«Қазақстан Халық Банкінің» өмірді сақтандыру жөніндегі «Халық-Life» еншілес компаниясы» АҚ ақпараттық қауіпсіздік САЯСАТЫ

ӨМІРДІ САҚТАНДЫРУ КОМПАНИЯСЫ
HALYK LIFE
КОМПАНИЯ ПО СТРАХОВАНИЮ ЖИЗНИ

Мазмұны

«Қазақстан Халық Банкінің өмірді сақтандыру жөніндегі «Халық-Life» еншілес компаниясы» АҚ ақпараттық қауіпсіздікті қамтамасыз ету мәселелеріне ерекше көңіл бөледі, ақпараттық қауіпсіздікті басқару жүйесін, ақпараттық қауіпсіздік қатерлерінен қорғанудың қолданылатын құралдары мен тәсілдерін үнемі жетілдіреді, сонымен қатар, ақпарат қорғау саласында жоғары деңгейдегі құзіреттілікті қолдау үшін Компания қызметкерлердің үздіксіз оқытылуын қамтамасыз етеді.

Бұл құжат «Ақпараттық технологиялар – Қауіпсіздікті қамтамасыз ету әдістері – Ақпараттық қауіпсіздікті басқару жүйелері - Талаптар» деген ISO 27001:2013 стандартының талаптарына сәйкес әзірленген және Компанияның корпоративтік веб-сайтында ашық жариялау үшін арналған.

Құжат ақпарат қауіпсіздігін қамтамасыз ету мәселесіне көзқарастар жүйесін, ақпаратты қорғау бойынша негізгі қағидаттарды, бағыттар мен талаптарды сипаттайды және құрамында Компания Басқармасы бекіткен Ақпараттық қауіпсіздік саясатының (бұдан әрі - Саясат) негізгі тараулары бар.

Саясаттың нормативтік-құқықтық негізін Қазақстан Республикасының ақпараттық жүйелерді пайдалану және ақпараттық қауіпсіздік мәселелері бойынша заңнамасының қағидалары, сондай-ақ ақпараттық қауіпсіздікті басқарудың халықаралық стандарттарына сәйкес талаптар құрайды.

Саясаттың ережелерін Компания қызметкерлерінің барлығы бірдей міндетті түрде орындауға тиіс, сондай-ақ Компанияның ақпараттық жүйелері мен құжаттарына қол жеткізе алатын клиенттері мен өзге үшінші тұлғалардың назарына, Компаниямен және оның қызметімен тікелей өзара байланысы бар ақпарат бөлігіне қатысты, жеткізілуге тиіс.

Саясатта Компанияның өзі иеленуші әрі пайдаланушы болып табылатын ақпараттық жүйелер мен құжаттардың барлығы қамтылады. Ақпараттық қауіпсіздікті қамтамасыз ету – Компанияның коммерциялық қызметті табысты жүргізуі үшін шарттардың бірі болып табылады. Компания айналысындағы ақпарат Компания активтердің барынша маңыздыларының бірі болып табылады.

Саясат қағидаларының барлығы бағытталған және қол жеткізу көзделген негізгі мақсат - ақпарат қауіпсіздігі үшін қаупі бар оқиғалардан болатын залалды неғұрлым азайту болып табылады (мұндай оқиғалардың алдын алу немесе салдарын барынша жою арқылы).

Ақпараттық қауіпсіздік жай ғана мақсат емес, АҚ қамтамасыз ету Компанияның ақпараттық ресурстарына тән төнуі мүмкін қауіпке байланысты тәуекелдер мен экономикалық шығынды азайту үшін қажет.

Бұл мақсатта ақпараттың негізгі қасиеттерін ұстап отыру қажет, атап айтқанда:

- қолжетімділік – қол жеткізуге тиісті түрде өкілеттігі бар субъектілердің ақпаратқа уақытында, кедергісіз қол жеткізу қабілетімен сипатталатын қасиет;

- конфиденциалдық – аталған ақпаратқа қол жеткізе алатын субъектілер қатарына шектеу қою қажеттігін көрсететін қасиет және жүйенің (ортаның) мұндай ақпаратқа қол жеткізу өкілеттігі жоқ субъектілерден осы ақпаратты құпияда сақтау қабілетін қамтамасыз ету қасиеті;

- тұтастық – ақпараттың бұрмаланбаған күйде болу (қандай да бір тіркелген күйіндегі қалпына қатысты өзгертілмеу) қасиеті.

Сенімді ақпараттық қорғаныс жасау процесі үздіксіз болып табылады. Жеткілікті түрдегі сенімді АҚ жүйесін жасауды қамтамасыз ету мақсатында оның көрсеткіштерін ұдайы реттестіріп отыру қажет, сыртқы және ішкі ортадан төнетін жаңа қауіптерді болдырмау үшін бейімделу керек.

Стандарттарға, рәсімдерге немесе Саясатқа өзгеріс енгізу кезінде, мұндай қажеттіліктің туындау ретіне қарай, қандай да бір кедергілер болмауға тиіс.

Осы аталған қағидаға сәйкес АҚ-ті басқарудың мынадай кезеңдері анықталады (PDCA: Plan-Do-Check-Act моделі):

Plan – жоспарлау (жасау) – Компанияның жалпы стратегиясы мен мақсаттарына сәйкес нәтижелерге қол жеткізу үшін тәуекелдерді басқаруға және АҚ жетілдіруге қатысты тәуекелдерге талдау жасау, Саясатты, мақсаттарды, міндеттерді, процестерді, рәсімдерді, бағдарламалық-аппараттық құралдарды анықтау;

Do – Жүзеге асыру (енгізу және пайдалану) – Саясаттың, бақылау жасау тетіктерінің, процестердің, рәсімдердің, бағдарламалық-аппараттық құралдардың қолданысқа енгізілуі және пайдаланылуы;

Check – Тексеру (мониторинг және талдау) – бағалау және қолдануға болатын жерде Саясатқа, мақсаттар мен практикалық тәжірибеге сәйкес процестердің орындалу сипаттамасына өлшем жасау, сыртқы және ішкі факторлардың өзгеруіне талдау жүргізу;

Act – Түзету (сүйемелдеу және жетілдіру) – АҚ жүйесінің үздіксіз жетілдірілуін қамтамасыз ету мақсатында ақпараттық қауіпсіздіктің жай-күйін тексерудің ішкі және сыртқы нәтижелеріне, басшылық тарапынан талаптарға, өзге де факторларға негізделген түзету жасау және алдын алу шараларын қабылдау.

Компанияның АҚ қамтамасыз ету жүйесін құру және оның функционалдық қызметі мынадай негізгі қағидаттарға сәйкес іске асырылуға тиіс:

- заңдылық – АҚ қамтамасыз ету үшін қолға алынатын кез келген әрекеттер, қолданыстағы заңнама негізінде, Компаниядағы ақпаратты қорғау объектілеріне жағымсыз ықпал-әрекеттерді анықтау, олардың алдын алу, локализациялау және жолын кесудің заңнамамен рұқсат етілген барлық әдісін қолдану арқылы жүзеге асырылады;

- бизнеске бағдарлану – АҚ Компанияның негізгі қызметіне қолдау жасау процесі ретінде қарастырылады. АҚ қамтамасыз ету бойынша шаралардың қайсысы болсын, Компания қызметі үшін айтарлықтай күрделі кедергі жасауға әкеп соқпауға тиіс;

- үздіксіздік – ақпаратты қорғау жүйелерін басқару құралдарын қолдану, Компанияның ақпараттық қорғанысын қамтамасыз ету бойынша іске асырылатын шаралардың кез келгені Компаниядағы ағымдағы бизнес-процестерді үзбестен немесе тоқтатусыз жүргізілуге тиіс;

- кешенділік – ақпараттық ресурстардың бүкіл циклы барысында, ресурстарды пайдаланудың технологиялық кезеңдерінің барлығында және функционалдық режимінің барлығында ақпарттың қауіпсіздігін қамтамасыз ету;

- негізділік және экономикалық орындылық - пайдаланылатын қорғаныс мүмкіндіктері мен құралдары ғылым мен техниканы дамытудың тиісті деңгейінде жүзеге асырылуға тиіс, қауіпсіздіктің тиісті деңгейі тұрғысынан негізделген болу керек және қойылатын талаптар мен тиісті нормаларға сәйкес келуге тиіс. Барлық жағдайда да АҚ шаралары мен жүйелерінің құны тәуекелдің кез келген түрінен келтірілуі мүмкін болатын шығын мөлшерінен аз болуы керек;

- басымдылық – Компаниятің ақпараттық ресурстарының барлығын ақпараттық қауіпсіздікке төнетін шынайы әрі ықтимал (әлеуетті) қаупіне баға беру кезінде маңыздылық деңгейіне қарай жіктемелеу (ранжирлеу);

- қажетті білім және артықшылықтардың барынша төмен деңгейі – пайдаланушы өзіне берілген өкілеттік шеңберінде артықшылықтарды барынша аз деңгейде және қызметтік міндеттерін орындау үшін қажетті болып табылатын мәліметтерге ғана қол жеткізу мүмкіндігін алады;

- мамандану – техникалық құралдарды пайдалануды және АҚ шараларын жүзеге асыруды Компаниятің кәсіби дайындығы бар мамандары жүзеге асырады;

- ақпарат алу және дербес жауапкершілік – барлық деңгейдегі басшылар мен орындаушылар АҚ бойынша талаптардың барлығы туралы хабардар болуға тиіс және олар осы талаптар мен АҚ бойынша белгіленген шаралардың орындалуы үшін дербес жауапкершілік арқалайды;

- өзара әрекет жасау және үйлестіру – АҚ бойынша шаралар Компаниятің тиісті құрылымдық бөлімшелерінің өзара үйлесімді әрекеттері негізінде, олардың алға қойылған мақсатқа қол жеткізуге күш салуы, сондай-ақ сыртқы ұйым-мекемелермен, кәсіби қоғамдастықтармен, бірлестіктермен, мемлекеттік органдармен, заңды және жеке тұлғалармен қажетті байланыс орнатуы негізінде жүзеге асырылады;

- растаушылық – маңызды құжаттама және АҚ бойынша талаптардың орындалуын және оны ұйымдастыру жүйесінің тиімділігінің орындалуын растайтын барлық жазба-құжаттар, оперативті түрде қол жеткізу және қалпына келтіру мүмкіндігімен жасалып, сақталуға тиіс.

Компаниядағы АҚ қамтамасыз етудің негізгі объектілері мына төмендегі элементтер болып табылады:

- қолданыстағы заңнамаға және Компанияның ішкі нормативтік құжаттарына сәйкес Компанияның және коммерциялық құпияға, дербес деректерге, қаржылық ақпаратқа жатқызылған мәліметтері бар ақпараттық ресурстар, Компанияның қалыпты қызмет жасауын қамтамасыз ету үшін қажетті кез келген өзге ақпарат (бұдан әрі – қорғалатын ақпарат);

- қорғалатын ақпаратты өңдеу, жіберу және сақтау жүргізілетін ақпараттандыру құралдары мен жүйелері (есептеу техникасының құралдары, ақпараттық-есептегіш кешендері, желілер, жүйелер);

- Компанияның автоматтандырылған жүйесінің бағдарламалық құралдары (операциялық жүйелер, мәліметтер базасын басқару жүйелері, басқа жалпыжүйелік және қолданбалы бағдарламалық жасақтама), бұлардың көмегімен қорғалатын ақпаратқа өңдеу жүргізіледі;

- ақпараттық ресурстарды басқарумен және пайдаланумен байланысты Компания процестері;

- қорғалатын ақпаратты өңдеу құралдары орналастырылған үй-жайлар;

- Компания қызметкерлерінің жұмыс істейтін үй-жайлары мен кабинеттері, жабық келіссөздер мен жиналыстар жүргізу үшін арналған Компания үй-жайлары;

- қорғалатын ақпаратқа қол жеткізе алатын Компания қызметкерлері;

- ашық ақпаратты өңдейтін, бірақ қорғалатын ақпарат өңделетін үй-жайларда орналастырылған техникалық құралдар мен жүйелер.

Қорғалуы тиіс ақпарат:

- қағаздық тасымалдаушыда орналастырылуы мүмкін;
- электрондық нұсқа түрінде болуы мүмкін (есептеуіш техника құралдарымен өңделуі, жіберілуі және сақталуы мүмкін, техникалық құралдар көмегімен жазылуы және қайта жаңғыртылуы мүмкін);
- телефон арқылы, телефакс, телекс бойынша, т.с.с. және электрондық дабыл белгісі түрінде жіберілуі мүмкін;
- әуелік ортада акустикалық және вибрациялық дабыл түрінде және жиылыстар мен келіссөздер жүргізу кезінде қоршалған конструкцияларда болуы мүмкін.

Осы Саясат Компания қызметкерлерінің барлығына бірдей және Компанияның ақпараттық ресурстарына қалай да қол жеткізе алатын немесе ақпарат алмасу процестеріне араласа алатын үшінші тұлғаларға қатысты қолданылады.

АҚ-ке төнетін қауіп ретінде ақпараттық басты қасиеттерін бұзудың ықтимал (әлеуетті) мүмкіндігі түсініледі.

АҚ төнетін қауіп былайша бөлінеді:

- кездейсоқ – табиғи апаттар, Компания қызметкерлерінің тарабынан байқаусыз жасалған қате әрекеттер, аппараттық және бағдарламалық құралдардың қатесі және т.б.;

- қасақана – яғни мәліметтерді әдейі бұрмалау немесе жою, мәліметтерді заңсыз жолмен пайдалану, компьютерлік қылмыс түрлері және т.б.

АҚ төнетін қауіпке мыналар жатады (бірақ мұнымен шектелмейді):

- Компания құпиясын құрайтын, Компанияның коммерциялық құпиясы болып табылатын және өзге де қорғалатын ақпараттың жоғалуы;

- қорғалатын ақпараттың бұрмалануы (рұқсат етілмеген модификация, жалған ақпарат);

- ақпараттың сыртқа шығарылуы (ағылуы) – қорғалатын ақпаратпен бөтен адамдардың (сырт тұлғалардың) рұқсатсыз танысуы (рұқсатсыз қол жеткізу, көшіру, ұрлау, т.б.);

- ақпараттық ресурстарды рұқсатсыз пайдалану (асыра пайдалану, алаяқтық жасау, т.б.);

- ақпараттың оқшауланууы, құрал-жабдықтағы немесе бағдарламадағы ақаудың, жұмыс станцияларындағы операциялық жүйелердің, серверлердің әрекет етуші желілік құрал-жабдықтың, мәліметтер базасын басқару жүйесінің, бөлінген есептеуіш желілерінің функционалдығының дұрыс ұйымдастырылмауы, вирустар әсерінің, табиғи апаттар және өзге де форс-мажорлық жағдайлар мен қасақана әрекеттер салдарынан ақпаратқа қол жеткізілмеуі.

Осы аталған қауіп-қатердің әсері нәтижесінде Компанияның АҚ жағдайына және оның қалыпты функциялық әрекет істеуіне ықпалы тиетіндей жағымсыз салдар туындауы мүмкін:

- қорғалатын ақпараттың жайылуына, жария етілуіне немесе оның рұқсат етілмеген түрлендірілуіне байланысты қаржылық жоғалтулар;
- жоғалған ақпаратты жоюмен және одан әрі қайта қалпына келтірумен байланысты қаржылық жоғалтулар;
- Компанияның ақпараттық ресурстарында рұқсат етілмеген әрекеттермен байланысты қаржылық жоғалтулар;
- Компания қызметінің дұрыс ұйымдастырылмауынан келетін залал және Компанияның өз міндеттемелерін орындай алмауымен байланысты қаржылық және беделдік жоғалтулар;
- басқарушылық шешімдерді объективтік емес ақпарат негізінде қабылдаудан келген шығын;
- Компания басшылығында объективті ақпараттың болмауы салдарынан келген шығын;
- Компания беделіне келтірілген нұқсан;
- залалдың өзге түрлері.

АҚ тәртібін бұзушылар былайша жіктелінеді:

- ішкі бұзушылар – АҚ тәртібін абайсыздықпен немесе қасақана бұзатын Компания қызметкерлері;

- сыртқы бұзушылар – Компаниямен өзара еңбек қатынасында тұрмайтын, бұзақылық немесе пайдакүнемдік ниетпен әрекет жасаушы, Компанияның ақпараттық ресурстарына шығын келтіре алатын тұлғалар (оның ішінде машықтанушылар және практиканттар).

АҚ тәртібін бұзушының қауіптілігі көпшілік жағдайда оның қол жеткізе алатын ақпараттық ресурстарының санымен және маңыздылық дәрежесімен айқындалады. Осыған байланысты неғұрлым тәуекелді қызметкерлер санатына жоғары және орта буындағы менеджерлерді, ақпараттық ресурстар әкімшілерін, сондай-ақ үлкен көлемдегі клиенттік және қаржылық ақпаратпен жұмыс істейтін тұлғаларды жатқызуға болады.

Ішкі бұзушылардың негізгі түрлері:

- «үйретілмеген/салдыр-салақ қызметкер» - өзінің білместігінен немесе немқұрайлығынан қасақаналық ойы жоқ тәртіп бұзушылыққа жол беретін Компания қызметкері;

- «бәсекелес қызметкер» - өзінің жеке басының кінәратына немесе басқа себепке байланысты өзге қызметкерге нұқсан келтіруге тырысатын Компания қызметкері. Оның мұндай әрекетінің салдарынан жеке өзінің «мақсаты» ғана емес, сондай-ақ тұтастай Компания те зардап шегуі мүмкін;

- «мүдделі бұзушы» - Компанияға қатысты немесе өзінің жеке басының пайдасы үшін үшінші тараптың заңсыз әрекеттер жасауына мүдделі Компания қызметкері. Әдетте, мұндай қызметкер Компаниямен өзара еңбек қатынастарын одан әрі сақтауға мүдделі болады және өзінің беделін түсіретін (атына кір келтіретін) тікелей әрекеттерге бармайды. Неғұрлым жол берілуі мүмкін бұзушылық - ақпараттың ағылуы (өзінің жеке басының пайдасы үшін мүдделі болған жағдайда – қаржылық алаяқтық);

- «енгізілген қаскөй» - үшінші бір тұлғалардың мүддесі үшін заңсыз әрекеттер жасау мақсатында жұмысқа кірген Компания қызметкері. Компаниямен одан әрі еңбек қатынасында тұруға мүдделі емес деуге болады;

- «жұмыстан шығатын қызметкер» - Компаниямен еңбек қатынасын ешқандай өзара кінәратсыз доғаратын қызметкер. Неғұрлым мүмкін болатын салдары - өзі тікелей қол жеткізе алған ақпараттың сыртқа ағылуы;

- «өкпелі қызметкер» - еңбек қызметінің жағдайларына қанағаттанбаған Компания қызметкері немесе басқа бір нұсқасы – қызметкердің жұмысына Компания басшылығының көңілі толмайтыны анық. Кез келген, тіпті қисынсыз бұзушылыққа, әсіресе, еңбек қатынастары үзілетін сәтте, жол берілуі мүмкін.

Сыртқы бұзушылардың негізгі түрлері (бұл бөлімде АҚ бойынша мамандар қоғамдастығында қазіргі сәтте қабылданған терминология пайдаланылады):

- «Script Kiddie» немесе «Бастаушы» – кез келген ақпараттық ресурстың бұзылуына мүдделі, жалпыға белгілі қауқарсыздық танытатын тұлға. Дәл Компанияның ақпараттық ресурстарын бұзу мақсатын алдына қоймайды, маңызды қорғаныс құралдары табылған жағдайда шабуыл әрекеттерін оңай тоқтатады. Әдетте, бұзушылықтың жалпыға кеңінен таралған әдістерін пайдаланады, өзінің қорғаныс құралдарын жасамайды;

- «Black hat» – «Қара хакер» – «Script Kiddie» салыстырғанда, нақты ресурсты бұзуға табандылық көрсетеді, қорғаныс жүйесін айналып өткенді жөн санайды, қарапайым шабуыл құралдарын жасай алады. Өзін-өзі таныту мақсатында немесе жеке басының пайдасы үшін әрекет жасайды, өз қызметін қылмыстық құрылымдарға сатуы мүмкін;

- «Кеңесші (консультант)» - ақпараттық ресурстарға қол жеткізу мүмкіндігі бар сервистік компанияның қызметкері. Рұқсат берілмеген қызмет көріністерінің түрлі сценарийлері дамуы мүмкін, әдетте қызмет көрсетілетін ақпараттық жүйе шеңберінде мүмкін болады;

- «Elite hacker» немесе «Гуру» – ақпараттық жүйелерді бұзу бойынша жоғары білікті маман. Әдетте, қылмыстық құрылымдардың немесе бәсекелес ұйымдардың тапсырысы бойынша жұмыс істейді. Бірінші жағдайда қаржылық алаяқтық жүргізуді жоспарлайды, екінші жағдайда – ақпараттың сыртқа ағылуын, не болмаса серверге қол жеткізілмеуін және Компанияның клиенттер алдында беделін жоғалтуын көздейді. Сонымен қатар қолында арнаулы бағдарламалық-техникалық жасақтамасының толық спектрі болады және әлеуметтік инженерия әдістерін кеңінен пайдалана алады.

- «Серіктес» - Компанияның ақпараттық жүйелеріне қол жеткізе алатын серіктес-ұйымның немесе еншілес ұйымның қызметкері. Ішкі тәртіп бұзушының кез келген тұрпатына сәйкестікпен айқындауға болады және Компанияда қабылданған АҚ талаптары туралы хабары аз;

- «Машықтанушы /Практикант» - әдетте ақпарат пен ақпараттық жүйелерге қол жеткізу мүмкіндігі шектеулі болады, дегенмен, Компания аумағында тұрақты бола алатындықтан, ақпаратты жанама түрде немесе әлеуметтік инженерия әдісімен алуы мүмкін. Аталған машықтанушыға /практикантқа жетекшілік жасаушы Компания қызметкері өз міндетіне немқұрайлы қарайтын жағдайда ғана кәдімгідей залал келтіре алады.

- «Клиент» - Компанияның қашықтықтан қызмет көрсету сервистеріне қол жеткізу мүмкіндігі бар Компания клиенті. Аталған сервистер дұрыс пайдаланылмаған, сәйкестендіру мәліметтері жоғалған жағдайда шығын келтіруі мүмкін, не болмаса Компанияның ақпараттық ресурстарға шектеулі түрде қол жеткізе отырып, сыртқы бұзушылардың алғашқы үш түріне тән әрекеттер жасауы мүмкін.

Компанияда АҚ-ті қамтамасыз етудің негізгі шаралары мыналар болып табылады:

- әкімшілік-құқықтық және ұйымдық шаралар;
- физикалық (табиғи) қауіпсіздік шаралары;
- бағдарламалық-техникалық шаралар.

Әкімшілік-құқықтық және ұйымдық шараларға мыналар жатады (алайда, мұнымен шектелмейді):

- Қазақстан Республикасы заңнамасының және Компанияның ішкі құжаттары талаптарының орындалуын бақылау;
- Саясатты қолдайтын қосымша ережелер, әдістемелер мен нұсқаулықтар жасау, оларды енгізу және орындалуын бақылау;
- бизнес-процестердің Саясат талаптарына сәйкес келуін бақылау;
- Компания қызметкерлерін ақпараттық ресурстармен және АҚ талаптарымен жұмыс істеу туралы хабардар ету және оқыту;
- инциденттерге (қолайсыз жағдайларға) жауап ретінде әрекет жасау, салдарын барынша оқшаулау және азайту;
- АҚ жаңа тәуекелдеріне талдау жасау;
- ұжымдағы моральдық-іскерлік ахуалды қадағалау және жақсарту;
- төтенше жағдайлар туындағанда қолға алынатын әрекеттерді айқындау;
- Компания қызметкерін жұмысқа қабылдағанда және жұмыстан шығарғанда профилактикалық іс-шаралар жүргізу.

Физикалық қауіпсіздік шаралары мыналардан құралады (алайда, мұнымен шектелмейді):

- объектіге өту тәртібін және объект ішіндегі режимді ұйымдастыру;
- қорғалатын объектілердің қауіпсіздік периметрлерін құрастыру;
- режимді объектілердің тәулік бойы, оның ішінде қауіпсіздіктің техникалық құралдарын пайдалану арқылы күзетілуін ұйымдастыру;
- күзетілетін объектілердің өртке қарсы қауіпсіздігін ұйымдастыру;
- қол жеткізуге (кіруге) шектеу қойылған үй-жайларға Компания қызметкерлерінің қол жеткізуін бақылау.

Бағдарламалық-техникалық шараларға мыналар жатады: (алайда, мұнымен шектелмейді):

- лицензияланған бағдарламалық жасақтаманы және ақпаратты қорғаудың сертификатталған құралдарын пайдалану;
- қорғаныс периметрінің құралдарын (firewall, Intrusion Prevention System (IPS) т.с.с.) пайдалану;
- вирусқа қарсы кешенді қорғаныс қолдану;
- ақпараттық жүйенің өз ішінде енгізілген АҚ құралдарын пайдалану;
- АҚ бойынша арнаулы кешенді құралдарды пайдалану (электронды ақпараттық ресурстарды қорғау болсын, сондай-ақ ақпараттың электромагниттік және акустикалық арналар бойынша ағылуынан болсын);
- ақпараттан ұдайы резервтік көшірме жасауды қамтамасыз ету;
- ақпаратты пайдаланушылардың, ең алдымен артықшылығы бар пайдаланушылардың құқықтары мен әрекеттерін бақылау;
- ақпараттың криптографиялық қорғаныс жүйесін қолдану;
- аппарат құралдарының тоқтаусыз жұмыс істеуін қамтамасыз ету;
- ақпараттық жүйенің күрделі элементтерінің жай-күйіне мониторинг жүргізу.

Саясат және АҚ жүйесі тұтастай мына төмендегі нормативтік құқықтық актілерге және халықаралық стандарттарға негізделеді (осы аталған бөлімде Компанияның тұтастай алғандағы АҚ жүйесін жасау процесіне тікелей әсер етуші нормативтік актілер көрсетілген; сонымен қатар АҚ-ті мемлекеттік деңгейде дамытудың стратегиялық аспектілері сипатталатын немесе жекелеген қосымшалардың /қызметтердің ақпараттық қорғаныс бойынша ережелері реттелетін бірқатар құжаттар бар):

- Қазақстан Республикасының «Қазақстан Республикасындағы Банктер және Компания қызметі туралы» 1995 жылғы 31 тамыздағы № 2444 Заңы;
- Қазақстан Республикасының «Электрондық құжат және электрондық қол қою туралы» 2003 жылғы 7 қаңтардағы № 370-II Заңы;
- Қазақстан Республикасының 2015 жылғы 24 қарашадағы \№418—V «Ақпараттандыру туралы» Заңы;
- Қазақстан Республикасының 1998 жылғы 22 желтоқсандағы № 326-I «Ұлттық архив қоры және архивтер туралы» Заңы;
- Қазақстан Республикасы Ұлттық Банк Басқармасының «Екінші деңгейдегі Банктерде және Банктік операциялардың жекелеген түрлерін іске асыратын ұйымдарда ақпараттық жүйелердің қауіпсіздігін қамтамасыз ету ережелерін бекіту туралы» 2001 жылғы 31 наурыздағы № 80 қаулысы
- Қазақстан Республикасының Ұлттық Банкі Басқармасының 2014 жылғы 26 ақпандағы «Екінші деңгейдегі Банктерге арналған тәуекелдерді басқару және ішкі бақылау жүйесін қалыптастыру кағидаларын бекіту туралы» №29 қаулысы;
- «Ақпараттық технологиялар – Қауіпсіздікті қамтамасыз ету әдістері – Ақпараттық қауіпсіздікті басқару жүйелері - Талаптар» деген ISO/IEC 27001:2013 халықаралық стандарты (СТ РК ИСО/МЭК 27001-2008);
- PCI DSS халықаралық стандарты, 3.2 нұсқасы (Payment Card Industry Data Security Standard – төлем карталары индустриясының мәліметтер қауіпсіздігінің стандарты).

Компанияда нормативтік құқықтық актілер талаптарын орындауды, зияткерлік (интеллектуалдық) меншік құқығын сақтауды, заңмен қорғалатын дербес ақпаратты қорғауды, криптографиялық құралдарды пайдалануға шектеулердің орындалуын қамтамасыз ету үшін тиісті процестер енгізілуге тиіс.

ISO/IEC 27001 және PCI DSS халықаралық стандарттарының барлық талаптары мен қағидалары тиісті құжаттармен анықталатын қолдану саласында (scope) орындалуға міндетті болып табылады.

АҚ құралдары мен әдістерін жасағанда және қолданғанда Компанияның үшінші тұлғалармен бекітілетін шарттық міндеттемелері мен келісім-шарттарының талаптары ескерілуге тиіс.

Компанияның ақпараттық ресурстарына үшінші тараптың қол жеткізуі тек осындай қол жеткізу құқығы берілгенде туындауы мүмкін тәуекелдерге талдау жасалғаннан кейін және барабар қорғаныс шаралары қабылданған соң ғана жүзеге асырылады.

Қажет болған жағдайда (оның ішінде, нормативтік құқықтық актілердің немесе халықаралық стандарттардың талаптары болған жағдайда) Компания контрагенттерге (тауарды жеткізушілерге, қызмет көрсетушілерге) қатысты олардың белгілі бір талаптарға сәйкестігі (мәселен, ұсынылатын қызметтердің PCI DSS стандартының талаптарына сәйкестігін растайтын құжаттарды) тұрғысынан тексеру (screening) жүргізеді.

Саясаттың негізінде АҚ-ті қамтамасыз етудің нақты ережелері мен әдістерін реттейтін бірқатар ішкі нормативтік бағыныштық құжаттар, стандарттар әрекеті саласындағы жеке-дара саясаттар, т.б. құжаттар жасалады. Бұл аталған құжаттар Саясаттың талаптарын толықтыруы және кеңейте түсуі мүмкін, алайда онымен қарама-қайшылықта бола алмайды.

«Қазақстан Халық Компанияінің өмірді сақтандыру жөніндегі «Халық-Life» еншілес компаниясы» АҚ ақпараттық қауіпсіздік Саясатымен танысу үшін алғысымызды білдіреміз!