Директорлар кеңесінің 19.02.2024 ж.
№0219/1 қаулысына қосымша

Басқарманың 29.01.2024 ж. № 0129/8
хаттамасымен мақұлданған

«Банк ЦентрКредит» АҚ-тың
Ақпараттық қауіпсіздік саясаты

Мазмұны:

1. Жалпы қағидалар

1. Осы Ақпараттық қауіпсіздік саясаты (бұдан әрі – Саясат) Банктің ақпараттық қауіпсіздікті басқару жүйесінің (бұдан әрі – АҚБЖ) мақсаттарын, міндеттерін және іс-әрекет ету саласын белгілейтін, «Банк ЦентрКредит» АҚ-тың (бұдан әрі – Банк) ақпараттық қауіпсіздікті басқару жүйесінің негізін қалайтын құжат болып табылады.

2. АҚБЖ банктің бизнес-процесі үшін ықтимал залалдың ең төменгі деңгейіне жол беретін Банктің ақпараттық активтерін қорғауды қамтамасыз етеді.

3. Саясат Қазақстан Республикасының заңнамасына, соның ішінде екінші деңгейдегі банктердің ақпараттық қауіпсіздігін қамтамасыз ету талаптарын реттейтін нормативтік құқықтық актілерге, сонымен қатар ақпараттық қауіпсіздік саласындағы халықаралық стандарттардың талаптарына сәйкес әзірленген.

4. Банктің ақпараттық қауіпсіздігін басқару жүйесінің процестеріне қойылатын және осы Саясатта сипатталған талаптар «Банктердің, Қазақстан Республикасының бейрезидент-банктері филиалдарының және банк операцияларының жекелеген түрлерін жүзеге асыратын ұйымдардың ақпараттық қауіпсіздігін қамтамасыз етуге қойылатын талаптарды, Ақпараттық жүйелердегі бұзушылықтар, іркілістер туралы мәліметтерді қоса алғанда, ақпараттық қауіпсіздіктің оқыс оқиғалары туралы ақпаратты беру қағидалары мен мерзімдерін бекіту туралы» Қазақстан Республикасы Ұлттық Банкі Басқармасының 2018 жылғы 27 наурыздағы №48 қаулысының «Ақпараттық қауіпсіздікті басқару жүйесінің процестеріне қойылатын талаптар» атты 9-бөліміне сәйкес әзірленген Банктің ішкі нормативтік құжаттарында толық сипатталған.

2. Ақпараттық қауіпсіздікті басқару жүйесінің мақсаттары, міндеттері және негізгі принциптері

5. Банктің бірінші басшысы ақпараттық қауіпсіздікті қамтамасыз ету процесін басқаруға арналған Банктің жалпы басқару жүйесінің, ұйымның бөлігі болып табылатын АҚБЖ құрылуын, оның жұмыс істеуін және жақсартуын қамтамасыз етеді.

6. АҚБЖ мақсаты – ақпараттық қауіпсіздікті қамтамасыз ету процесін арттыру, конфиденциалдылықтың талап етілген деңгейін қамтамасыз ету, маңызды ақпараттық активтердің тұтастығы және қолжетімділігі және салдарынан ақпараттық қауіпсіздік тәуекелдерін және оған байланысты залалды азайту.

7. АҚБЖ міндеттеріне төмендегілер жатады:

1) ақпараттық активтерді санатқа бөлу;

2) ақпараттық активтерді пайдалану құқығын беруді ұйымдастыруды;

3) ақпараттық инфрақұрылымның қауіпсіздігін қамтамасыз ету;

4) ақпараттық қауіпсіздікті және ақпараттық қауіпсіздіктің оқыс оқиғалары бойынша қауіп пен осалдықты анықтау және талдау, қақтығыстарға қарсы тұру және тергеу бойынша іс-шараларды қамтамасыз етуге қатысты қызметке мониторинг жүргізу;

5) ақпараттық қауіпсіздіктің оқыс оқиғалары туралы ақпаратты, оған қоса ақпараттық жүйелердегі бұзылулар, ақаулар туралы мәліметтерді талдау;

6) ақпаратты криптографиялық қорғау құралдарын басқару тәртібін белгілеу;

7) үшінші тұлғалар ақпараттық активтерді пайдаланған кезде ақпараттық қауіпсіздікті қамтамасыз ету;

8) ақпараттық қауіпсіздіктің жай-күйіне ішкі тексерулер жүргізу.

8. АҚБЖ құру және оның қызмет етуі келесі негізгі принциптерге сәйкес жүзеге асырылады:

1) заңдылық – ақпараттық қауіпсіздікті қамтамасыз ету үшін қабылданатын кез келген іс-әрекеттер қолданыстағы заңнаманың негізінде, заң рұқсат ететін Банктің ақпараттық активтеріне теріс әсер ететін жағдайларды анықтау, олардың алдын алу, оқшаулау және жою әдістерін қолдану арқылы жүзеге асырылады;

2) бизнеске бағдарлау – ақпараттық қауіпсіздік негізгі қызметті қолдау процесі ретінде қаралады, ақпараттық қауіпсіздікті қамтамасыз ету бойынша кез келген шаралар бизнесті жүргізу үшін маңызды кедергілерге әкеп соқпауы тиіс;

3) кешенділік – барлық өмірлік циклі ішінде, оларды пайдаланудың барлық технологиялық кезеңдерінде және барлық қызмет ету режимінде ақпараттық активтердің қауіпсіздігін қамтамасыз ету;

4) негізділік және экономикалық мақсаттылық – пайдаланылатын мүмкіндіктер мен қорғаныс құралдары ғылым мен техниканың дамуының сәйкес кезеңінде іске асырылуы, белгіленген қауіпсіздік деңгейінің көзқарасымен негізделген болуы қажет және белгіленген талаптар мен нормаларға сәйкес келуі тиіс. Барлық жағдайда ақпараттық қауіпсіздікті қамтамасыз ету бойынша шаралар мен технологиялық шешімдердің құны қорғалатын ақпараттық активтердің құнынан аспауы қажет;

5) бейімділік – олардың маңыздылығына сәйкес ақпараттық активтерді қорғау әдістері мен құралдарын анықтау және қолдану;

6) қажетті білім мен артықшылықтың төмен деңгейі – пайдаланушы өз өкілеттіктері шегінде қызметін орындау үшін қажет болатын ақпараттық активтерге ғана артықшылықтардың ең төмен деңгейі мен пайдалану рұқсатын алады;

7) мамандану – ақпараттық қауіпсіздікті қамтамасыз ету бойынша шараларды іске асыруды және технологиялық шешімдерді пайдалануды кәсіби тұрғыда даярланған мамандар жүзеге асыруы қажет;

8) ақпараттылық және жауапкершілік – барлық деңгейдегі басшылар және орындаушылар ақпараттық қауіпсіздіктің барлық талаптары жөнінде хабардар болуы қажет және осы талаптарды орындау, сонымен қатар ақпараттық қауіпсіздіктің белгіленген шараларын сақтау үшін жеке жауап береді;

9) Бірлесіп әрекет ету және үйлестіру – ақпараттық қауіпсіздік шаралары Банктің сәйкес құрылымдық бөлімшелерінің бірлесіп әрекет етуі, алдыға қойылған мақсаттарға қолжеткізу үшін күшін үйлестіру, сонымен қатар сыртқы ұйымдармен, кәсіби қауымдастықтармен және қоғамдастықтармен, мемлекеттік органдармен, заңды және жеке тұлғалармен қажетті байланыс орнату негізінде жүзеге асырылады;

10) растау – ақпараттық қауіпсіздік және АҚБЖ тиімділігі бойынша талаптардың орындалуын растайтын куәліктер жедел қолжеткізу және қалпына келтіру мүмкіндігімен әзірленуі және сақталуы қажет.

3. Ақпараттық қауіпсіздікті басқару жүйесінің әрекет ету саласы

9. АҚБЖ-ның қолданылу аясы клиенттерге қызмет көрсетуге тікелей бағдарланған, клиенттер үшін құнды болып табылатын және процедурамен белгіленген пайда табуды, бизнес-процестердің жіктелуін, сондай-ақ Банктің куәландырушы орталығының қызметін қамтамасыз ететін процестерді қамтамасыз ететін Банктің негізгі бизнес-процестері болып табылады.

10. Қорғаныс объектілері болып негізгі бизнес-процестердің қызмет етуі үшін қажетті маңызды ақпараттық активтер танылады, оларға төмендегілер жатады:

1) Ақпаратты өңдеудің жеке құрылғылары;
2) Ақпаратты тасымалдағыш;
3) Сыртқы компьютерлік жабдық;
4) Серверлер;
5) Желілік жабдық;
6) Телефония аппаратурасы;
7) Жеке байланыс арнасы;
8) Деректер базасы;
9) Виртуалды байланыс арнасы;
10) Шолу жүйелері;
11) Операциялық жүйелер;
12) Аппараттық құрылғылардың бағдарламалық қамсыздандыруы;
13) Қолданбалы бағдарламалық қамсыздандыру;
14) Телефониялы бағдарламалық қамсыздандыруы.
15) Ақпаратты криптографиялық қорғау құралдары.

4. Банктің ақпараттық жүйелерінде құрылатын, сақталатын және өңделетін ақпаратты пайдалану талаптары және ақпаратқа және оның пайдаланылуына мониторинг жүргізу

11. Банктің ақпараты мен ақпараттық жүйелерін пайдалану құқығы жұмыскерлерге қызметтік міндеттерін орындау үшін қажетті көлемде ұсынылады.

12. Банктің маңызды ақпараттық жүйелерін пайдалану құқығы ақпараттық жүйелерді пайдаланушылардың рұқсат беру құқығының олардың қызметтік міндеттеріне сәйкестігін қамтамасыз етуге арналған рөлдерді қалыптастыру және енгізу арқылы беріледі.

13. Банктің жұмыскері болып табылмайтын тұлғаларға (бұдан әрі – үшінші тұлғалар) Банктің ақпараттық активтерін пайдалану құқығы Қазақстан Республикасының заңнамасында көзделген жағдайларды қоспағанда, ақпараттық қауіпсіздікке қойылатын талаптарды сақтау туралы сәйкес келісімнің негізінде жұмыстарды жүргізу үшін қажетті кезеңге және көлемде беріледі. Үшінші тұлғалармен жасалатын ақпараттық қауіпсіздікке қойылатын талаптарды сақтау туралы келісім конфиденциалдылық туралы қағидаларды, ақпараттық қауіпсіздікті бұзу, сонымен қатар ақпараттық жүйелердегі ақаулар мен оның қауіпсіздігін бұзу салдарынан туындаған, үшінші тұлғалардың араласуынан туындаған залалды өтеу туралы талаптарын қамтиды.

5. Ақпараттық қауіпсіздікті қамтамасыз ету бойынша қызметке мониторинг жүргізуге және ақпараттық қауіпсіздіктің оқыс оқиғалары бойынша қауіпті анықтау және талдау, қақтығыстарға қарсы тұру және тергеу бойынша іс-шараларға қойылатын талаптар

14. Банк ақпараттық қауіпсіздіктің оқыс оқиғаларына ден қою бойынша құрылымдық бөлімшені – қауіпсіздіктің оқыс оқиғаларына ден қою қызметін құруды қамтамасыз етеді.

15. Банк ақпараттық қауіпсіздікті қамтамасыз ету бойынша қызметке және қауіптерді анықтау және талдау, шабуылдарға қарсы іс-қимыл және ақпараттық қауіпсіздік инциденттерін тергеу бойынша іс-шараларға тиісті мониторинг жүргізуді қамтамасыз етеді.

6. Ақпараттық қауіпсіздіктің оқыс оқиғалары туралы ақпаратты жинауға, шоғырландыруға және сақтауға қойылатын талаптар

16. Банк ақпараттық қауіпсіздіктің оқыс оқиғаларына ден қою тәртібін іске асыруды растайтын құжаттардың, мәліметтердің және фактілердің болуын, сонымен қатар ақпараттық қауіпсіздіктің оқыс оқиғалары, ақпараттық қауіпсіздіктің оқыс оқиғаларын ішкі тергеу нәтижелері туралы ақпараттың,

сонымен қатар қағаз және (немесе) электронды тасымалдағыштағы тергеу материалдарының шоғырлануын, жүйелендірілуін, тұтастығын және сақталуын қамтамасыз етеді.

7. Ақпараттық қауіпсіздіктің оқыс оқиғалары туралы ақпаратты талдауға қойылатын талаптар

17. Банк:

1) ақпараттық қауіпсіздік тәуекелдерін бағалау, ақпараттық қауіпсіздікті қамтамасыз ету әдістері мен құралдарын түзету, бизнесті өзгерту мақсатында анықталған ақпараттық қауіпсіздіктің оқыс оқиғаларына және Банктің алғалы органы қарастыруы үшін келтірілген залалға талдау жасауды;

2) ақпараттық қауіпсіздіктің оқыс оқиғаларына ден қою процесінің метрикаларын пайдалана отырып, ақпараттық қауіпсіздіктің оқыс оқиғаларына ден қою процесін түзету мақсатында тиімділікті талдауды;

3) ақпараттық қауіпсіздіктің оқыс оқиғаларына ден қою процесінің тиімділігін бағалау нәтижелерін есепке ала отырып, ақпараттық қауіпсіздіктің оқыс оқиғаларына ден қою процесінің метрикаларын қайта қарастыруды;

4) мониторинг жүргізілуі тиіс ақпараттық қауіпсіздіктің оқыс оқиғаларының тізбесін, оқиғалар көзін, ақпараттық қауіпсіздіктің оқыс оқиғаларына мониторинг жүргізу кезеңдігін, тәртібін және әдістерін қайта қарастыруды қамтамасыз етеді.

8. Банктің ақпараттық қауіпсіздікті қамтамасыз етуге жауапты жұмыскерлерінің жүктелген қызметтік міндеттерін орындаған кездегі жауапкершілігі

18. Банктің АҚБЖ қатысушылары:

1) Директорлар Кеңесі;

2) Басқарма;

3) ақпараттық қауіпсіздікті қамтамасыз ету міндеттері бойынша шешімдер қабылдауға уәкілетті алқалы орган (бұдан әрі – УАО);

4) Ақпараттық қауіпсіздік бойынша бөлімше;

5) Ақпараттық технологиялар бойынша бөлімше;

6) Қауіпсіздік бойынша бөлімше;

7) Қызметкерлермен жұмыс жүргізу бойынша бөлімше;

8) Заң бөлімшесі;

9) Комплаенс бақылау бойынша бөлімше;

10) Ішкі аудит бөлімшесі;

11) Ақпараттық технологиялар және ақпараттық қауіпсіздік тәуекелдерін басқару бойынша бөлімше;

12) Ақпараттық жүйелер мен кіші жүйелердің бизнес иелері;

13) Құрылымдық бөлімшелердің басшылары;

14) Құрылымдық бөлімшелердің жұмыскерлері.

19. Директорлар кеңесі ақпараттық қауіпсіздік саясатын және қорғалатын ақпарат тізімін, соның ішінде қызметтік, коммерциялық және заңмен қорғалатын басқа деректер туралы ақпаратты және қорғалатын ақпаратпен жұмыс жүргізу тәртібін бекітеді. Совет директоров при формировании бюджета учитывает потребности в ресурсах для обеспечения информационной безопасности Банка.

20. Басқарма ақпараттық қауіпсіздікті басқару процесін, қызметкерлерді оқыту бағдарламасын және оларды қайта қарастыру тәртібі мен кезеңділігі Банктің ішкі құжаттарымен белгіленетін ақпараттық қауіпсіздік бойынша ішкі нормативтік құжаттардың талаптарын білуге арналған тестілеуді өткізу жоспарын регламенттейтін ішкі нормативтік құжаттарды бекітеді.

21. Басқарма Басқарма берген өкілеттіктер аясында әрекет ететін ақпараттық қауіпсіздікті қамтамасыз ету мәселелері бойынша шешімдер қабылдау бойынша УАО-ның болуын қамтамасыз етеді.

22. Ақпараттық қауіпсіздік бойынша бөлімше Банктің ақпаратының конфиденциалдылығын, түгендігін және қолжетімділігін қамтамасыз ету мақсатында келесі қызметтерді жүзеге асырады:

1) ақпараттық қауіпсіздікті басқару жүйесін ұйымдастырады, ақпараттық қауіпсіздікті және қауіп-қатерді анықтау және талдау бойынша іс-шараларды қамтамасыз ету, шабуылдарға қарсы әрекет ету және ақпараттық қауіпсіздіктің оқыс оқиғаларын тергеу бойынша Банк бөлімшелерін үйлестіреді және олардың қызметін бақылайды;

2) Банктің ақпараттық қауіпсіздік саясатын әзірлейді;

3) Банктің ақпараттық қауіпсіздігін қамтамасыз ету процесіне әдіснамалық қолдау көрсетеді;

4) өзінің өкілеттіктері аясында Банктің ақпараттық қауіпсіздігін басқару, қамтамасыз ету және бақылау тәсілдерін, құралдары мен тетіктерін таңдауды, енгізуді жүзеге асырады;

5) ақпараттық қауіпсіздіктің оқыс оқиғалары туралы ақпаратты жинауды, шоғырландыруды, сақтауды және өңдеуді жүзеге асырады;

6) ақпараттық қауіпсіздіктің оқыс оқиғалары туралы ақпаратты талдауды жүзеге асырады;

7) ақпараттық қауіпсіздік комитеті ақпараттық қауіпсіздік мәселелері бойынша шешім қабылдауы үшін ұсыныстар әзірлейді;

8) Банктің ақпараттық қауіпсіздігін қамтамасыз ету процесін автоматтандыратын бағдарламалық-техникалық құраларды енгізуді, олардың тиісті түрде қызмет етуін, сонымен қатар оларға қолжеткізуді қамтамасыз етеді;

9) артықшылықты есептік жазбаларды пайдалану бойынша шектеулерді анықтайды;

10) Банк жұмыскерлерінің ақпараттық қауіпсіздік саласындағы хабардарлығын арттыру процесін ұйымдастыруға қатысады;

11) Банктің ақпараттық қауіпсіздігін басқару жүйесінің жай-күйіне мониторинг жүргізеді;

12) Банк басшылығына Банктің ақпараттық қауіпсіздігін басқару жүйесінің жай-күйі туралы ақпарат береді;

13) ақпараттық қауіпсіздік тәуекелдеріне бағалау жүргізеді;

14) ақпараттық қауіпсіздік тәуекелдерін өңдеу бойынша шаралар әзірлейді және Операциялық тәуекелдер дирекциясына оларды іске асыру бойынша есептілік ұсынады;

15) елеулі ақпараттық қауіпсіздік тәуекелдерін іске асыру туралы, сонымен қатар олардың салдарын жою туралы есептілікті әзірлейді және оларды Операциялық тәуекелдер дирекциясына ұсынады;

16) ақпараттық қауіпсіздікті қамтамасыз етуге қатысты Банктің стратегиясын іске асыру бойынша іс-шаралар жоспарын әзірлейді, олар келесі көрсетілгендерді ашып көрсетеді, бірақ олармен шектелмейді:

1) ресурстегі қажеттіліктерді анықтау, соның ішінде ақпараттық қауіпсіздік тәуекелдерін басқаруға бағытталған шараларды іске асыруға байланысты бюджетті анықтау;

2) мерзімі мен оларды іске асыру үшін жауапты орындаушыларды көрсетіп, ақпараттық қауіпсіздік саласында талап етілетін іс-шараларды сипаттау.

23. Ақпараттық технологиялар бойынша бөлімше келесі функцияларды жүзеге асырады:

1) Банктің ақпараттық инфрақұрылымының сұлбасын әзірлейді;

2) IT блогына қатысты болмайтын ақпараттық жүйелердің IT менеджерлері кіруге рұқсат беретін арнайы ақпараттық активтерді есепке алмағанда, пайдаланушылардың Банктің ақпараттық активтеріне кіру рұқсатын беруді қамтамасыз етеді;

3) Банктің жүйелік және қолданбалы бағдарламалық қамсыздандыруың конфигурациясын қамтамасыз етеді;

4) Банктің ішкі құжаттарына сәйкес ақпараттық инфрақұрылымның қызмет етуінің үздіксіздігі, Банктің аталған ақпараттық жүйелерінің конфиденциалдылығы, түгендігі мен қолжетімділігі бойынша белгіленген талаптарын орындалуын (ақпаратты резервтеу және (немесе) архивтеу және резервтік көшірмесін жасау) қамтамасыз етеді;

5) ақпараттық жүйелерді таңдаған, енгізген, әзірлеген және тестілеген кезде ақпараттық қауіпсіздіктің талаптарын сақтауды қамтамасыз етеді.

24. Қауіпсіздік бойынша бөлімше келесі функцияларды жүзеге асырады:

1) Банкте жеке және техникалық қауіпсіздік шараларын іске асырады, оған қаса кіруге рұқсат беруді және объекті ішіндегі режимді ұйымдастырады;

2) Банкте жұмыскерлерді жұмысқа қабылдаған және жұмыстан босатқан кезде ақпараттық қауіпсіздіктің қауіп-қатерінің пайда болу тәуекелін азайтуға бағытталған алдын ала іс-шараларды жүргізеді.

25. Қызметкерлермен жұмыс жүргізу бойынша бөлімше келесі функцияларды жүзеге асырады:

1) Банк жұмыскерлерінің, сонымен қатар қызмет көрсету шарты бойынша жұмысқа тартылған тұлғалардың, тәлімгерлердің, тәжірибеден өтушілердің конфиденциалды ақпаратты жария етпеу туралы міндеттемеге қол қоюын қамтамасыз етеді;

2) Банк жұмыскерлерінің ақпараттық қауіпсіздік саласындағы хабардарлығын арттыру процесін ұйымдастыруға қатысады.

3) Ақпараттық қауіпсіздік бойынша бөлімшенің жұмыскерлерін тағайындау және жұмыстан шығару туралы уәкілетті органды хабардар етеді.

26. Заң бөлімшесі ақпараттық қауіпсіздікті қамтамасыз ету мәселелері бойынша Банктің ішкі нормативтік құжаттарына құқықтық сараптама жүргізеді.

27. Комплаенс бақылау бойынша бөлімше Заң бөлімшесімен бірге осы Саясаттың 19-тармағында көрсетілген қорғалатын ақпараттың тізіміне қосылуы тиіс ақпарат түрлерін анықтайды.

28. Ішкі аудит бөлімшесі Банктің ішкі аудит қызметінің жүйесін ұйымдастыруды реттейтін Банктің ішкі нормативтік құжаттарына сәйкес Банктің ақпараттық қауіпсіздігін басқару жүйесінің жай-күйіне бағалау жүргізеді.

29. Ақпараттық технологиялар және ақпараттық қауіпсіздік тәуекелдерін басқару бойынша бөлімше «Екінші деңгейдегі банктерге, Қазақстан Республикасының бейрезидент-банктерінің филиалдарына арналған тәуекелдерді басқару және ішкі бақылау жүйесін қалыптастыру қағидаларын бекіту туралы» Қазақстан Республикасының Ұлттық Банкі Басқармасының 2019 жылғы 12 қарашадағы №188 қаулысымен бекітілген Екінші деңгейдегі банктерге арналған тәуекелдерді басқару және ішкі бақылау жүйесін қалыптастыру қағидаларында көзделген функцияларды жүзеге асырады.

30. Ақпараттық жүйелер мен шағын жүйелердің бизнес-иелері:

1) Қызметтер мен өнімдерді құрған, енгізген, модификациялаған, клиенттерге ұсынған кезде ақпараттық қауіпсіздікке қойылатын талаптардың сақталуы үшін жауап береді;

2) Ақпараттық жүйелерге кіруге рұқсат беретін матрицаларды құрады және олардың өзекті болуына қолдау көрсетеді.

31. Банктік құрылымдық бөлімшелерінің басшылары:

1) жұмыскерлердің ақпараттық қауіпсіздікке қойылатын талаптар қамтылатын Банктің ішкі нормативтік құжаттарымен танысуын қамтамасыз етеді;

2) олар басқаратын бөлімшелерде ақпараттық қауіпсіздікті қамтамасыз ету үшін жеке жауап береді;

3) Банктің бөлімшесі мұндай келісімдерді, шарттарды жасасуға бастамашы болған жағдайларда конфиденциалды ақпаратты жария етпеу туралы келісімдер жасасуды және ақпараттық қауіпсіздікті қамтамасыз ету туралы талаптарды қызмет көрсету/жұмыстарды орындау туралы келісімдерге/шарттарға енгізуді қамтамасыз етеді.

32. Банктік құрылымдық бөлімшелерінің жұмыскерлері:

1) Банкте қабылданған ақпараттық қауіпсіздікке қойылатын талаптардың сақталуы үшін жауап береді;

2) Өзінің қызметтік міндеттемелері аясында бірлесіп әрекет ететін үшінші тұлғалардың ақпараттық қауіпсіздікке қойылатын талаптарды орындауын, соның ішінде аталған талаптарды үшінші тұлғалармен жасалатын шарттарға қосу арқылы бақылайды;

3) ақпараттық активтермен жұмыс жүргізген кездегі барлық күдікті жағдайлар мен бұзушылықтар туралы өзінің тікелей басшысына және АҚҚО-ға хабарлайды.

33. Жұмыскер өзіне жүктелген қызметтік міндеттемелерді орындаған кезде, ақпараттық ресурстарды пайдалану тәртібі мен ережесін және ақпараттық қауіпсіздікті қамтамасыз ету бойынша Банкте қабылданған шараларды сақтамауы Қазақстан Республикасының қолданыстағы заңнамасына және Банктің ішкі нормативтік құжаттарына сәйкес жауапкершілікке себепші болады.

9. Банктің еншілес компанияларында ақпараттық қауіпсіздік жүйесін қамтамасыз ету

34. Банктің еншілес компанияларында ақпараттық қауіпсіздік деңгейін қажетті және жеткілікті қамтамасыз ету бөлігінде АҚҚО мен «Банк ЦентрКредит» АҚ-тың еншілес компаниялары арасында бағттауды қамтамасыз ету және бірлесіп әрекет етуді құру мақсатында, АҚҚО ЕК-тың АҚ-ты қамтамасыз ету саласындағы қызметін үйлестіру бойынша келесі функцияларды жүзеге асырады:

1) ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі талаптарды белгілейді;

2) ақпараттық қауіпсіздік бөлігінде ішкі нормативтік құжаттарды келісімге алады;

3) ақпараттық қауіпсіздікті қамтамасыз етудің ұйымдастыру шараларын және бағдарламалық-техникалық құралдарын енгізуді ұсынады және келісімге алады;

4) Ақпараттық қауіпсіздікті қамтамасыз ету саласындағы жыл сайынғы іс-шаралар жоспарларын және еншілес компаниялардың бюджетін келісімге алады;

5) Ақпараттық қауіпсіздікті басқару жүйесін дамыту бөлігінде, сондай-ақ ақпараттық қауіпсіздікті қамтамасыз етуге жауапты Еншілес компаниялардың қызметкерлерін оқыту және кәсіби дамыту мәселелерінде кеңес беріп, қолдау көрсетеді;

6) ақпараттық қауіпсіздікті қамтамасыз ету саласында сыртқы тексерулер мен аудиттерден өту үшін жәрдем береді;

7) ақпараттық қауіпсіздіктің жай-күйіне тексеру жүргізеді, ақпарат сұратады, анықталған ескертулерді жою бойынша іс-шаралар жоспарларын келісімге алады, олардың орындалуын талап етеді;

8) Еншілес компаниялардың бейінді комитеттеріне (болған жағдайда) қатысады.

10. Ақпараттық қауіпсіздікті қамтамасыз ету үшін жауапты басшылар мен жұмыскерлердің құзыреттеріне қойылатын талаптар

35. Ақпараттық қауіпсіздікті қамтамасыз ету үшін жауапты басшылар мен жұмыскерлердің ақпаратты қорғау саласында тиісті құзыреттері мен жұмыс тәжірибесі болу керек.

36. Ақпараттық қауіпсіздікті қамтамасыз ету үшін жауапты басшылар мен жұмыскерлердің біліктілігіне қойылатын егжей-тегжейлі талаптар тиісті біліктілік талаптары мен лауазымдық нұсқаулықтарда көрсетілген.

37. Ақпараттық қауіпсіздікті қамтамасыз ету үшін жауапты басшылар мен жұмыскерлер Қазақстан Республикасы Қаржы нарығын реттеу және дамыту агенттігі Басқармасының 2020 жылғы 21 қыркүйектегі № 89 қаулысының талаптарына сәйкес біліктілігін арттырады.

11. Қорытынды қағидалар

38. Осы Саясатта реттелмеген барлық мәселелер Қазақстан Республикасының заңнамасына, ішкі нормативтік құжаттарға және Банктің уәкілетті органдарының шешімдеріне, сонымен қатар Банк қызметінің қалыптасқан тәжірибесіне сәйкес шешімін табады.

39. Саясат Банктің Директорлар кеңесі бекіткен күннен бастап күшіне енеді және Банктің Директорлар кеңесі оның күші жойылған деп таныған сәттен бастап күшін жояды.

40. Қазақстан Республикасының заңнамасына өзгерістер енгізудің нәтижесінде осы Саясаттың жеке нормалары Қазақстан Республикасының қолданыстағы заңнамасына қайшы болса, онда Саясатқа өзгерістер енгізген сәтке дейін Қазақстан Республикасының қолданыстағы заңнамасын және Саясаттың Қазақстан Республикасының заңнамасына қайшы келмейтін бөлігін басшылыққа алу қажет.

41. Осы Саясат кемінде жылына бір рет қайта қарастырылады.

Одобрено
Протоколом Правления
№ 0129/8 от 29.01.2024 г.

Приложение
к Постановлению Совета директоров
№0219/1 от 19.02.2024 г.

Политика информационной безопасности
АО «Банк ЦентрКредит»

Содержание

1. Общие положения

1. Настоящая Политика информационной безопасности (далее – Политика) является основополагающим документом системы управления информационной безопасности АО «Банк ЦентрКредит» (далее – Банк), определяющим цели, задачи и область действия системы управления информационной безопасностью Банка (далее – СУИБ).

2. СУИБ обеспечивает защиту информационных активов Банка, допускающую минимальный уровень потенциального ущерба для бизнес-процессов Банка.

3. Политика разработана в соответствии с законодательством Республики Казахстан, в том числе нормативными правовыми актами, регулирующими требования к обеспечению

информационной безопасности банков второго уровня, а также требованиями международных стандартов в области информационной безопасности.

4. Требования, предъявляемые к процессам системы управления информационной безопасности Банка, изложенные в настоящей Политике, детально описаны во внутренних нормативных документах Банка, разработанных в соответствии с Главой 9 «Требования к процессам системы управления информационной безопасностью» постановления Правления Национального Банка Республики Казахстан от 27 марта 2018 года № 48 «Об утверждении Требований к обеспечению информационной безопасности банков, филиалов банков-нерезидентов Республики Казахстан и организаций, осуществляющих отдельные виды банковских операций, Правил и сроков предоставления информации об инцидентах информационной безопасности, включая сведения о нарушениях, сбоях в информационных системах».

2. Цели, задачи и основные принципы построения системы управления информационной безопасностью

5. Первый руководитель Банка обеспечивает создание, функционирование и улучшение СУИБ, являющейся частью общей системы управления банка, организации, предназначенной для управления процессом обеспечения информационной безопасности

6. Целью СУИБ является повышение эффективности процессов обеспечения информационной безопасности, обеспечение требуемого уровня конфиденциальности, целостности и доступности критичных информационных активов, и как следствие, снижение рисков информационной безопасности и связанного с ними ущерба.

7. К задачам СУИБ относятся:

1) категорирование информационных активов;

2) организация доступа к информационным активам;

3) обеспечение безопасности информационной инфраструктуры;

4) осуществление мониторинга деятельности по обеспечению информационной безопасности и мероприятий по выявлению и анализу угроз и уязвимостей, противодействию атакам и расследованию инцидентов информационной безопасности;

5) проведение анализа информации об инцидентах информационной безопасности, включая сведения о нарушениях, сбоях в информационных системах;

6) определение порядка управления средствами криптографической защиты информации;

7) обеспечение информационной безопасности при доступе третьих лиц к информационным активам;

8) проведение внутренних проверок состояния информационной безопасности.

8. Построение СУИБ и ее функционирование осуществляются в соответствии со следующими основными принципами:

1) законность – любые действия, предпринимаемые для обеспечения информационной безопасности, осуществляются на основе действующего законодательства, с применением всех дозволенных законодательством методов обнаружения, предупреждения, локализации и пресечения негативных воздействий на информационные активы Банка;

2) ориентированность на бизнес – информационная безопасность рассматривается как процесс поддержки основной деятельности, любые меры по обеспечению информационной безопасности не должны повлечь за собой серьезных препятствий для ведения бизнеса;

3) комплексность – обеспечение безопасности информационных активов в течение всего их жизненного цикла, на всех технологических этапах их использования и во всех режимах функционирования;

4) обоснованность и экономическая целесообразность – используемые возможности и средства защиты должны быть реализованы на соответствующем уровне развития науки и техники, обоснованы с точки зрения заданного уровня безопасности и должны соответствовать предъявляемым требованиям и нормам. Во всех случаях стоимость мер и

технологических решений по обеспечению информационной безопасности не должна превышать стоимость защищаемых информационных активов;

5) адаптивность – определение и применение методов и средств защиты информационных активов в соответствии с их критичностью;

6) необходимое знание и наименьший уровень привилегий – пользователь получает минимальный уровень привилегий и доступ только к тем информационным активам, которые являются необходимыми для выполнения им деятельности в рамках своих полномочий;

7) специализация – реализация мер и эксплуатация технологических решений по обеспечению информационной безопасности должны осуществляться профессионально подготовленными специалистами;

8) информированность и персональная ответственность – руководители всех уровней и исполнители должны быть осведомлены обо всех требованиях информационной безопасности и несут персональную ответственность за выполнение этих требований и соблюдение установленных мер информационной безопасности;

9) взаимодействие и координация – меры информационной безопасности осуществляются на основе взаимосвязи соответствующих структурных подразделений Банка, координации их усилий для достижения поставленных целей, а также установления необходимых связей с внешними организациями, профессиональными ассоциациями и сообществами, государственными органами, юридическими и физическими лицами;

10) подтверждаемость – свидетельства, подтверждающие исполнение требований по информационной безопасности и эффективности СУИБ должны создаваться и храниться с возможностью оперативного доступа и восстановления.

3. Область действия системы управления информационной безопасностью

9. Областью действия СУИБ являются основные бизнес-процессы Банка, непосредственно ориентированные на предоставление услуг клиентам, представляющие ценность для клиентов и обеспечивающие получение прибыли, определенные процедурой классификации бизнес-процессов, а также процессы, обеспечивающие деятельность Удостоверяющего Центра Банка.

10. Объектами защиты являются критичные информационные активы, необходимые для функционирования основных бизнес-процессов, а также информационные активы, обеспечивающие функционирование Удостоверяющего Центра, к которым могут быть отнесены:

1) индивидуальные устройства обработки информации;
2) носители информации;
3) периферийное компьютерное оборудование;
4) серверы;
5) базы данных;
6) сетевое оборудование;
7) аппаратура телефонии;
8) физические каналы связи;
9) виртуальные каналы связи;
10) системы виртуализации;
11) операционные системы;
12) программное обеспечение аппаратных средств;
13) прикладное программное обеспечение;
14) программное обеспечение телефонии;
15) средства криптографической защиты информации.

4. Требования к доступу к создаваемой, хранимой и обрабатываемой информации в информационных системах Банка и мониторинг информации и доступа к ней

11. Доступ к информации и информационным системам Банка предоставляется работникам в объеме, необходимом для исполнения их функциональных обязанностей.

12. Предоставление доступа к критичным информационным системам Банка производится путем формирования и внедрения ролей для обеспечения соответствия прав доступа пользователей информационных систем их функциональным обязанностям.

13. Доступ лицам, не являющимся работниками Банка (далее – третьи лица), к информационным активам Банка предоставляется на период и в объеме, необходимых для проведения работ на основании соответствующего соглашения/договора, включающего условия о соблюдении требований к информационной безопасности, за исключением случаев, предусмотренных законодательством Республики Казахстан. В соглашениях/договорах, заключаемых с третьими лицами, содержатся положения о конфиденциальности, условия о возмещении ущерба, возникшего вследствие нарушения информационной безопасности, а также сбоев в работе информационных систем и нарушения их безопасности, вызванных действием или бездействием третьих лиц.

5. Требования к осуществлению мониторинга деятельности по обеспечению информационной безопасности и мероприятий по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов информационной безопасности

14. Банк обеспечивает создание структурного подразделения по реагированию на инциденты информационной безопасности – службу реагирования на инциденты информационной безопасности.

15. Банк обеспечивает надлежащий мониторинг деятельности по обеспечению информационной безопасности и мероприятий по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов информационной безопасности.

6. Требования к осуществлению сбора, консолидации и хранения информации об инцидентах информационной безопасности

16. Банк обеспечивает наличие документов, сведений и фактов, подтверждающих реализацию порядка реагирования на инциденты информационной безопасности, а также учет, хранение, консолидацию, систематизацию, целостность и сохранность информации об инцидентах информационной безопасности, включая сведения о нарушениях, сбоях в информационных системах, о результатах внутреннего расследования инцидентов информационной безопасности и материалов расследования на бумажном носителе и (или) в электронном виде.

7. Требования к проведению анализа информации об инцидентах информационной безопасности

17. Банк обеспечивает:

1) проведение анализа выявленных инцидентов информационной безопасности и нанесенного ими ущерба для рассмотрения коллегиальным органом Банка, с целью оценки рисков информационной безопасности, корректировки методов и средств обеспечения информационной безопасности, изменения бизнес-процессов Банка;

2) оценку эффективности с целью корректировки процесса реагирования на инциденты информационной безопасности с использованием метрик процесса реагирования на инциденты информационной безопасности;

3) пересмотр метрик процесса реагирования на инциденты информационной безопасности с учетом результата оценки эффективности процесса реагирования на инциденты информационной безопасности;

4) пересмотр перечня событий информационной безопасности, подлежащих мониторингу, источников событий, периодичности, порядка и методов мониторинга событий информационной безопасности.

8. Ответственность работников Банка за обеспечение информационной безопасности при исполнении возложенных на них функциональных обязанностей

18. Участниками СУИБ Банка являются:

1) Совет Директоров;

2) Правление;

3) коллегиальный орган, уполномоченный принимать решения по задачам обеспечения информационной безопасности (далее – УКО);

4) подразделение по информационной безопасности;

5) подразделение по информационным технологиям;

6) подразделение по безопасности;

7) подразделение по работе с персоналом;

8) юридическое подразделение;

9) подразделение по комплаенс-контролю;

10) подразделение внутреннего аудита;

11) подразделение по управлению рисками информационных технологий и информационной безопасности;

12) бизнес-владельцы информационных систем и подсистем;

13) руководители структурных подразделений;

14) работники структурных подразделений.

19. Совет директоров утверждает политику информационной безопасности и перечень защищаемой информации, включающий в том числе информацию о сведениях, составляющих служебную, коммерческую или иную охраняемую законом тайну, и порядок работы с защищаемой информацией. Совет директоров при формировании бюджета учитывает потребности в ресурсах для обеспечения информационной безопасности Банка.

20. Правление утверждает внутренние нормативные документы, регламентирующие процесс управления информационной безопасностью, программу обучения и план проведения тестирования работников на знание требований внутренних нормативных документов по информационной безопасности, порядок и периодичность пересмотра которых определяется внутренними документами Банка.

21. Правление обеспечивает наличие УКО по принятию решений по вопросам обеспечения информационной безопасности, который действует в рамках полномочий, предоставленных Правлением.

22. Подразделение по информационной безопасности в целях обеспечения конфиденциальности, целостности и доступности информации Банка осуществляет следующие функции:

1) организует систему управления информационной безопасностью, осуществляет координацию и контроль деятельности подразделений Банка по обеспечению информационной безопасности и мероприятий по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов информационной безопасности;

2) разрабатывает политику информационной безопасности Банка;

3) обеспечивает методологическую поддержку процесса обеспечения информационной безопасности Банка;

4) осуществляет выбор, внедрение и применение методов, средств и механизмов управления, обеспечения и контроля информационной безопасности Банка, в рамках своих полномочий;

5) осуществляет сбор, консолидацию, хранение и обработку информации об инцидентах информационной безопасности;

6) осуществляет анализ информации об инцидентах информационной безопасности;

7) подготавливает предложения для принятия Комитетом по информационной безопасности решения по вопросам информационной безопасности;

8) обеспечивает внедрение, надлежащее функционирование программно-технических средств, автоматизирующих процесс обеспечения информационной безопасности Банка, а

также предоставление доступа к ним;

9) определяет требования информационной безопасности по использованию привилегированных учетных записей;

10) обеспечивает проведение мероприятий по повышению осведомленности работников Банка в области информационной безопасности;

11) осуществляет мониторинг состояния системы управления информационной безопасностью Банка;

12) осуществляет информирование руководства Банка о состоянии системы управления информационной безопасностью Банка;

13) проводит оценку рисков информационной безопасности;

14) разрабатывает меры по обработке рисков информационной безопасности и предоставляет отчетность по их реализации в подразделение по управлению рисками информационных технологий и информационной безопасности;

15) подготавливает и предоставляет отчетность о реализации существенных рисков информационной безопасности в подразделение по управлению рисками информационных технологий и информационной безопасности, а также об устранении их последствий;

16) разрабатывает план мероприятий по реализации стратегии Банка в части обеспечения информационной безопасности, который раскрывает, но, не ограничиваясь, следующее:

- определение потребностей в ресурсах, в том числе определение бюджета, связанного с реализацией мер, направленных на управление рисками информационной безопасности;
- описание требуемых мероприятий в области информационной безопасности с указанием сроков и ответственных исполнителей за их реализацию.

23. Подразделение по информационным технологиям осуществляет следующие функции:

1) разрабатывает и поддерживает актуальность схемы информационной инфраструктуры Банка;

2) обеспечивает предоставление доступа пользователям к информационным активам Банка, за исключением специализированных информационных активов, доступ к которым предоставляется ИТ-менеджерами информационных систем, не относящимися к Подразделению по информационным технологиям;

3) обеспечивает формирование типовых настроек и конфигурирование системного и прикладного программного обеспечения Банка с учетом требований информационной безопасности;

4) обеспечивает исполнение установленных требований по непрерывности функционирования информационной инфраструктуры, конфиденциальности, целостности и доступности данных информационных систем Банка (включая резервирование и (или) архивирование и резервное копирование информации) в соответствии с внутренними документами Банка;

5) обеспечивает соблюдение требований информационной безопасности при выборе, внедрении, разработке и тестировании информационных систем.

24. Подразделение по безопасности осуществляет следующие функции:

1) реализует меры физической и технической безопасности в Банке, в том числе организует пропускной и внутриобъектовый режим;

2) проводит профилактические мероприятия, направленные на минимизацию рисков возникновения угроз информационной безопасности при приеме на работу и увольнении работников Банка.

25. Подразделение по управлению персоналом осуществляет следующие функции:

1) обеспечивает подписание работниками Банка, а также лицами, привлеченными к работе по договору об оказании услуг, стажерами, практикантами обязательств о неразглашении конфиденциальной информации;

2) участвует в организации процесса повышения осведомленности работников Банка в области информационной безопасности;

3) уведомляет уполномоченный орган о назначении и увольнении работников подразделения по информационной безопасности.

26. Юридическое подразделение осуществляет правовую экспертизу внутренних нормативных документов Банка по вопросам обеспечения информационной безопасности.

27. Подразделение по комплаенс-контролю совместно с Юридическим подразделением определяет виды информации, подлежащие включению в перечень защищаемой информации, предусмотренной пунктом 19 настоящей Политики.

28. Подразделение внутреннего аудита проводит оценку состояния системы управления информационной безопасностью Банка в соответствии с внутренними нормативными документами Банка, регламентирующими организацию системы внутреннего аудита Банка.

29. Подразделение по управлению рисками информационных технологий и информационной безопасности осуществляет функции, предусмотренные Правилами формирования системы управления рисками и внутреннего контроля для банков второго уровня, утвержденными Постановление Правления Национального Банка Республики Казахстан от 12 ноября 2019 года №188 «Об утверждении Правил формирования системы управления рисками и внутреннего контроля для банков второго уровня, филиалов банков-нерезидентов Республики Казахстан».

30. Бизнес-владельцы информационных систем или подсистем:

1) отвечают за соблюдение требований к информационной безопасности при создании, внедрении, модификации, эксплуатации информационных систем и предоставлении продуктов и услуг клиентам и подразделениям Банка, а также при интеграции информационных систем с внешними информационными системами, включая информационные системы государственных органов;

2) формируют и поддерживают актуальность матриц доступа к информационным системам.

31. Руководители структурных подразделений Банка:

1) обеспечивают ознакомление работников с внутренними нормативными документами Банка, содержащими требования к информационной безопасности;

2) несут персональную ответственность за обеспечение информационной безопасности в возглавляемых ими подразделениях;

3) обеспечивают заключение соглашений о неразглашении конфиденциальной информации и включение условий об обеспечении информационной безопасности в соглашения, договоры на оказание услуг/выполнение работ в случаях, когда подразделение Банка выступает инициатором заключения таких соглашений, договоров.

32. Работники структурных подразделений Банка:

1) отвечают за соблюдение требований к информационной безопасности, принятых в Банке;

2) контролируют исполнение требований к информационной безопасности третьими лицами, с которыми они взаимодействуют в рамках своих функциональных обязанностей, в том числе путем включения указанных требований в договоры с третьими лицами;

3) извещают своего непосредственного руководителя и подразделение по информационной безопасности обо всех подозрительных ситуациях и нарушениях при работе с информационными активами.

33. Несоблюдение порядка и правил использования информационных ресурсов и принятых в Банке мер обеспечения информационной безопасности при исполнении работниками возложенных функциональных обязанностей, влечет за собой ответственность в соответствии с действующим законодательством Республики Казахстан и внутренними нормативными документами Банка.

9. Обеспечение информационной безопасности в Дочерних компаниях Банка

34. В целях обеспечения кураторства и построения взаимодействия между подразделением по информационной безопасности и Дочерними компаниями АО «Банк ЦентрКредит» (далее – ДК) в части обеспечения необходимого и достаточного уровня

информационной безопасности в ДК Банка, подразделение по информационной безопасности осуществляет следующие функции координации деятельности ДК:

1) определяет требования по обеспечению информационной безопасности;

2) согласовывает внутренние нормативные документы в части информационной безопасности;

3) рекомендует и согласовывает внедрение организационных мер и программно-технических средств обеспечения информационной безопасности;

4) согласовывает ежегодные планы мероприятий и бюджет ДК в области обеспечения информационной безопасности;

5) оказывает консультационную поддержку в части развития системы управления информационной безопасностью, а также в вопросах обучения и профессионального развития работников ДК, ответственных за обеспечение информационной безопасности;

6) оказывает содействие в прохождении внешних проверок и аудитов в области обеспечения информационной безопасности;

7) проводит проверки состояния информационной безопасности, запрашивает информацию, согласовывает планы мероприятий по устранению выявленных замечаний, требует их исполнения;

8) участвует в профильных комитетах ДК (при наличии).

10. Требования к компетенциям руководителей и работников, ответственных за обеспечение информационной безопасности

35. Руководители и работники, ответственные за обеспечение информационной безопасности, обладают соответствующими компетенциями и опытом работы в сфере защиты информации.

36. Детальные требования к квалификации руководителей и работников, ответственных за обеспечение информационной безопасности, отражены в соответствующих квалификационных требованиях и должностных инструкциях.

37. Руководители и работники, ответственные за обеспечение информационной безопасности повышают квалификацию в соответствии с требованиями Постановления Правления Агентства Республики Казахстан по регулированию и развитию финансового рынка от 21 сентября 2020 года № 89.

11. Заключительные положения

38. Все вопросы, не урегулированные настоящей Политикой, решаются в соответствии с законодательством Республики Казахстан, внутренними нормативными документами и решениями уполномоченных органов Банка, а также сложившейся практикой деятельности Банка.

39. Политика вступает в силу с даты утверждения Советом Директоров Банка и прекращает свое действие с момента признания ее утратившей силу Советом Директоров Банка.

40. Если в результате изменения законодательства Республики Казахстан отдельные нормы настоящей Политики вступают в противоречие с действующим законодательством Республики Казахстан, то до момента внесения изменений в Политику, необходимо руководствоваться действующим законодательством Республики Казахстан и Политикой в части, не противоречащей законодательству Республики Казахстан.

41. Пересмотр настоящей Политики осуществляется не реже одного раза в год.