менеджмент жүйелері. Талаптар.

3) келісімдерге (шарттарға) сәйкес Ұлттық Банкпен ынтымақтастықты немесе қызмет көрсетуді жүзеге асыратын барлық басқа ұйымдарды қамтиды.

3. Саясаттың мақсаты

5. Саясаттың мақсаты ақпаратты өңдеу және сақтау нысанына, орнына және құралдарына қарамастан ақпаратты қорғауды ұйымдастыруға бағытталған Ұлттық Банктің ақпараттық қауіпсіздігін қамтамасыз етудегі бірыңғай тәсілді айқындау болып табылады.

4. Негізгі ережелер

6. Саясаттың мақсатына қол жеткізу үшін Ұлттық Банкте АҚБЖ енгізіледі, ол:

1) ақпараттық активтерді ақпараттық қауіпсіздік қатерлерінен қорғау шараларының және құралдарының жеткіліктілігін қамтамасыз етуге;

2) ақпараттық қауіпсіздікті бақылау шараларын және құралдарын қолдануға, ақпараттық қауіпсіздік тәуекелдерін бағалау мен талдау жүргізу нәтижелері негізінде оларды үздіксіз жақсартуға;

3) ақпараттық қауіпсіздіктің оқыс оқиғаларына уақтылы және барабар ден қоюға;

4) Қазақстан Республикасы заңнамасының талаптарына сәйкес келуге;

5) ақпараттық қауіпсіздікті қамтамасыз етуді бақылау ортасын үздіксіз жақсартуға мүмкіндік береді.

7. Ұлттық Банкте Саясатты іске асыру АҚБЖ-ның мынадай талаптарын сақтауға негізделген:

1) ақпараттық қауіпсіздіктің тәуекелдерін үнемі сәйкестендіру мен бағалауды жүргізу;

2) ақпараттық қауіпсіздіктің оқыс оқиғаларын басқаруды жүзеге асыру;

3) Қазақстан Республикасының ақпараттық қауіпсіздік саласындағы талаптарын орындау;

4) ақпараттық активтерді және ақпаратты өңдеу құралдарын нысансыз пайдалануға тыйым белгілеу;

5) Ұлттық Банктің барлық қызметкерлеріне Саясаттың талаптарын жеткізу;

6) Ұлттық Банк қызметкерлерінің ақпараттық қауіпсіздікті қамтамасыз ету мәселелерінде хабардарлығын арттыру жөніндегі тұрақты іс-шараларды өткізу;

7) ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі іс-шараларды және ақпаратты өңдеу мен сақтау процестерін ұйымдастыру мен жүзеге асыруға жауапты Ұлттық Банк қызметкерлерінің ақпараттық қауіпсіздік саласындағы оқудан өтуі.

5. Жауапкершілік және бақылау

8. Ұлттық Банктің басшылығы Ұлттық Банктегі ақпараттық қауіпсіздікті қамтамасыз етуге жалпы бақылауды жүзеге асырады, АҚБЖ үйлестіру, енгізу, дамыту мен жетілдіру арқылы Саясаттың мақсатына қол жеткізуді қамтамасыз етеді.

9. Ұлттық Банкте ақпараттық қауіпсіздікті, Саясаттың іске асырылуын қамтамасыз етуді, сондай-ақ Ұлттық Банкте белгіленген ақпараттық қауіпсіздік жөніндегі талаптар мен іс-шаралардың орындалуын үздіксіз бақылауды қауіпсіздік бөлімшесі (филиалдарда, өкілдікте – ақпараттық қауіпсіздікке жауапты адам) жүзеге асырады.

10. Ұлттық Банктің қызметкерлері ақпаратты және оны өңдеу құралдарын қорғау жөніндегі талаптарды және іс-шараларды бұзғаны және/немесе орындамағаны үшін дербес жауапкершілік атқарады.

Ұлттық Банктің қызметкерлері барлық анықталған жөнсіздіктер және оқыс оқиғалар туралы қауіпсіздік бөлімшесіне (филиалдарда, өкілдікте – ақпараттық қауіпсіздікке жауапты адамға) хабарлауға міндетті.

6. Басқа ережелер

11. Саясат:

- 1) ақпараттық қауіпсіздікті басқару жүйесінің жай-күйі мен тиімділігін;
- 2) ақпараттық қауіпсіздіктің жай-күйін ағымдағы тексерулерді;
- 3) ақпараттық қауіпсіздіктің анықталған тәуекелдерін, оқыс оқиғаларын және талаптарын бұзуды;
- 4) Қазақстан Республикасының заңнамасын және Ұлттық Банктің актілерін;
- 5) Ұлттық Банктің аудит нәтижелерін жыл сайынғы талдау мен бағалау негізінде қайта қаралады.