«Бекітілді»
Жалғыз қатысушының шешімімен
ЖШС «Ломбард Верный»
Бұйрық № 01/02-П
«22» сәуір 2024 жыл

Интернет-ресурс және терминалдар арқылы қызмет көрсету кезінде ақпараттық қауіпсіздік және ақпаратты рұқсатсыз қол жеткізуден қорғау саясаты.

Алматы облысы
2024 жыл

Алғысөз

Енгізілгені: 22 сәуір 2024 жыл.
Қайта қарау мерзімі: 2026 жыл немесе Қазақстан Республикасының заңнамасына енгізілген өзгерістерге сәйкес және қажеттілігіне қарай бұрын жүргізілген жағдайда.

Мазмұны

1. Жалпы ережелер

1. ЖШС «Ломбард Верный» интернет-ресурстар (веб-сайт) және (немесе) терминалдар (бұдан әрі - Компания) арқылы қызмет көрсету кезінде ақпаратты рұқсатсыз қол жеткізуден қорғау және қауіпсіздік саясаты Қазақстан Республикасының ақпараттық қауіпсіздік саласындағы заңнамасына, уәкілетті органның актілеріне және ұйымның ішкі құжаттарына сәйкес әзірленді.
2. Осы Саясаттың негізгі мақсаты ақпараттың қауіпсіздігіне қатер төндіруі мүмкін оқиғалардан келтірілген залалды олардың алдын алу немесе олардың салдарын барынша азайту жолымен барынша азайту болып табылады. ақпараттық қауіпсіздікті қамтамасыз ету – бұл өз-өзінен соңы емес; Ұйымның ақпараттық ресурстарымен бетпе-бет келетін түрлі қауіп-қатерлерге байланысты тәуекелдер мен экономикалық шығындарды азайту қажет. Ол үшін ақпараттың негізгі сипаттамаларын сақтаудың маңызы зор:

    - Қол жетімділік: уәкілетті субъектілердің ақпаратқа уақтылы және кедергісіз қол жеткізуін қамтамасыз ету.
    - Құпиялылық: ақпаратқа қол жеткізуі бар адамдар шеңберіне шектеулер енгізу және оның рұқсат етілмеген адамдардың қол жеткізуінен қауіпсіздігін қамтамасыз ету.
    - Тұтастық: ақпаратты белгілі бір күйге қатысты бұрмалауға немесе өзгертуге ұшыратпай өзгеріссіз сақтау.

3. Осы Саясат мынадай құжаттардың негізінде әзірленді:

– Қазақстан Республикасының Ұлттық Банкі Басқармасының 2019.11.28 № 217 қаулысы.

– ISO/IEC 27001:2022 Ақпараттық технологиялар — Қауіпсіздік техникасы — Ақпараттық қауіпсіздікті басқару жүйелері — Талаптар;

– ISO/IEC 27002:2022 Ақпараттық технологиялар – Қауіпсіздік техникасы – ақпараттық қауіпсіздікті басқару ережелері мен ережелері.

4. Саясаттың негізгі қағидаттары мыналар болып табылады:
    - заңдылық – ақпараттық қауіпсіздікті қамтамасыз ету үшін қабылданған кез келген іс-әрекеттер қолданыстағы заңнама негізінде, Компанияның ақпаратты қорғау объектілеріне жағымсыз әсерлерді анықтау, алдын алу, оқшаулау және жолын кесу үшін заңмен рұқсат етілген барлық әдістерді пайдалана отырып жүзеге асырылады;
    - бизнеске баса назар аудару – ақпараттық қауіпсіздік негізгі қызметті қолдау процесі ретінде қарастырылады. Ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі кез келген шаралар Компанияның қызметіне елеулі кедергі келтірмеуге тиіс;
    - үздіксіздік – ақпараттық қауіпсіздік жүйесін басқару құралдарын пайдалану, Компанияның ақпаратты қорғауды қамтамасыз ету жөніндегі кез келген іс-шараларды іске асыру Компанияның ағымдағы бизнес-процестерін үзбей немесе тоқтатпай жүзеге асырылуы тиіс;
    - күрделілік – ақпараттық ресурстардың өмірлік цикл бойы, оларды пайдаланудың барлық технологиялық кезеңдерінде және барлық жұмыс режимдерінде қауіпсіздігін қамтамасыз ету;
    - Техникалық-экономикалық орындылық - қолданылатын қорғаудың мүмкіндіктері мен құралдары ғылым мен техниканың тиісті даму деңгейінде іске асырылуы тиіс, қауіпсіздіктің белгіленген деңгейі тұрғысынан негізделген және талаптар мен стандарттарға сәйкес келуге тиіс. Барлық жағдайларда ақпараттық қауіпсіздік шаралары мен жүйелерінің құны тәуекелдің кез келген түрлерінен болуы мүмкін залалдың мөлшерінен кем болуы тиіс;

- басымдылық – Компанияның барлық ақпараттық ресурстарын ақпараттық қауіпсіздікке нақты және әлеуетті қауіп-қатерлерді бағалау кезінде маңыздылық дәрежесі бойынша санаттау (рейтингтеу).

5. Осы Саясат мыналарды анықтайды:
   - Компанияның ақпараттық қауіпсіздігін қамтамасыз ету жөніндегі негізгі шаралар, оның ішінде ақпараттық қауіпсіздік қатерін барынша азайту, яғни ақпараттық қауіпсіздік инцидентінің туындауына алғышарттар жасайтын жағдайлар мен факторлардың жиынтығы;
   - екі факторлы аутентификация және әлеуетті қарыз алушыларды интернет-ресурс, терминалдар және (немесе) веб-сайт арқылы тексеру әдістері;
   - микрокредит беру туралы шарт бойынша тараптардың міндеттемелері тоқтатылғаннан кейін кемінде 5 (бес) жыл ішінде олардың тұтастығы мен құпиялылығын сақтай отырып, қарыз алушыға берілетін және одан алынған электрондық хабарламалар мен өзге де құжаттарды қауіпсіз сақтауды қамтамасыз ету;
   - үшінші тұлғалардың жоспарлы құқық бұзушылықтардың алдын алу жөніндегі шаралар.
6. Осы Саясаттың ережелері объектілердің мынадай тізбесіне қолданылады:
   - Компанияның бизнес-бөлімшелерінің қызметкерлері (тағылымдамадан өтушілер мен тағылымдамадан өтушілерді қоса алғанда);
   - Компанияның ақпараттық жүйелері мен құжаттарына қол жеткізуі бар және басқа да үшінші тұлғалардың қарыз алушылары, олардың бөлігінде Компанияның және олардың қызметімен тікелей байланысты;
   - Компаниямен шарттық қатынастарға ие жеткізушілерге, үшінші тұлғаларға және тараптарға;
   - құпия ақпаратты, кездейсоқ және рұқсат етілмеген әсерлерге және олардың қауіпсіздігін бұзуға сезімтал өзге де ақпаратты, ақпараттық ресурстарды (деректер базасы, файлдар, жүйелік құжаттама, пайдаланушы жөніндегі нұсқаулықтар, оқу материалдары, саясаттар мен рәсімдер және т.б.), оның ішінде жалпыға қолжетімді ақпаратты электрондық түрде ұсынатын ақпараттық ресурстар;
7. Компанияның ақпараттық инфрақұрылымы, оның ішінде ақпаратты өңдеу және талдау жүйелері, ақпарат алмасу және телекоммуникация арналарын, деректерді жеткізушілерді, ақпараттық қауіпсіздік жүйелері мен құралдары, IT-ресурстардың элементтері орналасқан үй-жайлар мен үй-жайларды қоса алғанда, оны өңдеуге, беруге және көрсетуге арналған аппараттық-бағдарламалық қамтамасыз ету.
8. **Осы Саясат қоғамдық құжат болып табылады және Компанияның ресми сайтында https://tezbai.kz/**
9. Ақпаратты сенімді қорғауды құру процесі ешқашан аяқталмайды. Ақпараттық қауіпсіздіктің жеткілікті сенімді жүйесін қамтамасыз ету үшін оның параметрлерін үнемі түзетіп отыру, сыртқы және ішкі ортадан шығатын жаңа қауіптерге тойтарыс беруге бейімделу қажет.

2. Ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі шаралар

10. Компанияның ақпараттық қауіпсіздігін қамтамасыз ету жөніндегі негізгі шаралар мыналар болып табылады:
    - әкімшілік, құқықтық және ұйымдастырушылық шаралар;
    - физикалық қауіпсіздік шаралары;
    - бағдарламалық және техникалық іс-шаралар.

10.1. Әкімшілік, құқықтық және ұйымдық шаралар мыналарды қамтиды (бірақ олармен шектелмейді):
- Қазақстан Республикасы заңнамасының және ішкі құжаттардың талаптарының сақталуын бақылау;
- Саясатты қолдайтын ережелерді, әдістер мен нұсқауларды әзірлеу, іске асыру және іске асырылуын бақылау;
- бизнес-процестердің Саясат талаптарына сәйкестігін бақылау;
- Компания қызметкерлерін ақпараттық жүйелермен және ақпараттық қауіпсіздік талаптарымен жұмыс істеуге ақпараттандыру және оқыту;
- инциденттерге ден қою, салдарын тежеу және азайту;
- ақпараттық қауіпсіздіктің жаңа тәуекелдерін талдау;
- ұжымдағы моральдық-іскерлік ахуалды бақылау және жақсарту;
- төтенше жағдайлар туындаған жағдайдағы іс-қимылдарды анықтау;
- Кәсіпорын қызметкерлерін жұмысқа қабылдау және жұмыстан босату жөніндегі алдын алу шаралары.

10.2. Физикалық қауіпсіздік шаралары мыналарды қамтиды (бірақ олармен шектелмейді):
- күзетілетін объектілерді, оның ішінде техникалық қауіпсіздік техникасын пайдалануды тәулік бойы күзетуді ұйымдастыру;
- күзетілетін объектілердің өрт қауіпсіздігін ұйымдастыру;
- Компания қызметкерлерінің және үшінші тұлғалардың шектеулі үй-жайларға (серверлерге) қол жеткізуін бақылау.

10.3. Бағдарламалық-техникалық іс-шаралар мыналарды қамтиды (бірақ олармен шектелмейді):
- лицензияланған бағдарламалық қамтамасыз етуді және сертификатталған ақпараттық қауіпсіздік құралдарын пайдалану;
- вирусқа қарсы кешенді қорғау құралдарын қолдану;
- периметрді қорғау құралдарын (брандмауэр, антивирус және т.б.) пайдалану;
- ақпараттық жүйелерге құрылған ақпараттық қауіпсіздік құралдарын пайдалану;
- ақпараттың тұрақты резервтік көшірмесін қамтамасыз ету;
- пайдаланушылардың, ең алдымен артықшылықты пайдаланушылардың құқықтары мен іс-әрекеттерін бақылау;
- ақпаратты криптографиялық қорғау жүйелерін қолдану;
- Аппараттық құралдардың уақытын қамтамасыз ету.
- Бастапқы кодты, компоненттер мен кітапханаларды сыналған бағдарламалық қамтамасыз етуде пайдаланылатын барлық бағдарламалау тілдерін талдауды қолдайтын статикалық бастапқы кодты талдау сканерін пайдалана отырып талдау.

3. Ақпараттық қауіпсіздік саласындағы тәуекелдерді бағалау

11. Компанияның ақпараттық қауіпсіздігі саласындағы тәуекелдерін бағалау мақсатында мынадай шаралар қабылданады:
    - аса маңызды ақпараттық активтер тізбесін қалыптастыру;
    - Аса маңызды ақпараттық активтер үшін ақпараттық қауіпсіздік тәуекелдерін бағалау.
12. Аса маңызды ақпараттық активтердің тізбесіне жылжымайтын мүлік объектілерінің бұзылуынан болған шығындар ақпараттық қауіпсіздікті бұзудан болған шығындардың материалдықлықтың белгіленген деңгейінен асатын ақпараттық активтер енгізіледі.
13. Аса маңызды ақпараттық активтер үшін ақпараттық қауіпсіздік тәуекелдерін бағалау мақсатында Компания мынадай процестерді іске асыруды қамтамасыз етеді:
    - аса маңызды ақпараттық активтерге ақпараттық қауіпсіздік қатерін анықтау;
    - аса маңызды ақпараттық активтерге қатысы бар ақпараттық қауіпсіздікке қатер төндіретін көздерді анықтау;
    - аса маңызды ақпараттық активтердің осал тұстарын анықтау;
    - ақпараттық қауіпсіздік тәуекелдерін басқару жөніндегі қолданыстағы шараларды айқындау;
    - ақпараттық қауіпсіздікке қатер төндіретін көздермен іске асырылатын аса маңызды ақпараттық активтерге ақпараттық қауіпсіздікке қатер төну ықтималдығын бағалау;
    - ақпараттық қауіпсіздік тәуекелдерінің деңгейін бағалау.
14. Ақпараттық қауіпсіздіктің аса маңызды активтеріне ақпараттық қауіпсіздік қатерін анықтауды ақпараттық қауіпсіздік бөлімшесі жүзеге асырады. Ақпараттық активтің әрбір сыни түрлері бойынша ақпараттық қауіпсіздікке төнетін қатерлерге талдау жүргізіледі.
15. Аса маңызды ақпараттық активтерге қатысы бар ақпараттық қауіпсіздік қатерлерінің көздерін анықтауды ақпараттық қауіпсіздікке төнетін қатерлердің көздерін ескере отырып, Компанияның ақпараттық қауіпсіздік бөлімшесі жүзеге асырады.
16. Аса маңызды ақпараттық активтердегі осал тұстарды анықтауды Компанияның ақпараттық қауіпсіздік бөлімшесі мынадай мәліметтерді ескере отырып жүзеге асырады:
    - ақпараттық активті салу;
    - ақпараттық активтің физикалық орналасуы;
    - бағдарлама кодындағы белгілі қателер;
    - Баптау қателері
    - ақпараттық активті пайдалану үдерісіндегі кемшіліктер.
17. Аса маңызды ақпараттық активтерге қатысты ақпараттық қауіпсіздік тәуекелін басқарудың қолданыстағы шараларын айқындауды ақпараттық қауіпсіздік бөлімшесі аса маңызды ақпараттық активтердің ақпараттық қауіпсіздігін қамтамасыз ету процесінде бар кемшіліктерді немесе оны бұзудың салдарын жоюға бағытталған ұйымдастырушылық-техникалық іс-шаралар туралы ақпаратты ескере отырып жүзеге асырады.
18. Ақпараттық қауіпсіздік қатерлерінің көздерімен іске асырылатын ақпараттық активтерге ақпараттық қауіпсіздіктің қатерлерінің ықтималдығын бағалауды ақпараттық қауіпсіздік қауіпсіздігінің қатер көзінің, ақпараттық қауіпсіздік қатерінің және аса маңызды ақпараттық активке қатысы бар осалдықтың барлық үйлесімдері үшін ақпараттық қауіпсіздік бөлімі мынадай мәліметтерді ескере отырып жүргізеді:
    - ақпараттық қауіпсіздік қатері көзінің тиісті аса маңызды ақпараттық активтерге қатысты (ішкі немесе сыртқы) орналасқан жері туралы деректер. Ақпараттық қауіпсіздікке төнетін қауіп-қатердің ішкі көздері үшін активті пайдаланушылардың

саны, ақпараттық қауіпсіздік қатерлерінің сыртқы көздері үшін - қорғау периметрінен тыс жерлерден мүмкін болатын қол жеткізудің болуы ескеріледі;

- ақпараттық қауіпсіздік қатерінің көзіне қол жеткізу деңгейі туралы деректер;
- ақпараттық қауіпсіздіктің аса маңызды ақпараттық активтерге бұрынғы кездегі қауіптілігінің жиілігі туралы статистикалық деректер;
- аса маңызды ақпараттық активке ақпараттық қауіпсіздік қатерін іске асырудың күрделілігі туралы ақпарат;
- қарастырылып отырған аса маңызды ақпараттық активтерге қатысты қорғау шараларының болуы туралы деректер.

19. Ақпараттық қауіпсіздік қатерлерінің көздерімен іске асырылатын ақпараттық қауіпсіздік қатерлерінің ықтималдығын бағалауға бірнеше сарапшы қатысқан және әр түрлі баға алған кезде ең жоғары ықтималдықты анықтайтын бағалауға тең қорытынды, қорытылған баға алынады.
20. Ақпараттық қауіпсіздік тәуекелдерінің деңгейін бағалау ақпараттық қауіпсіздікке қатер төндіретін көздермен ақпараттық қауіпсіздік қатерінің туындау ықтималдығын бағалау және құпиялылықты, тұтастықты немесе аса маңызды ақпараттық активтің болуын бұзудан тиісті ықтимал шығындарды бағалау негізінде жүзеге асырылады.

4. Автоматтандырылған ақпараттық жүйеге қойылатын талаптар

21. Автоматтандырылған ақпараттық жүйе мыналарды қамтиды:
1) веб-қосымша серверлерінің бағдарламалық қамтамасыз етуі (бұдан әрі - веб-қосымша деп аталады);
2) бағдарламалық интерфейс серверлеріне арналған бағдарламалық қамтамасыз ету (осыдан серверлік бағдарламалық қамтамасыз ету деп аталады).
22. Автоматтандырылған ақпараттық жүйені әзірлеуді және (немесе) пысықтауды Компания әзірлеу және (немесе) жетілдіру тәртібін, даму кезеңдерін және олардың қатысушыларын реттейтін ішкі құжатқа сәйкес жүзеге асырады.
23. Компания әзірлеген автоматтандырылған ақпараттық жүйенің бастапқы кодтары резервтік көшірмесін жасай отырып, Компанияның қорғау периметрі шегінде орналасқан код қоймаларын басқарудың мамандандырылған жүйелерінде сақталуы тиіс.
24. Қауіпсіздік жөніндегі тестілеу міндетті кезең болып табылады, оның барысында кемінде мынадай іс-шаралар жүргізіледі:
1) бастапқы кодтың статикалық талдауы;
2) Компоненттер мен бөгде кітапханаларды талдау.
25. Автоматтандырылған ақпараттық жүйенің бастапқы кодын статикалық талдау функциялары мынадай осал тұстарды анықтауды қамтитын, бірақ олармен шектелмейтін, тексерілетін бағдарламалық қамтамасыз етуде пайдаланылатын барлық бағдарламалау тілдерін талдауды қолдайтын статикалық бастапқы кодты талдау сканерін пайдалана отырып жүргізіледі:
1) зиянды кодты инъекцияға мүмкіндік беретін тетіктердің болуы;
2) әлсіз операторлар мен бағдарламалау тілдерінің функцияларын пайдалану;
3) әлсіз және осал криптографиялық алгоритмдерді қолдану;
4) белгілі бір жағдайларда қызмет көрсетуден бас тартуды немесе өтініштің едәуір баяулауын туғызатын кодты пайдалану;
5) қосымшаны қорғау жүйелерін айналып өту тетіктерінің болуы;
6) кодтағы құпияларды ашық түрде пайдалану;
7) қолдану қауіпсіздігінің заңдылықтары мен практикаларын бұзу.
26. Автоматтандырылған ақпараттық жүйенің құрамдас бөліктерін және (немесе) бөгде кітапханаларын талдау пайдаланылатын компоненттің және (немесе) бөгде кітапхананың

нұсқасына тән белгілі осал тұстарды анықтау, сондай-ақ компоненттер мен (немесе) бөгде кітапханалар мен олардың нұсқалары арасындағы тәуелділікті қадағалау мақсатында жүргізіледі.

27. Компания анықталған осал тұстарды жою жөніндегі түзету іс-шараларын ішкі құжатта ұйғарылған тәртіппен жүзеге асыруды қамтамасыз етеді және автоматтандырылған ақпараттық жүйені және (немесе) оның жаңа нұсқаларын пайдалануға енгізгенге дейін аса маңызды осал тұстарды жоюға тиіс.

28. Компания соңғы 3 (үш) жыл ішінде пайдалануға енгізілген автоматтандырылған ақпараттық жүйенің бастапқы кодтарының барлық нұсқаларын және қауіпсіздікті тексеру нәтижелерін онлайн сақтауды және қол жеткізуді қамтамасыз етуге тиіс.

29. Автоматтандырылған ақпараттық жүйенің клиенттік және серверлік жақтары арасындағы деректер алмасу 1.2 және одан жоғары Transport Layer Security (Транспорт Лейер Секьюрити) шифрлау хаттамасының нұсқасын пайдалана отырып шифрлануы тиіс.

30. Веб-қосымшада:

1) Компанияның веб-қосымшасын бір мәнді сәйкестендіру (домен атауы, логотиптер, корпоративтік түстер);

2) браузер жадында авторизация деректерін сақтауға тыйым салу;

3) енгізілген секрецияларды бүркемелеу;

4) веб-қосымшаны пайдалану кезінде сақталуға ұсынылатын кибер гигиена шаралары туралы клиенттің авторизация бетінде хабардар ету;

5) қате туралы ең аз жеткілікті ақпаратты ұсына отырып, клиент интерфейсінде сезімтал деректерді көрсетуге мүмкіндік бермейтін қателер мен ерекшеліктерді қауіпсіз тәсілмен өңдеу.

31. Автоматтандырылған ақпараттық жүйедегі ақпаратқа қол жеткізу Компанияның қызметкерлеріне олардың функционалдық міндеттерін орындау үшін қажетті көлемде берілуі тиіс.

32. Автоматтандырылған ақпараттық жүйеге қол жеткізу Компания қызметкерлерінің сәйкестендірілуі мен түпнұсқалығын растау арқылы қамтамасыз етілуге тиіс.

33. Автоматтандырылған ақпараттық жүйеде шоттар мен парольдерді басқару, сондай-ақ Компанияның ішкі құжатында айқындалатын пайдаланушылардың шоттарын бұғаттау функциялары пайдаланады.

34. Автоматтандырылған ақпараттық жүйеге техникалық қолдау көрсетіледі, оған қауіпсіздікті жаңартуды қоса алғанда, автоматтандырылған ақпараттық жүйені жаңартуды қамтамасыз ету жөніндегі қызметтер кіреді.

35. Автоматтандырылған ақпараттық жүйе деректердің, файлдар мен параметрлердің резервтік сақталуын қамтамасыз етуге тиіс, бұл оның жұмыс істеу көшірмесін қалпына келтіруді қамтамасыз етуге тиіс.

36. Кәсіпорын автоматтандырылған ақпараттық жүйенің аудиторлық соқпағының ұйымдастырушылық және техникалық деңгейлерде ұсталуын және әрдайым жұмыс істеп тұрмауын қамтамасыз етуге тиіс.

37. Автоматтандырылған ақпараттық жүйені қорғау үшін вирусқа қарсы лицензияланған бағдарламалық қамтамасыз ету немесе жұмыс стансаларында, ноутбуктерде және жылжымалы құрылғыларда бағдарламалық ортаның тұтастығын немесе қайтарымдылығын бақылауды қамтамасыз ететін жүйелер қолданылады.

38. Компания микрокредит беру туралы шарт бойынша тараптардың міндеттемелері тоқтатылғаннан кейін кемінде 5 (бес) жыл ішінде клиентке берілген және одан алынған электрондық хабарламалар мен басқа да құжаттардың олардың тұтастығы мен құпиялылығын сақтай отырып, қауіпсіз сақталуын қамтамасыз етуге тиіс.

Электрондық хабарламалар мен басқа да құжаттар қалыптастырылған, клиентке жіберілген немесе одан алынған форматта сақталады.

5. Электрондық хабарламалар мен басқа да құжаттарды сақтау қауіпсіздігі

39. Компания ақпараттық қауіпсіздікті қамтамасыз ету мақсатында мынадай шарттарды орындайды:

- ақпараттық қауіпсіздікті басқару жүйесін ұйымдастыру туралы;
- ақпараттық активтерге қол жеткізуді ұйымдастыру туралы;
- ақпараттық инфрақұрылымның қауіпсіздігін қамтамасыз етуге;
- ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі іс-шараларды және қауіп-қатерлерді анықтау және талдау, шабуылдарға қарсы іс-қимыл жасау және ақпараттық қауіпсіздік инциденттерін тергеу жөніндегі іс-шараларды бақылау;
- ақпараттық қауіпсіздік инциденттері туралы ақпаратты, оның ішінде ақпараттық жүйелердегі бұзушылықтар, істен шығулар туралы ақпаратты талдау;
- ақпаратты криптографиялық қорғау құралдарымен;
- ақпараттық активтерге үшінші тұлғалар қол жеткізген жағдайда ақпараттық қауіпсіздікті қамтамасыз етуге;
- ақпараттық қауіпсіздіктің жай-күйіне ішкі аудит жүргізуге;
- ақпараттық қауіпсіздікті басқару жүйесінің процестері туралы.

40. Қорғауға жататын ақпарат:

- қағазға орналастыруға;
- электрондық түрде бар (компьютерлік техника құралдарымен өңделген, берілетін және сақталатын, техникалық құралдармен жазылған және қайта шығарылатын);
- телефон, телефакс, телекс, т.б. арқылы, электр сигналдары түрінде беріледі;
- кездесулер мен келіссөздер кезінде ауадағы акустикалық және діріл сигналдары түрінде және конструкцияларды қоршап тұру.

41. Жасалған келісімдер шеңберінде кредиттік бюродан (бұдан әрі – КБ деп аталатын) әлеуетті қарыз алушылар туралы ақпаратты (ресми кірістер, Мемлекеттік әлеуметтік сақтандыру қорынан берілетін трансферттер, республикалық бюджеттен зейнетақы төлемдерінің саны мен орташа мөлшері туралы, кредиттік есеп деректері және басқа есептер) беру туралы келісімдер бөлігінде Компания қызметін ұйымдастыру кезінде ақпараттық қауіпсіздікті қамтамасыз етуге қойылатын талаптар:

a. Компания КБ ақпараттық жүйесінен алынған ақпараттың құпиялылығын және тұтастығын қамтамасыз етеді.

b. Компания КБ-мен жасалған Келісімдердің шарттарына сәйкес ақпараттық қауіпсіздіктің тиісті деңгейін қамтамасыз етеді.

c. Компания КБ ақпараттық жүйесімен өзара іс-қимыл жасау және одан алынған ақпаратты өңдеу үшін пайдаланылатын жүйелік және қолданбалы бағдарламалық қамтамасыз етудің жұмыс істеуі мен қорғалуы үшін қажетті ұйымдастырушылық, техникалық, технологиялық талаптар мен іс-шаралардың орындалуын қамтамасыз етеді.

d. КБ ақпараттық жүйесімен жұмыс істеу үшін жабдықтарды пайдалану кезінде оны рұқсатсыз қол жеткізуден қорғау, сондай-ақ деректерді жеткізушілерді және КБ ақпараттық жүйесімен жұмыс істеу үшін пайдаланылатын желілік ресурстарды қорғау қажеттілігі ескеріледі.

e. Компания жауапты тұлғалардың тізбесін белгілеп, бекітеді.

f. Компания ұйымның жауапты тұлғалары (тұлғалары) қол қойған олардың функционалдық міндеттерін орындау барысында белгілі болған ақпаратты жария етпеу және таратпау жөніндегі міндеттемелерінің болуын қамтамасыз етеді.

g. Компания жауапты адамдардың тізбесін, олардың құқықтары мен міндеттерін (оның ішінде лауазымдық міндеттерді) айқындау және бекіту тәртібін айқындайтын ішкі құжаттардың болуын қамтамасыз етеді.

h. Ақпаратқа қол жеткізу Компания қызметкерлеріне олардың функционалдық міндеттерін орындау үшін қажетті көлемде беріледі.

i. КБ ақпараттық жүйесінде ол анықталған жауапты тұлғаның шоты нақты жеке тұлғаға (операторға) сәйкес келеді.

j. Компания жұмыс стансаларының (веб-сайттардың, мобильді қосымшалардың, веб-сайттың) Ақпараттық қауіпсіздік саясатына сәйкестігіне жоспарлы және жоспардан тыс тексерулер жүргізеді.

k. Уәкілетті органның талап етуі бойынша кәсіпорын КБ-мен жасалған шарттарда көзделген талаптарға өзінің сәйкестігін растайтын ақпарат беруге тиіс.

l. Жұмыс станциясының операциялық жүйесі пайдаланушыларды сәйкестендіру және аутентификациялау функцияларын, сондай-ақ берілген құқықтарға сәйкес пайдаланушылардың қол жеткізу және авторизация құқықтарын саралау функцияларын қамтамасыз етеді.

m. Кәсіпорын өзінің жұмыс станциясын пайдаланады.

n. Кредиттік бюроның ақпараттық жүйесіне қосу үшін жұмыс станциясын пайдалану кезінде басқа интернет-ресурстарға бір мезгілде қосылу жүргізілмейді.

o. Компанияның қызметкерлері ақпараттық жүйелерге қол жеткізу үшін пайдаланылатын жеке сәйкестендіру және аутентификация деректерінің құпиялылығын қамтамасыз етеді.

p. Компанияның қызметкерлері Кредиттік бюроның ақпараттық жүйесін пайдалану процесінде оларға белгілі болған ақпараттың құпиялылығын қамтамасыз етеді.

42. Компанияның ақпараттық қауіпсіздігін қамтамасыз ету жөніндегі жауапкершілік Компанияның барлық құрылымдық бөлімшелеріне өз өкілеттіктері шегінде және осы Саясатта белгіленген ережелерге және оның негізінде әзірленген құжаттарға сәйкес жүктелсін.

43. Осы Саясаттың және оның негізінде әзірленген құжаттардың талаптарын бұзғаны үшін жауапкершілік Компанияның ішкі нормативтік құжаттарына және Қазақстан Республикасының заңнамасына сәйкес қамтамасыз етіледі.

6. Ақпараттық қауіпсіздікті бұзудың алдын алу жөніндегі іс-шаралар

44. Киберқауіпсіздік инциденттерінің алдын алуда бағдарламалық қамтамасыз етуді әзірлеу, ақпараттық жүйелердің құрамдас бөліктерін және қаржы секторының инфрақұрылымын жобалау кезінде тиісті ұлттық және халықаралық талаптарды сақтау маңызды рөл атқарады. Компания киберқауіпсіздік тәуекелдерін тұрақты бағалайды, ол осы тәуекелдерді барынша азайту жөніндегі іс-шараларды әзірлеуге және іске асыруға, сондай-ақ іске асырылатын іс-шаралардың тиімділігін бағалауға негіз болады.

45. Алдын алу сатысында алынған нәтижелер, сондай-ақ өңделген инциденттердің тәжірибесі ескеріледі. Киберқауіпсіздік инциденттерінің сипаты, шамасы және әсері олардың әсерін жұмсарту мақсатында уақтылы бағаланады, ішкі және сыртқы мүдделі тараптар уақтылы хабардар етіледі, сондай-ақ бірлескен ден қою шаралары үйлестіріледі. Мүдделі тараптар мыналарды қамтиды:

- Қазақстан Республикасының Ұлттық Банкі;
- Компанияның қызметін реттейтін өзге де уәкілетті мемлекеттік және заң шығарушы органдар;
- - қарыз алушылар;
- кредиторлар мен инвесторлар;

- Компания қызметі барысында өзара іс-қимыл жасайтын құрылымдық бөлімшелердің қызметкерлері;
- қызмет көрсету провайдерлері.

46. Инциденттен кейін операцияларды жалғастыру қамтамасыз етуге, бұл ретте қалпына келтіру рәсімдері қолданылады, оның ішінде:

- болған оқиғаның салдарын жою;
- ақпараттық жүйелер мен деректердің қалыпты жай-күйін олардың қалыпты жай-күйін растап қалпына келтіру;
- болашақта осындай оқиғалардың алдын алу мақсатында болған оқиғаның бір бөлігі ретінде пайдаланылған осал тұстарды анықтау және жою;
- ел ішінде және елден тыс жерлерде тиісті ақпарат алмасуды қамтамасыз ету.

47. Пайдаланушылардың да, қызметкерлердің де хабардарлығы мен құзыретін арттыру (біліктілігін арттыру, оқыту) қауіп-қатерлерді жоюға және Компанияда ақпаратты қауіпсіз құру және пайдалану мәдениетін қалыптастыруға көмектеседі. Ақпараттандыруды арттыру кезеңі пайдаланушылардың нақты тәуекелдер мен оларды жұмсартудың тиімді әдістері туралы хабардар болуын қамтамасыз ету мақсатында алдын алу мен ден қоюдан алынған сабақтарға сүйенуге тиіс.

48. Ақпараттық қауіпсіздіктің классикалық моделі ақпараттың қауіпсіздігі үшін маңызды үш атрибутты: құпиялылықты, тұтастықты және қол жетімділікті қамтамасыз етуге негізделеді.

49. Ақпараттың құпиялылығы оның иесі анықтаған адамдардың қатаң шектеулі саны ғана онымен таныса алатынын білдіреді.

50. Егер рұқсат етілмеген адам ақпаратқа қол жеткізе алса, рұқсатсыз қолжетімділік немесе құпиялылықтың бұзылуы орын алады.

51. Қол жетімділік (қажетті ақпараттық қызметті ақылға қонымды мерзімде алу мүмкіндігі)

52. тұтастық (ақпараттың өзектілігі мен дәйектілігі, оны жоюдан және рұқсатсыз өзгертуден қорғау);

53. Микрокредит беру құпиясын құрайтын ақпаратқа рұқсатсыз қол жеткізу, оның санкцияланбаған өзгеруі, үшінші тұлғалардың санкцияланбаған іс-әрекеттері анықталған жағдайда Компания мұндай іс-әрекеттердің себептері мен салдарын жою жөнінде дереу шаралар қабылдауға, сондай-ақ бұл туралы уәкілетті органды бір жұмыс күні ішінде хабардар етуге тиіс.

54. Компания қылмыстық жолмен алынған кірістерді заңдастыру (жылыстату) және терроризмді қаржыландыру схемаларында микрокредиттерді электрондық құралдармен қамтамасыз етудің қолданыстағы немесе енгізілген әдістері мен технологияларын пайдаланудың алдын алу жөнінде шаралар қабылдайды. Әлеуетті қарыз алушының микрокредиттер беруі және кредиттік есеп жүргізуі кезінде Компания Қазақстан Республикасының 28 тамыздағы Заңында көзделген қажетті шараларды қолданады. 2009 жылы «Қылмыстан түскен кірістерді заңдастыруға (жылыстатуға) және терроризмді қаржыландыруға қарсы күрес туралы» (бұдан әрі – «КЖ/ТҚҚ заңы» деп аталатын), сондай-ақ Қазақстан Республикасының Ұлттық Банкі Басқармасының қаулысына өзгерістер мен толықтырулар енгізу туралы» Қазақстан Республикасының Ұлттық Банкі Басқармасының қаулысына сәйкес «Қаржы институттарының банктік және өзге де операциялардың жекелеген түрлеріне шектеулер енгізу туралы» Қазақстан Республикасы Банкінің 2013 жылғы 25 желтоқсандағы No 292 қаулысы.