ҚАЗАҚСТАН ХАЛЫҚ БАНКІНІҢ ЕНШІЛЕС ҰЙЫМЫ
HALYK KAZTELEPORT
ДОЧЕРНЯЯ ОРГАНИЗАЦИЯ НАРОДНОГО БАНКА КАЗАХСТАНА

БЕКІТІЛГЕН
«Казтелепорт» АҚ Директорлар кеңесінің шешімімен
20.06.2025 жылғы № 28 хаттама
08.09.2025 ж. өзгерістермен (№37 хаттама)

«Казтелепорт» АҚ
Ақпараттық қауіпсіздік саясаты

Әзірлеуші:	Ақпараттық қауіпсіздік департаменті
Бизнес- иесі:	Ақпараттық қауіпсіздік департаменті

Алматы қ. 2025 ж.

Мазмұны

1 тарау. Жалпы ережелер

1. «Казтелепорт» АҚ Ақпараттық қауіпсіздік саясаты (бұдан әрі – АҚ саясаты) «Казтелепорт» АҚ Ақпараттық қауіпсіздікті ұйымдастыруға қойылатын талаптарды айқындайды және өз қызметінде «Казтелепорт» АҚ (бұдан әрі – Компания) басшылыққа алатын ақпараттық қауіпсіздік саласындағы мақсаттарды, міндеттер мен қағидаттарды белгілейді.
2. Ақпараттық қауіпсіздік немесе ақпараттық активтерді қорғау деп ақпараттық активтерді кездейсоқ немесе қасақана өзгертуден, ашудан немесе жоюдан қажетті шараларды қабылдау және орындау, сондай-ақ олардың құпиялылығын, тұтастығы мен қолжетімділігін қамтамасыз ету түсініледі.
3. Компанияның табысты қызметі клиенттердің оларға көрсетілетін қызметтер олардың ақпараттық қауіпсіздігін бұзбайтындығына тікелей байланысты, сондықтан Компания мен оның клиенттерінің ақпараттық қауіпсіздігін қамтамасыз ету компанияның өмір сүру мақсаттары үшін негізгі қызмет болып табылады.
4. АҚ саясаты талаптар мен ұсыныстарды ескере отырып әзірленген:
   1) СТ РК ISO/IEC 27001-2023 «Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар»;
   2) СТ РК ISO/IEC 27002-2023 – «Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару құралдары»;
   3) СТ РК ISO/IEC 27005-2022 – «Ақпараттық технологиялар. Қауіпсіздікті қамтамасыз ету әдістері. Ақпараттық қауіпсіздік тәуекелдерін басқару»;
   4) Халық тобында ақпараттық қауіпсіздікті қамтамасыз ету қағидаларын қамтиды.

2 тарау. Терминдер мен қысқартулар

5. АҚ саясатында келесі терминдер мен қысқартулар қолданылады:
   1) актив бұл компания үшін құндылығы бар нәрсе;
   2) актив иесі - активтерді өндіруге, әзірлеуге, қызмет көрсетуге, пайдалануға және қауіпсіздікке жауапты ретінде бекітілген құрылымдық бөлімшенің басшысы / уәкілетті тұлға. «Иесі»- термині адамның активтерге меншік құқығы бар дегенді білдірмейді;
   3) ақпараттық активтің бизнес-иесі - ақпараттық актив өмірлік циклін қамтамасыз ету үшін пайдаланылатын бизнес-процестің иесі;
   4) ІНҚ - ішкі нормативтік құжат;
   5) қолжетімділік - уәкілетті Субъектінің сұрау салуы бойынша беру және пайдалану мүмкіндігін айқындайтын қасиет;
   6) қорғалатын қолжетімділік - ақпаратты алу, көшіру, тарату, бұрмалау, жою немесе бұғаттау жөніндегі заңсыз әрекеттерді қоса алғанда, компанияның ақпараттық активтеріне заңсыз қол жеткізуді болғызбауға бағытталған құқықтық, ұйымдастырушылық және техникалық шаралар кешені;
   7) АА – ақпараттық актив - компания үшін құндылығы бар ақпарат пен ақпараттық инфрақұрылымның жиынтығы;
   8) АҚ - Ақпараттық қауіпсіздік;
   9) ақпарат - оларды ұсыну нысанына қарамастан, біреу немесе бір нәрсе туралы мәліметтер;

10) ақпараттық инфрақұрылым-ақпараттық жүйелердің, байланыс жүйелерінің, басқару орталықтарының, аппараттық-бағдарламалық құралдар мен ақпаратты жинауды, сақтауды, өңдеуді және беруді қамтамасыз ету технологияларының жиынтығы;

11) бақыланатын қол жеткізу-басқарылатын қол жеткізудің жұмыс істеу процесін және нақты жай-күйін бақылау және тексеру жүйесі;

12) құпиялылық-ақпараттың рұқсат етілмеген тұлғаға, ұйымға немесе процеске қолжетімді немесе ашылмайтынын айқындайтын қасиет;

13) ең аз қажетті қол жеткізу құқықтары-белгілі бір (қойылған) міндеттерді орындау үшін жеткілікті шектеулі қол жеткізу құқықтары;

14) тәуекелді өңдеу-тәуекелді өзгерту жөніндегі шараларды таңдау және іске асыру процесі;

15) тәуекелдерді бағалау-қауіптерді, олардың салдарын, ақпарат пен оны өңдеу құралдарының осалдығын, сондай-ақ олардың туындау ықтималдығын бағалау;

16) тәуекел-белгісіздіктің мақсаттарға әсері;

17) ақпараттық қауіпсіздік менеджменті жүйесі (АҚМЖ) – ақпараттық қауіпсіздікті құру, енгізу, қолдану, мониторинг, талдау, қолдау және жақсарту үшін тәуекелдер менеджменті тәсіліне негізделген жалпы менеджмент жүйесінің бөлігі;

18) АТҚ - Ақпараттық технологиялар қызметі-міндеттеріне компанияның ақпараттық инфрақұрылымын әзірлеу, енгізу, сүйемелдеу және қолдау, қол жеткізу құқықтарын беру, өзгерту және жою, компанияның ақпараттық инфрақұрылымының, оның ішінде ақпараттық қауіпсіздікті қамтамасыз ету талаптарына сәйкестігін қамтамасыз ететін параметрлерін жүзеге асыру кіретін компанияның бөлімшелері/қызметкерлері;

19) тұтастық-активтердің дұрыстығы мен толықтығына кепілдік беретін қасиет;

20) ДӨО – деректер өндеу орталығы.

3 тарау. АҚ саясатының мақсаттары мен қолданылу саласы

6. АҚ саясаты мақсатпен әзірленген:

1) Компания мен оның клиенттерінің ақпаратын нақты және ықтимал қауіптерден қорғау;

2) қатерлерге ұшыраған кезде салдарларды барынша азайту және оқшаулау;

3) компанияның ақпаратын, ақпараттық активтерін және ақпараттық инфрақұрылымын іске асырылуы залалға әкеп соғуы мүмкін ақпараттық қауіпсіздіктің сыртқы және ішкі қатерлерінен қорғауды және осы қатерлер іске асырылған жағдайда залалды барынша азайтуды қамтамасыз ететін СМЖ құру және өзекті жай-күйде ұстау;

4) компанияның АҚМЖ ҚР СТ ISO / IEC 27001-2023 стандартының талаптарына сәйкестігін қамтамасыз ету және тиісті сәйкестік сертификатын алу / растау.

7. АҚ саясаты компанияның бизнес мақсаттарын, Компанияның қызметіне қатысы бар және оның АҚМЖ-тен күтілетін нәтижелерге қол жеткізу қабілетіне, мүдделі тараптардың талаптарына әсер ететін сыртқы және ішкі факторларды ескере отырып әзірленген.

8. Компанияда АҚМЖ қолдану саласы қызмет көрсету кезіндегі ақпараттық қауіпсіздік менеджменті болып табылады:

1) телекоммуникациялық;

2) деректерді өңдеу орталықтарының қызметтері;

3) құрылымдық кабельдік желілерді, Бейнебақылау жүйелерін, күзет-өрт дабылы жүйелерін, қолжетімділікті бақылау жүйелерін монтаждау және техникалық қызмет көрсету жөніндегі қызметтер;

4) Ақпараттық қауіпсіздік, оның ішінде Деректер орталығының қызметтері және периметрді сыртқы желілік қауіптерден қорғау;

5) «1С Кәсіпорын» бағдарламалық қамтамасыз етуді сүйемелдеу жөніндегі қызметтер, оның ішінде «бұлтты 1С» қызметтері;

6) аутсорсингтік;

7) гермозона жүйелеріне техникалық қызмет көрсету қызметтері;

8) тауарлар мен көрсетілетін қызметтерді өткізу;

9) электр зарядтау құрылғыларына техникалық қызмет көрсету қызметтері.

9. АҚМЖ - қолданудың шекаралары Алматы, Ақтау және Астана қалаларында орналасқан компанияның барлық құрылымдық бөлімшелері, ДӨО, серверлік компаниялар болып табылады.

10. АҚ саясаты қызметтік функциялары АҚМЖ қолдану саласы мен шекарасына кіретін компанияның барлық қызметкерлері үшін міндетті болып табылады.

11. АҚ саясаты барлық мүдделі тараптарға шектеусіз ұсынылуы мүмкін жалпыға қол жетімді құжат болып табылады.

4 тарау. АҚ саясатының мақсаттарына қол жеткізу жөніндегі міндеттер

12. АҚ саясатының мақсаттарына мынадай міндеттерді қамтамасыз ету және тұрақты қолдау арқылы қол жеткізіледі:

1) АҚМЖ -тің жұмысқа қабілеттілігін қамтамасыз ететін ұйымдық құрылымды құру;

2) компания басшылығы тарапынан АҚ саясатын нақты басқаруды және қолдауды қамтамасыз ету үшін ДӨО әзірлеу;

3) компания активтеріне басқарылатын, қорғалатын және бақыланатын қолжетімділікті қамтамасыз ету;

4) Ақпараттық қауіпсіздік тәуекелдеріне тұрақты бағалау мен талдау жүргізу және ҚР СТ ISO/IEC 27005-2022 сәйкес оларды төмендету жөніндегі шараларды әзірлеу;

5) Бизнестің үздіксіздігіне әсер етуі мүмкін оқиғалардың алдын алу және ескерту шараларын әзірлеу;

6) АҚ инциденттерін басқару жүйесін әзірлеу және енгізу.

5 тарау. АҚ саясатының принциптері

13. Алға қойылған мақсаттарға қол жеткізу үшін және міндеттерді орындау кезінде Компания келесі қағидаттарды басшылыққа алуға міндеттенеді:

1) **заңнамалық және өзіне қабылдаған өзге де міндеттемелерге сәйкестігі.** Ақпараттық қауіпсіздікті қамтамасыз ету шараларын іске асыру Қазақстан Республикасының қолданыстағы заңнамасына, акционердің – «Қазақстан

Халық Банкі» АҚ талаптарына және шарттық міндеттемелерге қатаң сәйкестікте жүзеге асырылады;

2) **Компания басшылығының ақпараттық қауіпсіздікті қамтамасыз ету процесін басқаруы.** Ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі қызметті компанияның Басқарма Төрағасы бастамашылық етеді және бақылайды. Ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі қызметті үйлестіруді компанияның Басқарма Төрағасының бұйрығымен тағайындалатын АҚМЖ жауапты адам жүзеге асырады;

3) **АҚМЖ үздіксіз жақсарту.** АҚМЖ үздіксіз жақсарту, ҚР СТ ISO/IEC 27001-2023 талаптарына сәйкес барлық қажетті процестерді және олардың өзара іс-қимылын қоса алғанда, тұрақты жақсарту. Жақсарту мүмкіндіктері туралы ақпаратты Компания алады:

   a) АҚМЖ мониторингінің нәтижелері;

   b) аудит нәтижелері;

   c) басшылық тарапынан АҚМЖ талдауы.

   Алынған ақпарат негізінде АҚ мақсаттары өзектендіріледі және оларды іске асыру бойынша қажетті іс шаралар әзірленеді;

4) **Тәуекелдерді басқару.** Ақпараттық қауіпсіздік тәуекелдерін басқару келесі бағыттар бойынша тұрақты қызметті қолдауда көрінеді:

   a) қорғалатын активтерді сәйкестендіру және осы активтердің "иелерін" анықтау;

   b) сәйкестендірілген активтерге қатысты ақпараттық қауіпсіздік қатерлерін уақтылы анықтау және болжау;

   c) ақпараттық қауіпсіздік тәуекелдерін бағалау және өңдеу;

   d) ақпараттық қауіпсіздікті қамтамасыз етудің, оның ішінде ішкі және сыртқы аудиторларды тарта отырып, қолданылатын әдістері мен құралдарының тиімділігін бағалау;

5) **Іс-әрекеттердің келісімділігі.** Ақпараттық және физикалық қауіпсіздікті қамтамасыз ету жөніндегі іс-шаралар компания бөлімшелерінің нақты өзара іс-қимылы негізінде жүзеге асырылады және мақсаттар, міндеттер, қағидаттар, әдістер мен құралдар бойынша өзара келісіледі;

6) **Экономикалық орындылығы.** Ақпараттық қауіпсіздікті қамтамасыз ету шараларын таңдау оларды іске асыруға жұмсалатын шығындарды, ақпараттық қауіпсіздікке төнетін қатерлердің туындау ықтималдығын және оларды іске асырудан болатын ықтимал ысыраптардың көлемін ескере отырып жүзеге асырылады;

7) **Персоналды басқару.** Қызметкерлерді (қызметкерлерді) мұқият іріктеу, компания қызметі үшін қолайлы жағдай жасайтын және ақпараттық қауіпсіздік тәуекелдерін төмендететін корпоративтік этиканы әзірлеу және қолдау;

8) **Ақпараттық қауіпсіздік талаптарының құжатталуы.** Ақпараттық қауіпсіздіктің барлық талаптары Компанияның уәкілетті органдары / тұлғалары бекітетін ішкі нормативтік құжаттарда тіркеледі;

9) **Ақпараттық қауіпсіздікті қамтамасыз ету мәселелеріндегі хабардарлық.** Ақпараттық қауіпсіздік саласындағы құжатталған талаптар компанияның барлық қызметкерлері мен контрагенттердің назарына оларға қатысты бөлігінде жеткізіледі. Компания мерзімді негізде қызметкерлерді ақпараттық

қауіпсіздікті қамтамасыз ету мәселелері бойынша ақпараттандыруды және оқытуды жүзеге асырады;

10) **Конфигурацияның өзгеруін басқару.** Ақпараттық қауіпсіздіктің жүйелік бұзылулары мен инциденттерін болдырмау мақсатында ақпаратты өңдеу құралдары мен жүйелеріндегі конфигурацияларды өзгерту жөніндегі барлық іс әрекеттер тиісті түрде бақыланады және құжатталады;

11) **Ақпараттық қауіпсіздік инциденттеріне ден қою.** Ақпараттық қауіпсіздіктің жарамды, қабылданатын және ықтимал бұзылуларын анықтау, тіркеу және жедел ден қою;

12) **Дербес жауапкершілік.** Ақпараттық қауіпсіздікті сақтау жөніндегі талаптарды компанияның ІНҚ белгілейді. Ақпараттық қауіпсіздік талаптарын сақтау жөніндегі міндеттер еңбек шарттарына және қызметкерлердің лауазымдық нұсқаулықтарына енгізіледі. Ақпараттық қауіпсіздік талаптарын қамтамасыз ету және сақтау жөніндегі міндеттерді орындамағаны немесе тиісінше орындамағаны үшін қызметкерлерге Қазақстан Республикасының Еңбек кодексінде және компанияның ІНҚ көзделген тәртіппен тәртіптік жазалар қолданылуы мүмкін;

13) **Қол жеткізудің ең аз қажетті құқықтарын беру.** Компания қызметкерлері мен контрагенттерге Еңбек міндеттері мен шарттық міндеттемелерді сапалы және уақтылы орындау үшін ең аз қажетті қол жеткізу құқықтары беріледі;

14) **Ақпараттық қауіпсіздік аудиттерін жүргізудің жүйелілігі.** Ақпараттық қауіпсіздікке қатысты Компанияның саясаттары мен басқа да ішкі нормативтік құжаттарының тиімділігін тексеру үшін жылына кемінде бір рет кезеңділікпен аудит жүргізу орындалады. Аудит қорытындылары бойынша компанияның ақпараттық қауіпсіздігіне қатысты мақсаттар мен міндеттер өзектендірілуі мүмкін;

15) **Жобалау қызметіндегі ақпараттық қауіпсіздік талаптарын есепке алу.** Ақпараттық қауіпсіздік талаптары жобалау қызметінде ескеріледі. Ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі талаптарды әзірлеу және құжаттау ақпаратты өңдеуге, сақтауға және беруге байланысты жобаларды іске асырудың бастапқы кезеңдерінде жүзеге асырылады;

16) **Тәртіптік практика рәсімдерін қолдану.** АҚМЖ ішкі құжаттарының талаптарын байқаусызда және қасақана орындамағаны үшін персоналға Қазақстан Республикасының заңнамасына сәйкес тәртіптік жауапкершілік рәсімдері қолданылады. Бұл қағида міндетті түрде компанияның барлық қызметкерлеріне жеткізіледі.

6 тарау. АҚ саясатының қағидаттарын іске асыру

14. АҚ саясатының принциптері арқылы жүзеге асырылады:

1) «Казтелепорт» АҚ Басқармасының шешімімен бекітілетін және қолданысқа енгізілетін басқару құралдарын қолдану;

2) Компанияның ақ саясатының құрылымына кіретін тақырыптық саясаттарды, оның ішінде, бірақ олармен шектелмей:

a) кіруді басқару саясаты;

b) желілік қауіпсіздік саясаты;

c) ақпаратты беру саясаты;

d) мобильді соңғы құрылғыларға және қашықтан жұмыс істеуге қатысты саясат;

e) физикалық қауіпсіздік саясаты;

f) криптографияны қолдану саясаты;

g) таза үстел және таза экран саясаты;

h) жеткізушілермен қарым-қатынасқа арналған ақпараттық қауіпсіздік саясаты;

i) Сақтық көшірме саясаты;

j) өзгерістерді басқару саясаты.

15. Қол жеткізуді басқару саясаты.

Саясаттың мақсаты-қызметкерлердің қызметтік міндеттерін орындау үшін қажетті ақпараттық активтерге ғана қол жеткізуін қамтамасыз ету.

16. Желілік қауіпсіздік саясаты.

Саясаттың мақсаты-Желілік қызметтерді персонал мен бөгде адамдардың рұқсатсыз кіруінен қорғау.

17. Ақпаратты беру саясаты.

Саясаттың мақсаты-компания ішінде және кез келген сыртқы мүдделі Тарапқа берілетін ақпараттың қауіпсіздігін қамтамасыз ету.

18. Мобильді соңғы құрылғыларға және қашықтан жұмыс істеуге қатысты саясат.

Саясаттың мақсаты-ақпаратты мобильді құрылғыларды пайдалану кезінде және персоналдың қашықтан жұмыс істеуі кезінде туындайтын тәуекелдерден қорғау.

19. Физикалық қауіпсіздік саясаты;

Саясаттың мақсаты-рұқсатсыз физикалық қол жетімділіктің, ақпараттың және басқа да байланысты активтердің бүлінуі мен қозғалысының алдын алу.

20. Криптографияны қолдану саясаты.

Саясаттың мақсаты-криптографияны бизнестің және ақпараттық қауіпсіздіктің талаптарына сәйкес ақпараттың құпиялылығын, түпнұсқалығын немесе тұтастығын қорғау үшін, сондай-ақ криптографияға қатысты заңды, заңнамалық, нормативтік және шарттық талаптарды ескере отырып, тиісті және тиімді пайдалануды қамтамасыз ету.

21. Таза үстел және таза экран саясаты.

Саясаттың мақсаты-жұмыс және жұмыс уақытынан тыс уақытта кестелерде, экрандарда және басқа да қол жетімді жерлерде ақпаратқа рұқсатсыз қол жеткізу, жоғалту және бүліну қаупін болдырмау.

22. Жеткізушілермен қарым-қатынасқа арналған ақпараттық қауіпсіздік саясаты.

Саясаттың мақсаты-жеткізушілермен қарым-қатынаста ақпараттық қауіпсіздіктің келісілген деңгейін сақтау.

23. Сақтық көшірме саясаты.

Саясаттың мақсаты-деректерді немесе жүйелерді жоғалтқаннан кейін қалпына келтіру мүмкіндігін қамтамасыз ету

24. Өзгерістерді басқару саясаты.

Саясаттың мақсаты-жүйенің бүкіл өмірлік циклі кезінде ақпаратты өңдеу құралдары мен ақпараттық жүйелердегі ақпараттың құпиялылығын, тұтастығын және қолжетімділігін қамтамасыз етуге кепілдік беретін өзгерістерді басқару процесін ұйымдастыру, жобалаудың алғашқы кезеңдерінен бастап барлық кейінгі техникалық қызмет көрсету әрекеттеріне дейін.

25. Тақырыптық саясатты іске асыру үшін компанияның тиісті ІНҚ әзірленеді және қолданысқа енгізіледі.

7 тарау. Ақпараттық қауіпсіздікке төнетін қатерлер

26. АҚ қатерлері деп ақпараттық қауіпсіздік инцидентінің пайда болуының алғышарттарын жасайтын жағдайлар мен факторлардың жиынтығы түсініледі.

27. АҚ қауіптері мыналарға бөлінеді:

1) кездейсоқ – Дүлей зілзалалар (қауіптердің табиғи көздері – жер сілкінісі, өрт, жауын-шашын, су тасқыны және т. б.), компания қызметкерлері мен компанияның ақпараттық активтерімен өзара іс-қимыл жасайтын үшінші тұлғалар тарапынан байқаусызда қате әрекеттер, аппараттық және бағдарламалық құралдардың қателіктері және т. б.;

2) қасақана, яғни деректерді қасақана бұрмалау немесе жою, деректерді заңсыз пайдалану, компьютерлік қылмыстар және т. б.

28. АҚ қауіптерінің қатарына мыналар жатады (бірақ олармен шектелмейді):

1) компанияның коммерциялық құпиясын және заңмен қорғалатын өзге де ақпаратты құрайтын ақпараттың жоғалуы;

2) қорғалатын ақпаратты бұрмалау (рұқсатсыз өзгерту, қолдан жасау);

3) ағып кету-бөгде адамдардың қорғалатын ақпаратпен рұқсатсыз танысуы (рұқсатсыз кіру, көшіру, ұрлау, беру және т. б.);

4) ақпараттық ресурстарды рұқсатсыз пайдалану (теріс пайдалану, алаяқтық және т. б.);

5) оны бұғаттау, жабдықтың немесе бағдарламалардың істен шығуы мен істен шығуы, жұмыс станцияларының операциялық жүйелерінің, серверлердің, белсенді желілік жабдықтардың, деректер базасын басқару жүйелерінің, таратылған есептеу желілерінің, вирустардың, дүлей зілзалалардың және өзге де форс-мажорлық мән-жайлардың және зиянды әрекеттердің жұмыс істеуін ұйымдастырмау нәтижесінде ақпараттың қолжетімсіздігі.

29. Аталған қауіптерді іске асыру нәтижесінде компанияның АҚ-ның жай-күйіне және оның қалыпты жұмыс істеуіне әсер ететін мынадай жағымсыз салдарлар туындауы мүмкін:

1) қорғалатын ақпараттың жария етілуіне, жария етілуіне немесе рұқсатсыз модификациялануына байланысты қаржылық шығындар;

2) жоғалған ақпаратты жоюға және кейіннен қалпына келтіруге байланысты қаржылық шығындар;

3) компанияның ақпараттық ресурстарында рұқсат етілмеген әрекеттермен байланысты қаржылық шығындар;

4) Компания қызметінің ұйымдастырылмауынан келтірілген залал, компанияның өз міндеттемелерін орындай алмауына байланысты қаржылық және беделдік шығындар;

5) объективті емес ақпарат негізінде басқарушылық шешімдер қабылдаудан болатын залал;

6) компания басшылығында объективті ақпараттың болмауынан болатын залал;

7) компанияның беделіне келтірілген залал;

8) залалдың өзге де түрлері.

8 тарау. Ықтимал бұзушының модельдері

30. Компанияда АҚ ықтимал бұзушыларының модельдерінің келесі жіктемесі қабылданды:

    1) ішкі бұзушылар АҚ режимін бейсаналық не қасақана бұзатын Компания қызметкерлері;

    2) сыртқы бұзушылар - Компаниямен еңбек қатынастарымен байланысты емес адамдар (оның ішінде тағылымдамадан өтушілер мен практиканттар), бұзақылық, пайдакүнемдік және өзге де талпыныстардан компанияның ақпараттық ресурстарына залал келтіруге қабілетті іс-әрекеттер жасайтын адамдар.

31. Құқық бұзушының қауіптілігі көбінесе оған қол жетімді ақпараттық ресурстардың саны мен маңыздылығымен анықталады. Осыған сүйене отырып, жоғары және орта буын менеджерлері, ақпараттық ресурстардың әкімшілері және клиенттік және қаржылық ақпараттың үлкен көлемімен жұмыс істейтін адамдар ең қауіпті санаттар болып саналуы керек.

32. Ішкі құқық бұзушылардың негізгі түрлері:

    1) «оқытылмаған / немқұрайлы жұмыскер» – компанияның білместігі бойынша немесе өзінің немқұрайлылығы бойынша өзіне қасақана ниет білдірмейтін бұзушылыққа жол беретін жұмыскері;

    2) «бәсекелес қызметкер» – компанияның қызметкері, жеке дұшпандық немесе басқа себептермен басқа Қызметкерге зиян келтіруге тырысады. Оның іс-әрекетінің нәтижесінде оның «мақсаты» ғана емес, жалпы Компания да зардап шегуі мүмкін;

    3) «мүдделі бұзушы» – үшінші тараптың компанияға қатысты заңсыз әрекеттеріне немесе өз пайдасына мүдделі компания қызметкері. Әдетте, ол компаниямен еңбек қатынастарын одан әрі сақтауға мүдделі және оны тікелей айыптайтын іс-қимыл жасамайды. Ең ықтимал бұзушылық - бұл ақпараттың ағуы (өз пайдасына қызығушылық танытқан жағдайда-қаржылық алаяқтық);

    4) «енгізілген шабуылдаушы» – үшінші тұлғалардың мүддесі үшін заңсыз әрекеттер жасау мақсатында жұмысқа түскен компания қызметкері Компаниямен одан әрі еңбек қатынастарына іс жүзінде мүдделі емес;

    5) «жұмыстан босатылған қызметкер» – компаниямен еңбек қатынастарын өзара талаптарсыз тоқтататын қызметкер. Ол тікелей қол жеткізген ақпараттың ағып кетуі ықтимал;

    6) «ренжіген жұмысшы» – еңбек жағдайларына қанағаттанбаған компания қызметкері немесе, мүмкін, компания басшылығы қызметкердің қызметіне наразы. Кез-келген, тіпті ең қисынсыз бұзушылықтар болуы мүмкін, әсіресе еңбек қатынастары бұзылған кезде.

33. Сыртқы құқық бұзушылардың негізгі түрлері (бұл бөлімде қазіргі уақытта АҚ мамандары қауымдастығында қабылданған терминология қолданылады):

    1) «Script Kiddie», немесе «Бастаушы» – белгілі осалдықтары бар кез-келген ақпараттық ресурсты бұзуға қызығушылық танытқан адам. Компанияның ақпараттық ресурстарын бұзуға бағытталған емес, маңызды қорғаныс құралдары табылған жағдайда шабуылды оңай тоқтатады. Әдетте, кең таралған хакерлік әдістерді қолданады, өз қаражатын дамытпайды;

2) «Black hat» – «Қара хакер» – «Script Kiddie» айырмашылығы, белгілі бір ресурсты бұзуға көп күш жұмсайды, қорғаныс жүйелерін айналып өту «Ар-намыс» мәселесі деп санайды, қарапайым шабуыл құралдарын жасай алады. Өзін-өзі растау мақсатында немесе жеке пайда табу үшін әрекет етеді, өз қызметтерін қылмыстық құрылымдарға сата алады;

3) «Elite hacker» немесе «Гуру» – Ақпараттық жүйелерді бұзу бойынша жоғары деңгейлі маман. Әдетте, ол қылмыстық құрылымдардың немесе бәсекелес ұйымдардың "тапсырысымен" жұмыс істейді. Бірінші жағдайда ол қаржылық алаяқтық жасауға, екіншісінде – ақпараттың ағып кетуіне немесе серверлердің қол жетімсіздігіне және клиенттердің көз алдында компанияның компаға келуіне бағытталған. Арсеналда арнайы бағдарламалық-техникалық қамтамасыз етудің толық спектрі бар, сондай-ақ әлеуметтік инженерия әдістерін пайдаланады;

4) «Партнер» – Компанияның ақпараттық жүйелеріне қол жеткізе алатын серіктес ұйымның немесе еншілес ұйымның қызметкері. Ішкі құқық бұзушының кез-келген түрін анықтауға болады, бірақ ол әдетте аз басқарылады және компанияда қабылданған АҚ талаптары туралы аз біледі;

5) «Консультант» – ақпараттық ресурстарға қол жеткізе алатын сервистік ұйымның қызметкері. Рұқсат етілмеген іс-әрекеттің әртүрлі сценарийлері, әдетте, қызмет көрсетілетін ақпараттық жүйе шеңберінде мүмкін;

6) «Стажер/практикант» – әдетте, ақпарат пен ақпараттық жүйелерге қол жетімділік шектеулі, бірақ ол үнемі компанияның аумағында болады және жанама немесе әлеуметтік инженерия әдістерімен ақпарат ала алады. Осы тағылымдамадан өтушіге/практикантқа жетекшілік ететін компания қызметкерінің өз міндеттеріне немқұрайлы қараған жағдайда ғана елеулі залал келтіруі мүмкін;

7) «Клиент» – қашықтан қызмет көрсету қызметтеріне қол жеткізе алатын Компанияның клиенті. Бұл қызметтерді дұрыс пайдаланбау, сәйкестендіру деректерін жоғалту немесе компанияның ақпараттық активтеріне қол жетімділігі шектеулі болса да, сыртқы құқық бұзушылардың алғашқы үш түрі ретінде әрекет ету кезінде зиян келтіруі мүмкін.

9 тарау. АҚМЖ қатысушылары, олардың өкілеттіктері мен жауапкершіліктері

34. Компанияның Директорлар кеңесі осы АҚ саясатын, оған өзгерістер мен толықтыруларды бекітеді, сондай-ақ компанияның коммерциялық құпиясын айқындау қағидаларын және компанияның коммерциялық құпиясын құрайтын мәліметтер тізбесін бекітеді.

35. Компанияның Басқарма төрағасы осы ақ саясатын іске асыруға жауапты болады.

36. Компания Басқармасы АҚМЖ әзірлеу, енгізу, пайдалану, сүйемелдеу және жетілдіру үшін ресурстардың жеткіліктілігін қамтамасыз етеді, АҚ саласындағы бөлімшелер мен қызметкерлердің өкілеттіктері мен жауапкершілігін айқындайды.

37. Ақпараттық қауіпсіздік бөлімшесі осы ақ саясатының ережелерін іске асыру жөніндегі іс-шараларды жоспарлауды жүзеге асырады, компанияның функционалдық блоктары мен құрылымдық бөлімшелерінің АҚ қамтамасыз ету, АҚМЖ құру, енгізу және қолдау жөніндегі қызметін үйлестіреді және бақылайды, АҚМЖ қойылған мақсаттарына қол жеткізуге жауапты болады.

38. Функционалдық блоктардың, құрылымдық бөлімшелердің басшылары, компания қызметкерлері компанияның АҚ және ІНҚ осы саясатына сәйкес ақпараттық

қауіпсіздікті қамтамасыз ету жөніндегі өз міндеттерін сөзсіз толық орындауға жауапты болады.

39. Компаниядағы ақпараттық қауіпсіздікті сақтамағаны үшін, сондай-ақ осы ақ саясатының ережелерін орындамағаны үшін компанияның әрбір қызметкері Қазақстан Республикасының қолданыстағы заңнамасына және компанияның ІНҚ сәйкес жауапты болады.

40. Ақпараттық қауіпсіздік бөлімшесі АҚ Саясатын өзекті күйде ұстауға жауапты болады.

10 тарау. Қорытынды ережелер

41. Осы ақ саясатын қайта қарау қажеттілігіне қарай, бірақ кемінде бес жылда бір рет жүзеге асырылады. Қайта қарау компания басшылығы тарапынан АҚМЖ талдауының нәтижелері негізінде жүзеге асырылады.

42. АҚ саясаты компанияның ресми веб-сайтында орналастырылған және барлық мүдделі тұлғалар үшін қол жетімді.

43. АҚ саясаты компания қызметкерлеріне жеткізіледі, олар түсініп, орындау үшін қабылдануы керек.