Қорғау бейіндерін және Қорғау бейіндерін әзірлеу әдістемесін бекіту туралы

Қазақстан Республикасының Қорғаныс және аэроғарыш өнеркәсібі министрінің 2018 жылғы 27 маусымдағы № 105/НҚ бұйрығы. Қазақстан Республикасының Әділет министрлігінде 2018 жылғы 30 шілдеде № 17247 болып тіркелді

"Ақпараттандыру туралы" 2015 жылғы 24 қарашадағы Қазақстан Республикасының Заңы 7-1-бабының 18) тармақшасына сәйкес БҰЙЫРАМЫН:

1. Мыналар:

1) осы бұйрыққа 1-қосымшаға сәйкес Жұмыс станцияларына және серверлерге арналған вирусқа қарсы қорғау құралдарының, сондай-ақ желі деңгейіне басып кіруді айқындау жүйелерінің қорғау бейіндері;

2) осы бұйрыққа 2-қосымшаға сәйкес Қорғау бейіндерін әзірлеу әдістемесі бекітілсін.

2. Қазақстан Республикасы Қорғаныс және аэроғарыш өнеркәсібі министрлігінің Ақпараттық қауіпсіздік комитеті:

1) осы бұйрықтың Қазақстан Республикасы Әділет министрлігінде мемлекеттік тіркеуді;

2) осы бұйрық мемлекеттік тіркелген күнінен бастап күнтізбелік он күннің ішінде оның қағаз және электрондық түрдегі қазақ және орыс тілдеріндегі көшірмесін Қазақстан Республикасы Әділет министрлігінің "Республикалық құқықтық ақпарат орталығы" шаруашылық жүргізу құқығындағы республикалық мемлекеттік кәсіпорнына ресми жариялауға және Қазақстан Республикасы нормативтік құқықтық актілерінің эталондық бақылау банкіне енгізу үшін жіберуді ;

3) осы бұйрық мемлекеттік тіркелген күнінен бастап күнтізбелік он күннің ішінде оның көшірмесін мерзімді баспасөз басылымдарында ресми жариялауға жіберуді;

4) осы бұйрықты Қазақстан Республикасы Қорғаныс және аэроғарыш өнеркәсібі министрлігінің ресми интернет-ресурсында орналастыруды;

5) осы бұйрық Қазақстан Республикасы Әділет министрлігінде мемлекеттік тіркелгеннен кейін он жұмыс күні ішінде Қазақстан Республикасы Қорғаныс және аэроғарыш өнеркәсібі министрлігінің Заң департаментіне осы бұйрықтың 3-тармағының 1), 2), 3) және 4) тармақшаларында көзделген іс-шаралардың орындалуы туралы мәліметтер ұсынуды қамтамасыз етсін .

3. Осы бұйрықтың орындалуын бақылау жетекшілік ететін Қазақстан Республикасының Қорғаныс және аэроғарыш өнеркәсібі вице-министріне жүктелсін.

4. Осы бұйрық алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі.

Қазақстан Республикасы Қорғаныс және аэроғарыш	*Б. Атамқұлов*

өнеркәсібі министрі	

"КЕЛІСІЛДІ"

Қазақстан Республикасы

Ұлттық қауіпсіздік комитетінің төрағасы

_____ К. Мәсімов

"___" _____ 2018 жыл

	Қазақстан Республикасы Қорғаныс және аэроғарыш өнеркәсібі министрінің 2018 жылғы 27 маусымдағы № 105/НҚ бұйрығына 1-қосымша

Жұмыс станцияларына және серверлерге арналған вирусқа қарсы қорғау құралдарының, сондай-ақ желі деңгейіне басып кіруді айқындау жүйелерінің қорғау бейіндері

1-бөлім. Жұмыс станцияларына және серверлерге арналған вирусқа қарсы қорғау құралдарын қорғау бейіні

1-тарау. Жалпы ережелер

1. Осы Жұмыс станцияларына және серверлерге арналған вирусқа қарсы қорғау құралдарын қорғау бейіні "Ақпараттандыру туралы" 2015 жылғы 24 қарашадағы Қазақстан Республикасының Заңы (бұдан әрі – Заң) 7-1-бабының 18) тармақшасына сәйкес әзірленді.

2. Осы Қорғау бейінінде және серверлерге арналған вирусқа қарсы қорғау құралдарын қорғау бейінінде мынадай негізгі ұғымдар пайдаланылады:

1) ақпараттық-коммуникациялық инфрақұрылым объектілері (бұдан әрі – АКИО) – ақпараттық жүйелер, технологиялық платформалар, аппараттық-бағдарламалық кешендер, телекоммуникация желілері, сондай-ақ техникалық құралдардың үздіксіз жұмыс істеуін және ақпараттық қауіпсіздікті қамтамасыз ету жүйелері;

2) ақпараттың қауіпсіздік қатері – ақпараттың қауіпсіздігін бұзудың ықтимал немесе нақты төнген қаупін айқындайтын шарттар мен факторлардың жиынтығы;

3) бағалау объектісі (бұдан әрі – БО) – бағалауға жататын әкімшінің және пайдаланушының басшысымен АКИО-ның компоненттері;

4) БО қауіпсіздік саясаты (бұдан әрі – ОҚС) – ақпараттық ресурстарды, бақылаудағы БО басқаруды, қорғау мен бөлуді реттейтін қағидалар жиынтығы;

5) БО қауіпсіздік функциялары (бұдан әрі – ОҚФ) – ОҚС жүзеге асыруға бағытталған БО-ның барлық қауіпсіздік функцияларының жиынтығы;

6) вирусқа қарсы қорғау – ақпаратты және АКИО компоненттерін зиянды компьютерлік бағдарламалардан (вирустардан) қорғау (зиянды компьютерлік бағдарламаларды (вирустарды) айқындау, "зақымдалған" объектілерді бұғаттау, оқшаулау, "зақымдалған" объектілердегі зиянды компьютерлік бағдарламаларды жою);

7) вирусқа қарсы қорғау құралы (бұдан әрі – ВҚҚҚ) – компьютерлік ақпаратты рұқсатсыз жоюға, бұғаттауға, түрлендіруге, көшіруге немесе ақпаратты қорғау құралдарын бейтараптандыруға арналған компьютерлік бағдарламаларды немесе өзге компьютерлік ақпаратты айқындау, сондай-ақ осы бағдарламалар мен ақпаратты айқындауға әрекет ету функцияларын іске асыратын бағдарламалық құрал;

8) зиянды компьютерлік бағдарламалар (вирустар) белгілерінің дерекқоры (бұдан әрі – КВБ ДҚ) – ВҚҚҚ-ның зиянды компьютерлік бағдарламалар (вирустар) (сигнатуралар) туралы ақпаратты қамтитын, ВҚҚҚ зиянды компьютерлік бағдарламаларды (вирустарды) айқындау және оларды өңдеу үшін пайдаланатын қосалқы бөлігі;

9) қауіпсіздік әкімшісі – БО-ны орнатуға, әкімшілендіруге және пайдалануға пайдаланушы ;

10) қауіпсіздік жөніндегі тапсырма (бұдан әрі – ҚТ) – нақты БО-ны бағалаудың негізі ретінде пайдалануға арналған қауіпсіздік талаптары мен ерекшеліктердің жиынтығы;

11) қорғау бейіні (бұдан әрі – ҚБ) – ақпараттандыру объектілерінің компаненттері болып табылатын бағдармалық және техникалық құралдардың қауіпсіздігіне ең аз қойылатын талаптардың тізбесі;

12) сигнатура – зиянды компьютерлік бағдарламаның (вирустың) (бұдан әрі – КВ) оны айқындау үшін пайдаланылатын өзіндік белгілері.

3. ВҚҚҚ қарсы тұру үшін пайдаланылатын, негізгі қатерлер халықаралық ақпарат алмасу желілерін (жалпыға ортақ пайдаланылатын байланыс желілерін) және (немесе) алмалы машиналық ақпарат тасығыштарды қоса алғанда, ақпараттық-коммуникациялық желілерден АКИО-ға КВ енгізуге байланысты қатерлер болып табылады.

4. ВҚҚҚ-да мынадай қауіпсіздік функциялары іске асырылған:

1) ВҚҚҚ-ны басқаруға қолжетімділіктің аражігін ажырату;

2) ВҚҚҚ жұмысын басқару;

3) ВҚҚҚ параметрлерін басқару;

4) ВҚҚҚ-ның КВБ ДҚ жаңартуларды (өзектілендіруді) орнатуды басқару;

5) ВҚҚҚ қауіпсіздік аудиті;

6) әсер ету объектілерін тексерулерді орындау;

7) әсер ету объектілерін өңдеу;

8) ВҚҚҚ сигнализациясы.

5. ВҚҚҚ жұмыс істейтін ортада ортаның мынадай қауіпсіздік функциялары іске асырылған:

1) ВҚҚҚ мен пайдаланушылар арасында сенімді байланысты (маршрутты) қамтамасыз ету;

2) ВҚҚҚ-ның жаңартуларын алудың сенімді арнасын қамтамасыз ету;

3) қауіпсіз жұмыс істеу жағдайларын қамтамасыз ету;

4) қауіпсіздік атрибуттарын басқару.

6. ҚБ-да ВҚҚҚ-ға қойылатын қауіпсіздік талаптарының мынадай түрлері жазылды:

1) қауіпсіздіктің функционалдық талаптары(бұдан әрі – ҚФТ);

2) қауіпсіздікке қойылатын сенімділік талаптары.

7. ВҚҚҚ-ның ҚФТ:

1) КВ-ны айқындау мақсатында тексерулерді орындау режимдері мен әдістеріне қойылатын талаптарды;

2) зиянды компьютерлік бағдарламалар (вирустар) белгілері дерекқорын (КВБ ДҚ) жаңарту бойынша функционалдық мүмкіндіктерге қойылатын талаптарды;

3) ВҚҚҚ-ның қауіпсіздік функцияларын орындау (ВҚҚҚ жұмысын) режимдерін басқару жөніндегі талаптарды;

4) қауіпсіздік функциялары деректерін (ВҚҚҚ деректерін) басқару жөніндегі талаптарды;

5) басқару жөніндегі талаптарды;

6) ВҚҚҚ-ның жұмыс істеу аудитіне қойылатын талаптарды қамтиды.

8. ВҚҚҚ-ның қауіпсіздігіне қойылатын сенімділік талаптары мынадай негізгі мәселелерді қамтиды:

1) конфигурацияны басқару;

2) жеткізу және пайдалану;

3) әзірлеу;

4) басшылықтар;

5) өміршеңдік кезеңді қолдау;

6) тестілеу;

7) осалдықтарды бағалау;

8) ВҚҚҚ-ны жаңарту.

9. Осы ҚБ-ға сәйкес келетін ВҚҚҚ:

1) ақпарат тасығыштардың файлдық аумақтарында КВ-мен зақымдалған объектілерді айқындау мақсатында тексерулерді орындау мүмкіндігін;

2) КВ-мен зақымдалған объектілерді айқындау мақсатында команда бойынша тексерулерді орындау мүмкіндігін;

3) КВ-мен зақымдалған объектілерді айқындау мақсатында сигнатуралық әдістермен тексерулерді орындау мүмкіндігін;

4) автоматтандыру құралдарын пайдаланбай, КВБ ДҚ жаңартуларын алу және орнату мүмкіндігін;

5) аудит жүргізілетін оқиғалар үшін аудит жазбаларын өндіру мүмкіндігін;

6) аудит жазбаларындағы ақпаратты оқу мүмкіндігін;

7) аудит жазбаларын оқуға қолжетімділікті шектеуді;

8) аудиттің деректерін іздеуді, іріктеуді, реттеуді;

10. ВҚҚҚ есептеу желісінің базасында жұмыс істейтін АКИО жұмыс станциялары мен серверлеріне орнатылады.

11. ВҚҚҚ-ны АКИО-да пайдаланудың үлгілік кескіні осы ҚБ-ға 1-қосымшада беріледі.

2-тарау. Бағалау объектісінің қауіпсіздік ортасы

1-Параграф. Қауіпсіздік болжамдары

12. БО-ны алдын ала белгілеп пайдалануға қатысты болжамдар:

1) 1-болжам.

БО-ға өзінің функционалдық мүмкіндіктерін іске асыру үшін қажетті барлық АКИО-ларға (бақылаудағы АКИО-ларға) БО-ның қолжетімділігі қамтамасыз;

2) 2-болжам.

Пайдалану құжаттамасына сәйкес БО-ны орнату, конфигурациялау мен басқару қамтамасыз;

3) 3-болжам.

АКИО-ның бақылаудағы ресурстарымен БО-ның үйлесімділігі қамтамасыз;

4) 4-болжам.

Ақпараттық жүйеде бірге пайдаланылған жағдайда ВҚҚҚ-ның басқа өндірушілердің ВҚҚҚ-мен бірлесіп дұрыс жұмыс істеу;

5) 5-болжам.

БО орнатылған АКИО элементтерінің физикалық қорғалуы;

6) 6-болжам.

БО компоненттері арасында, сондай-ақ БО мен оның жұмыс істеу ортасы арасында уақыт бойынша синхрондау;

7) 7-болжам.

БО-ның жұмыс істеуіне жауапты персонал пайдалану құжаттамасын басшылыққа ала отырып, БО-ның тиісінше жұмыс істеуін қамтамасыз.

2-Параграф. Қатерлер

13. БО қарсы тұруы қатерлер:

1) 1-қатер;

қатердің сипаттау - халықаралық ақпарат алмасу желілерін (жалпыға ортақ пайдаланылатын байланыс желілерін) қоса алғанда, сыртқы ақпараттық-телекоммуникациялық желілермен ақпараттық өзара іс-қимылды жүзеге асырған кезде АКИО-ның автоматтандырылған жұмыс орындарына КВ енгізу;

қатер көзі – ішкі бұзушы, сыртқы бұзушы;

қатерді іске асыру тәсілі – КВ-ны ақпарат алмасуды жүзеге асырған кезде АКИО-ға енгізу ;

пайдаланылатын осалдықтар – АКИО-да қолданылатын ақпаратты қорғау құралдары кешенінің толық еместігі;

әлеуетті қатерге ұшырағыш ақпараттық ресурстардың түрі – БО орнатылған АКИО ақпараттық ресурстары;

ақпараттық ресурстардың бұзылатын қауіпсіздік ерекшеліктері – құпиялылық, тұтастық, қолжетімділік;

қатерді іске асырудың ықтимал салдарлары – АКИО есептеу желісінің бағдарламалық-техникалық құралдарын компьютерлік вирустармен зақымдау, құпия ақпараттың таралуы, АКИО-ның жұмыс істеу режимдерін бұзу;

2) 2-қатер;

қатердің сипаттау - алмалы машиналық ақпарат тасығыштардан АКИО-ның автоматтандырылған жұмыс орындарына КВ енгізу;

қатер көзі – ішкі бұзушы;

қатерді іске асыру тәсілі – пайдаланушылардың алмалы машиналық ақпарат тасығыштардан АКИО объектілеріне КВ енгізуі;

пайдаланылатын осалдықтар – АКИО-да қолданылатын ақпаратты қорғау құралдары кешенінің толық еместігі;

әлеуетті қатерге ұшырағыш ақпараттық ресурстардың түрі - БО орнатылған АКИО ақпараттық ресурстары;

ақпараттық ресурстардың бұзылатын қауіпсіздік ерекшеліктері – құпиялылық, тұтастық, қолжетімділік;

қатерді іске асырудың ықтимал салдарлары – АКИО есептеу желісінің бағдарламалық-техникалық құралдарын компьютерлік вирустармен зақымдау, құпия ақпараттың таралуы, АКИО-ның жұмыс істеу режимдерін бұзу.

14. Орта қарсы тұруы қатерлер:

1) 1-орта қатері:

Қатердің сипаттау - бұзушылардың вирусқа қарсы қорғау құралдарын ажыратуы немесе бұғаттауы;

қатер көзі – ішкі бұзушы, сыртқы бұзушы;

қатерді іске асыру тәсілі – штаттық және штаттық емес құралдарды пайдалана отырып, ВҚҚҚ-ға рұқсатсыз қол жеткізу;

пайдаланылатын осалдықтар – АКИО-да өкілеттіктердің аражігін ажырату рәсімдерінің жеткіліксіздігі, ВҚҚҚ-мен өзара іс-қимыл жасайтын және ВҚҚҚ-ның жұмыс істеуіне әсер етуі мүмкін АКИО техникалық, бағдарламалық және бағдарламалық-техникалық құралдарының осалдықтары , АКИО-дағы қолжетімділікті басқару, сеанстарды қорғау, жабдықты физикалық қорғау механизмдерінің жеткіліксіздігі;

әлеуетті қатерге ұшырағыш ақпараттық ресурстардың түрі – ОҚФ деректері;

ақпараттық ресурстардың бұзылатын қауіпсіздік ерекшеліктері –тұтастық, қолжетімділік;

қатерді іске асырудың ықтимал салдарлары – ВҚҚҚ жұмысының тиімсіздігі;

2) 2-орта қатері:

қатердің сипаттау - ВҚҚҚ конфигурациясын рұқсатсыз өзгерту;

қатер көзі – ішкі бұзушы, сыртқы бұзушы;

қатерді іске асыру тәсілі – ВҚҚҚ-ның конфигурациялық ақпаратына (баптауларына) рұқсатсыз қол жеткізу;

пайдаланылатын осалдық – АКИО-да өкілеттіктердің аражігін ажырату рәсімдерінің жеткіліксіздігі, ВҚҚҚ-мен өзара іс-қимыл жасайтын және ВҚҚҚ-ның жұмыс істеуіне әсер етуі мүмкін АКИО техникалық, бағдарламалық және бағдарламалық-техникалық құралдарының осалдықтары , АКИО-да қолжетімділікті басқару, сеанстарды қорғау, жабдықты физикалық қорғау механизмдерінің жеткіліксіздігі;

әлеуетті қатерге ұшырағыш ақпараттық ресурстардың түрі – ВҚҚҚ бағдарламалық қамтылымының баптаулары;

ақпараттық ресурстардың бұзылатын қауіпсіздік ерекшеліктері –тұтастық;

қатерді іске асырудың ықтимал салдарлары – ВҚҚҚ-ның жұмыс істеу режимдерін бұзу, АКИО-ға КВ-ның енгізілуін айқындамау;

3) 3-орта қатері:

қатердің сипаттау - КВБ ДҚ-ны жаңарту механизмі арқылы ВҚҚҚ-ның жұмыс істеу логикасына рұқсатсыз өзгерістер енгізу;

қатер көзі – ішкі бұзушы, сыртқы бұзушы;

қатерді іске асыру тәсілі – АКИО ұсынатын штаттық емес құралдарды, сондай-ақ мамандандырылған аспаптық құралдарды пайдалана отырып, рұқсат етілмеген іс-қимылдарды жүзеге асыру;

пайдаланылатын осалдық – КВБ ДҚ жаңартуларын алудың сенімді арнасын қамтамасыз ету механизмдерінің жеткіліксіздігі;

әлеуетті қатерге ұшырағыш ақпараттық ресурстардың түрі – ВҚҚҚ бағдарламалық қамтылымы мен КВ белгілерінің дерекқоры;

ақпараттық ресурстардың бұзылатын қауіпсіздік ерекшеліктері –тұтастық, қолжетімділік;

қатерді іске асырудың ықтимал салдарлары – ВҚҚҚ-ның жұмыс істеу режимдерін бұзу, АКИО-ға КВ-ның енгізілуін айқындамау. ВҚҚҚ төменде берілген ұйымның қауіпсіздік саясаты қағидаларын басшылыққа алуы.

3-Параграф. Ұйымның қауіпсіздік саясаты

15. ВҚҚҚ ұйымның қауіпсіздік саясаты басшылыққа алуы жұмыс істейді:

1) 1-қауіпсіздік саясаты.

Тіркеу механизмдері осындай уәкілеттік берілген АКИО субъектілеріне орын алған оқиғалар туралы ақпаратпен ішінара танысуға мүмкіндік беруге тиіс;

2) 2-қауіпсіздік саясаты.

ВҚҚҚ-ның қауіпсіздік функцияларын орындауына әсер ететін ВҚҚҚ параметрлерін басқаруды АКИО-ның уәкілетті субъектілері ғана жүзеге асыру керек;

3) 3- қауіпсіздік саясаты.

АКИО-ның уәкілетті субъектілері тарапынан ВҚҚҚ-ның қауіпсіздік функцияларын орындау режимдерін басқару жүзеге асырылуы тиіс;

4) 4-қауіпсіздік саясаты.

ВҚҚҚ рұқсатсыз қол жеткізуден және ВҚҚҚ-ның функциялары мен деректеріне қатысты бұзулардан қорғалған тиіс;

5) 5-қауіпсіздік саясаты.

ВҚҚҚ белгіленген жады аумақтары мен файлдардағы КВ-мен зақымдалған объектілерді айқындау мақсатында тексерулер орындауды қамтамасыз тиіс;

6) 6-қауіпсіздік саясаты.

КВ-мен зақымдалған объектілерді айқындау мақсатында ВҚҚҚ тексерулерді орындау режимдерін орнату мүмкіндігін қамтамасыз тиіс;

7) 7-қауіпсіздік саясаты.

ВҚҚҚ зақымдалған объектілерден КВ кодын жою (егер техникалық тұрғыдан жою мүмкін болса) мүмкіндігін қамтамасыз тиіс;

8) 8-қауіпсіздік саясаты.

ВҚҚҚ КВБ ДҚ жаңартуларын орындау режимдерін орнату мүмкіндігін ВҚҚҚ қамтамасыздандырады.

3-тарау. Қауіпсіздік мақсаттары

1-Параграф. Бағалау объектісіне арналған қауіпсіздік мақсаттары

16. БО-ға арналған қауіпсіздік мақсаттарының сипаттамасы беріледі:

1) 1-қауіпсіздік мақсаты. ВҚҚҚ қауіпсіздік аудиті.

ВҚҚҚ-ның қауіпсіздікті ықтимал бұзуларға жататын кез келген оқиғаларды тіркеу мен болдырмаудың тиісті механизмдері. Тіркеу механизмдері уәкілетті АКИО субъектілеріне орын алған оқиғалар туралы ақпаратпен ішінара танысуға мүмкіндік беруге тиіс;

2) 2-қауіпсіздік мақсаты. ВҚҚҚ параметрлерін басқару.

ВҚҚҚ-ның қауіпсіздік функцияларын орындауына әсер ететін ВҚҚҚ параметрлерін уәкілетті АКИО субъектілері тарапынан басқару мүмкіндігін ВҚҚҚ қамтамасыз ету;

3) 3-қауіпсіздік мақсаты. ВҚҚҚ жұмысын басқару.

Уәкілетті АКИО субъектілері тарапынан ВҚҚҚ-ның қауіпсіздік функцияларын орындау режимдерін басқаруды ВҚҚҚ қамтамасыз етуі;

4) 4-қауіпсіздік мақсаты. ВҚҚҚ басқаруға қолжетімділіктің аражігін ажырату.

АКИО субъектілерінің ВҚҚҚ басқаруға қолжетімділіктің аражігін ажыратуды ВҚҚҚ қамтамасыз етуі;

5) 5-қауіпсіздік мақсаты. Объектілерді тексерулерді орындау.

КВ-мен зақымдалған объектілерді айқындау мақсатында ВҚҚҚ тексерулерді орындауды қамтамасыз етуі;

6) 6-қауіпсіздік мақсаты. Тексерулерді орындау режимдері.

КВ-мен зақымдалған объектілерді айқындау мақсатында ВҚҚҚ тексерулерді орындау режимдерін орнату мүмкіндігін қамтамасыз етуі;

7) 7-қауіпсіздік мақсаты. Зақымдалған объектілерді өңдеу.

ВҚҚҚ зақымдалған объектілерден КВ кодын жою (егер техникалық тұрғыдан жою мүмкін болса) мүмкіндігін қамтамасыз етуі;

8) 8-қауіпсіздік мақсаты. Дерекқорын жаңарту.

ВҚҚҚ КВБ ДҚ жаңартуларын орындау режимдерін орнату мүмкіндігін ВҚҚҚ қамтамасыз етуі.

2-Параграф. Бағалау объектісінің ортасына арналған қауіпсіздік мақсаттары

17. Осы бөлімде БО-ның жұмыс істеу ортасына арналған қауіпсіздік мақсаттарының сипаттамасы беріледі:

1) БО-ның жұмыс істеу ортасына арналған 1-мақсат. АКИО деректеріне қол жеткізу.

БО өзінің функционалдық міндеттерін іске асыру үшін қажетті АКИО деректеріне ВҚҚҚ-ның қолжетімділігі қамтамасыз ету;

2) БО-ның жұмыс істеу ортасына арналған 2-мақсат. БО-ны пайдалану.

Пайдалану құжаттамасына сәйкес ВҚҚҚ-ны орнату, конфигурациялау мен басқару қамтамасыз ету;

3) БО-ның жұмыс істеу ортасына арналған 3-мақсат. Үйлесімділік.

ВҚҚҚ-ның бақылаудағы АКИО объектілерімен үйлесімділігі қамтамасыз ету;

4) БО-ның жұмыс істеу ортасына арналған 4-мақсат. Бірлескен жұмыс.

АКИО-да бірге пайдаланылған жағдайда ВҚҚҚ-ның басқа өндірушілердің ВҚҚҚ-мен бірлесіп дұрыс жұмыс істеу мүмкіндігі қамтамасыз ету;

5) БО-ның жұмыс істеу ортасына арналған 5-мақсат. БО бөліктерін физикалық қорғау.

ВҚҚҚ орнатылған бағдарламалық-техникалық құралдардың физикалық қорғалуы қамтамасыз етілуі;

6) БО-ның жұмыс істеу ортасына арналған 6-мақсат. Уақытты синхрондау.

ВҚҚҚ компоненттері арасында, сондай-ақ ВҚҚҚ мен олардың жұмыс істеу ортасы арасында тиісті уақыт белгілерінің көзі және уақыт бойынша синхрондау қамтамасыз етілуі;

7) БО-ның жұмыс істеу ортасына арналған 7-мақсат. Персоналға қойылатын талаптар.

ВҚҚҚ-ның жұмыс істеуіне жауапты персонал пайдалану құжаттамасын басшылыққа ала отырып, ВҚҚҚ-ның тиісінше жұмыс істеуін қамтамасыз етуі тиіс;

8) БО-ның жұмыс істеу ортасына арналған 8-мақсат. Сенімді байланыс.

ВҚҚҚ мен уәкілетті АКИО субъектілері (қауіпсіздік әкімшілері) арасында сенімді байланыс қамтамасыз етілуі;

9) БО-ның жұмыс істеу ортасына арналған 9-мақсат. Аутентификация және сәйкестендіру механизмдері.

ВҚҚҚ-ның жұмыс істеуі ВҚҚҚ қауіпсіздік әкімшілерінің аутентификациясы мен сәйкестендіру механизмдерін ұсынатын жұмыс істеу ортасында жүзеге асырылуы тиіс;

10) БО-ның жұмыс істеу ортасына арналған 10-мақсат. Сенімді арна.

ВҚҚҚ КВБ ДҚ жаңартуларын алудың сенімді арнасы қамтамасыз етілуі;

11) БО-ның жұмыс істеу ортасына арналған 11-мақсат ОҚФ деректерін қорғау.

ВҚҚҚ қауіпсіздік функцияларын орындаудың қорғалған аясы қамтамасыз етілуі;

12) БО-ның жұмыс істеу ортасына арналған 12-мақсат. Қауіпсіздік атрибуттарын басқару.

ВҚҚҚ функциялары мен деректеріне қол жеткізуге байланысты қауіпсіздік атрибуттарын басқару ВҚҚҚ және АКИО әкімшілерін ғана берілуі тиіс.

4-тарау. Негіздеме

1-Параграф. Бағалау объектісінің қауіпсіздік мақсаттарының негіздемесі

18. Қауіпсіздік мақсаты:

1) 1-қауіпсіздік мақсаты.

Бұл қауіпсіздік мақсатына қол жеткізу 1-қатер, 2-қатер қатерлеріне қарсы тұру мен ұйымның 1-қауіпсіздік саясаты қауіпсіздік саясатын іске асыру үшін қажет, себебі қауіпсіздікті ықтимал бұзуларға жататын кез келген оқиғалардың тиісінше тіркелуін және олар

туралы ескертуді, орын алған оқиғалар туралы ақпаратпен іріктеп таныстыру мүмкіндігін қамтамасыз етеді;

2) 2-қауіпсіздік мақсаты.

Бұл қауіпсіздік мақсатына қол жеткізу 1-қатер, 2-қатер қатерлеріне қарсы тұру мен ұйымның 2-қауіпсіздік саясаты қауіпсіздік саясатын іске асыру үшін қажет, себебі ВҚҚҚ қауіпсіздік функцияларын орындауға әсер ететін ВҚҚҚ-ның параметрлерін уәкілетті АКИО субъектілері тарапынан басқару мүмкіндігін қамтамасыз етеді;

3) 3-қауіпсіздік мақсаты.

Бұл қауіпсіздік мақсатына қол жеткізу 1-қатер, 2-қатер қатерлеріне қарсы тұру мен ұйымның 3-қауіпсіздік саясаты қауіпсіздік саясатын іске асыру үшін қажет, себебі ВҚҚҚ қауіпсіздік функцияларын орындау режимдерін уәкілетті АКИО субъектілері тарапынан басқару мүмкіндігін қамтамасыз етеді;

4) 4-қауіпсіздік мақсаты.

Бұл қауіпсіздік мақсатына қол жеткізу 2-қатер қатеріне қарсы тұру мен ұйымның 4-қауіпсіздік саясаты қауіпсіздік саясатын іске асыру үшін қажет, себебі ВҚҚҚ-ны басқаруға қолжетімділікті бөлуді уәкілетті АКИО субъектілерінің негізінде қамтамасыз етеді;

5) 5-қауіпсіздік мақсаты.

Бұл қауіпсіздік мақсатына қол жеткізу ұйымның 5-қауіпсіздік саясаты қауіпсіздік саясатын іске асыру үшін қажет, себебі жадының белгіленген аумағы мен файлдарда КВ-мен зақымдалған объектілерді айқындау мақсатында тексерулер орындауды қамтамасыз етеді;

6) 6-қауіпсіздік мақсаты.

Бұл қауіпсіздік мақсатына қол жеткізу ұйымның 6-қауіпсіздік саясаты қауіпсіздік саясатын іске асыру үшін қажет, себебі КВ-мен зақымдалған объектілерді айқындау мақсатында тексерулерді орындау режимдерін белгілеу мүмкіндігін қамтамасыз етеді;

7) 7-қауіпсіздік мақсаты.

Бұл қауіпсіздік мақсатына қол жеткізу ұйымның 7-қауіпсіздік саясаты қауіпсіздік саясатын іске асыру үшін қажет, себебі зақымдалған объектілерден КВ кодын жою (егер техникалық тұрғыдан жою мүмкін болса) мүмкіндігін қамтамасыз етеді;

8) 8-қауіпсіздік мақсаты.

Бұл қауіпсіздік мақсатына қол жеткізу ұйымның 8-қауіпсіздік саясаты қауіпсіздік саясатын іске асыру үшін қажет, себебі ВҚҚҚ КВБ ДҚ жаңартуларын орындау режимдерін орнату мүмкіндігін қамтамасыз етеді.

19. Осы ҚБ-ға 2-қосымшада БО-ға арналған ұйымның мақсаттарының қаупсіздік саясаты мен қатерлерге әсері беріледі.

2-Параграф. Бағалау объектісі ортасына арналған қауіпсіздік мақсаттарының негіздемесі

20. Осы ҚБ-ға 3-қосымшада ортаға арналған қауіпсіздік мақсаттарының қауіпсіздік болжамдарына, қауіпсіздік саясаты мен қатерлерге әсері беріледі:

1) БО-ның жұмыс істеу ортасына арналған 1-мақсат.

Бұл қауіпсіздік мақсатына қол жеткізу 1-болжам қауіпсіздік болжамын іске асыру үшін қажет, себебі ВҚҚҚ-ға өзінің функцияларын іске асыру үшін қажетті АКИО-ның барлық деректеріне ВҚҚҚ-ның қолжетімділігі қамтамасыз ету;

2) БО-ның жұмыс істеу ортасына арналған 2-мақсат.

Бұл қауіпсіздік мақсатына қол жеткізу 2-болжам қауіпсіздік болжамын іске асыру үшін қажет, себебі ВҚҚҚ-ны пайдалану құжаттамасына сәйкес орнату, конфигурациялау және басқару қамтамасыз ету;

3) БО-ның жұмыс істеу ортасына арналған 3-мақсат.

Бұл қауіпсіздік мақсатына қол жеткізу 3-болжам қауіпсіздік болжамын іске асыру үшін қажет, себебі АКИО-ның бақылаудағы ақпараттық ресурстарымен ВҚҚҚ-ның үйлесімділігін қамтамасыз ету;

4) БО-ның жұмыс істеу ортасына арналған 4-мақсат.

Бұл қауіпсіздік мақсатына қол жеткізу 4-болжам қауіпсіздік болжамын іске асыру үшін қажет, себебі ақпараттық жүйеде бірге пайдаланылған жағдайда ВҚҚҚ-ның басқа өндірушілердің ВҚҚҚ-мен бірлесіп дұрыс жұмыс істеу мүмкіндігі қамтамасыз ету;

5) БО-ның жұмыс істеу ортасына арналған 5-мақсат.

Бұл қауіпсіздік мақсатына қол жеткізу 1-орта қатері ортасына төнетін қауіпсіздік қатеріне қарсы тұру мен 5-болжам қауіпсіздік болжамын іске асыру үшін қажет, себебі ВҚҚҚ орнатылған АКИО элементтерін физикалық қорғау қамтамасыз ету;

6) БО-ның жұмыс істеу ортасына арналған 6-мақсат.

Бұл қауіпсіздік мақсатына қол жеткізу 6-болжам қауіпсіздік саясатын іске асыру үшін қажет, себебі ВҚҚҚ компоненттері арасында, сондай-ақ ВҚҚҚ мен оның жұмыс істеу ортасы арасында уақыт бойынша синхрондау қамтамасыз етіледі;

7) БО-ның жұмыс істеу ортасына арналған 7-мақсат.

Бұл қауіпсіздік мақсатына қол жеткізу 7-болжам қауіпсіздік болжамын іске асыру үшін қажет, себебі ВҚҚҚ-ның жұмыс істеуіне жауапты персонал пайдалану құжаттамасын басшылыққа ала отырып, ВҚҚҚ-ның тиісінше жұмыс істеуін қамтамасыз етеді;

8) БО-ның жұмыс істеу ортасына арналған 8-мақсат.

Бұл қауіпсіздік мақсатына қол жеткізу 2-орта қатері ортасына төнетін қауіпсіздік қатеріне қарсы тұру үшін қажет, себебі ВҚҚҚ мен уәкілетті АКИО субъектілері қауіпсіздік әкімшілері арасында сенімді байланысты қамтамасыз етеді;

9) БО-ның жұмыс істеу ортасына арналған 9-мақсат.

Бұл қауіпсіздік мақсатына қол жеткізу 1-орта қатері мен 2-орта қатері ортасына төнетін қауіпсіздік қатерлеріне қарсы тұру үшін қажет, себебі ВҚҚҚ-ның жұмыс істеуін ВҚҚҚ қауіпсіздік әкімшілерінің аутентификациясы мен сәйкестендіру механизмдерін ұсынатын жұмыс істеу ортасында қамтамасыз етеді;

10) БО-ның жұмыс істеу ортасына арналған 10-мақсат.

Бұл қауіпсіздік мақсатына қол жеткізу 3-орта қатері ортасына төнетін қауіпсіздік қатеріне қарсы тұру үшін қажет, себебі ВҚҚҚ КВБ ДҚ жаңартуларын алудың сенімді арнасы қамтамасыз етіледі;

11) БО-ның жұмыс істеу ортасына арналған 11-мақсат.

Бұл қауіпсіздік мақсатына қол жеткізу 1-орта қатері мен 2-орта қатері ортасына төнетін қауіпсіздік қатерлеріне қарсы тұру үшін қажет, себебі ВҚҚҚ-ның қауіпсіздік функцияларын орындаудың қорғалған аясы қамтамасыз етіледі;

12) БО-ның жұмыс істеу ортасына арналған 12-мақсат.

Бұл қауіпсіздік мақсатына қол жеткізу 1-орта қатері мен 2-орта қатері ортасына төнетін қауіпсіздік қатерлеріне қарсы тұру үшін қажет, себебі БО-ның функциялары мен деректеріне қол жеткізуге байланысты қауіпсіздік атрибуттарын басқару мүмкіндігін уәкілетті ВҚҚҚ және АКИО әкімшілеріне ғана беру қамтамасыз етіледі.

2-бөлім. Желі деңгейіне басып кіруді айқындау жүйелерін қорғау бейіні

1-тарау. Жалпы ережелер

1. Осы Желі деңгейіне басып кіруді айқындау жүйелерін қорғау бейіні "Ақпараттандыру туралы" 2015 жылғы 24 қарашадағы Қазақстан Республикасының Заңы 7-1-бабының 18) тармақшасына сәйкес әзірленді.

2. Осы Желі деңгейіне басып кіруді айқындау жүйелерін қорғау бейінінде мынадай негізгі ұғымдар пайдаланылады:

1) ақпараттық-коммуникациялық инфрақұрылым объектілері (бұдан әрі – АКИО) – ақпараттық жүйелер, технологиялық платформалар, аппараттық-бағдарламалық кешендер, телекоммуникация желілері, сондай-ақ техникалық құралдардың үздіксіз жұмыс істеуін және ақпараттық қауіпсіздікті қамтамасыз ету жүйелері;

2) ақпараттың қауіпсіздік қатері – ақпараттың қауіпсіздігін бұзудың ықтимал немесе нақты төнген қатерін айқындайтын шарттар мен факторлардың жиынтығы;

3) басып кірулерді айқындау жүйесі (бұдан әрі – БАЖ) – ақпаратқа оны алу, жою, бұрмалау және оған қолжетімділікті бұғаттау мақсатында қасақана қол жеткізуге, ақпаратқа (ақпарат тасығыштарға) арнайы әсер етуге бағытталған ақпараттық жүйедегі іс-қимылдарды автоматты айқындау (бұғаттау) функцияларын іске асыратын бағдарламалық немесе бағдарламалық-техникалық құрал;

4) БАЖ әкімшісі – БО-ны орнатуға, әкімшілендіруге және пайдалануға пайдаланушы;

5) БАЖ талдағышы – ақпаратты БАЖ сенсорларынан (датчиктерінен) жинауға, оның бақылаудағы АКИО-ға басып кірулерді (шабуылдарды) айқындау тұрғысынан қорытынды талдауын жинауға арналған БАЖ–дың бағдарламалық немесе бағдарламалық-техникалық компоненті;

6) БАЖ деректері – өзінің функцияларын орындау нәтижесінде БАЖ жинаған немесе құрған деректер;

7) БАЖ датчигі (сенсоры) – бақылаудағы АКИО-дағы оқиғалар туралы ақпаратты (деректерді) жинауға және бастапқы талдауды жүргізуге, сондай-ақ – осы ақпаратты (деректерді) БАЖ талдағышына жіберуге арналған БАЖ–дың бағдарламалық немесе бағдарламалық-техникалық компоненті;

8) басып кіру (шабуыл) – мақсаты ақпараттық ресурстарға рұқсатсыз қол жеткізуді жүзеге асыру болып табылатын іс-қимыл;

9) бағалау объектісі - пайдалану жөніндегі басшылығы қоса берілген сертификаттауға (бағалауға) жататын желі деңгейінің БАЖ;

10) БО қауіпсіздік саясаты – ақпараттық ресурстарды, бақылаудағы БО басқаруды, қорғау мен бөлуді реттейтін қағидалар жиынтығы;

11) қорғау бейіні (бұдан әрі – ҚБ) – ақпараттандыру объектілерінің компаненттері болып табылатын бағдармалық және техникалық құралдардың қауіпсіздігіне ең аз қойылатын талаптардың тізбесі;

12) БО қауіпсіздік функциялары – бағалау объектісінің қауіпсіздік саясатын (бұдан әрі – ОҚС) жүзеге асыруға бағытталған БО-ның барлық қауіпсіздік функцияларының жиынтығы;

13) сигнатура – басып кірудің (шабуылдың) оны айқындау үшін пайдаланылатын сипаттық белгілері;

14) қауіпсіздік жөніндегі тапсырма – нақты БО-ны бағалаудың негізі ретінде пайдалануға арналған қауіпсіздік талаптары мен ерекшеліктердің жиынтығы;

15) шешуші қағидалар базасы (бұдан әрі – ШҚБ) - БАЖ оның негізінде басып кірулердің (шабуылдың) орын алуы туралы шешім қабылдайтын басып кірулер (сигнатуралар) туралы ақпаратты қамтитын БАЖ - дың құрамдас бөлігі.

3. БАЖ есептеу желілерінің базасында жұмыс істейтін ақпараттық жүйелердің ақпаратын қорғау жүйесінің элементін білдіреді және ақпараттық жүйелердегі ақпаратқа рұқсатсыз қол жеткізуден ақпаратты қорғаудың басқа құралдарымен бірге пайдаланылады.

4. БАЖ басып кірулерге (шабуылдарға) жататын мынадай негізгі ақпараттың қауіпсіздік қатерлерін айқындауды және (немесе) бұғаттауды қамтамасыз етуі тиіс:

1) халықаралық ақпарат алмасу желілерін қоса алғанда, ақпараттық-телекоммуникациялық желілерден іс-қимыл жасайтын сыртқы бұзушылардың тарапынан ақпаратқа (ақпарат тасығыштарға) рұқсатсыз қасақана қол жеткізу немесе арнайы әсер ету;

2) ақпараттық жүйедегі ақпаратқа қол жеткізуге құқығы мен өкілеттігі бар ішкі бұзушылардың тарапынан ақпаратқа (ақпарат тасығыштарға) рұқсатсыз қасақана қол жеткізу немесе арнайы әсер ету.

5. БАЖ-дың негізгі компоненттері датчиктер (сенсорлар) мен талдағыштар болып табылады.

6. Датчиктер (сенсорлар) осы датчиктер орнатылған АКИО шегінде жіберілетін деректердің топтамалары туралы ақпарат жинайды. Желі деңгейінің БАЖ датчиктері стандартты бағдарламалық-техникалық платформаларға орнатылатын бағдарламалық қамтылым (БҚ) түрінде, сондай-ақ АКИО-ға қосылатын бағдарламалық-техникалық құрылғылар түрінде іске асырылуы мүмкін . Талдағыштар датчиктер жинаған ақпаратты талдауды орындайды, талдау нәтижелері бойынша есептерді өндіреді және айқындалған басып кірулерге әрекет ету процестерін басқарады.

7. БАЖ басып кірудің айқындалуы туралы шешімді БАЖ шешуші қағидалар базасын пайдалана отырып, БАЖ датчиктері жинайтын ақпаратты талдау нәтижелеріне сәйкес қабылдайды.

8. БАЖ-да мынадай қауіпсіздік функциялары іске асырылған:

1) БАЖ-ды басқаруға қолжетімділіктің аражігін ажырату;

2) БАЖ жұмысын басқару;

3) БАЖ параметрлерін басқару;

4) БАЖ-дың шешуші қағидалар базасын жаңартуларды (өзектілендіруді) орнатуды басқару;

5) БАЖ деректерін талдау;

6) БАЖ қауіпсіздік аудиті;

7) бақылаудағы ақпараттық жүйедегі оқиғалар мен белсенділік туралы деректерді жинау;

8) БАЖ-дың әрекет етуі.

9. БАЖ жұмыс істейтін ортада ортаның мынадай қауіпсіздік функциялары іске асырылған:

1) сенімді маршрутты қамтамасыз ету;

2) сенімді арнаны қамтамасыз ету;

3) қауіпсіз жұмыс істеу жағдайларын қамтамасыз ету;

4) қауіпсіздік атрибуттарын басқару.

10. БАЖ қауіпсіздік функцияларының осы функцияларды іске асыруды қамтамасыз ететін функционалдық мүмкіндіктер құрамы.

11. БАЖ ҚФТ:

1) БАЖ деректерін жинауды жүзеге асыру жөніндегі талаптарды;

2) БАЖ деректерін талдауға қойылатын талаптарды;

3) БАЖ-дың әрекет етуіне қойылатын талаптарды;

4) БАЖ шешуші қағидалар базасын жаңарту құралдарына қойылатын талаптарды;

5) БАЖ-ды қорғау жөніндегі талаптарды;

6) қауіпсіздік функцияларын орындау (БАЖ жұмысын) режимдерін басқару жөніндегі талаптарды;

7) қауіпсіздік функциялары деректерін (БАЖ деректерін) басқару жөніндегі талаптарды;

8) субъектілердің басқару жөніндегі талаптарды;

9) БАЖ-ды әкімшілендіру құралдарына қойылатын талаптарды;

10) БАЖ-дың жұмыс істеу аудитіне қойылатын талаптарды қамтиды.

12. ҚБ-да жазылған БАЖ-дың қауіпсіздігіне қойылатын сенімділік талаптары мынадай мәселелерді қамтиды:

1) конфигурацияны басқару; жеткізу мен пайдалану; әзірлеу; басшылықтар;

2) өміршеңдік кезеңін қолдау;

3) тестілеу;

4) осалдықтарды бағалау;

5) шешуші қағидалар базасын жаңарту.

13. Осы ҚБ-ға сәйкес келетін БАЖ:

1) желілік трафик туралы ақпаратты жинау мүмкіндігін;

2) БАЖ жинаған желілік трафик туралы деректерді уақыттың нақты масштабына жақын режимде талдауды орындау мүмкіндігін және талдаудың нәтижелері бойынша талдау жүргізілген күні мен уақыты, нәтижесі, деректер көзін сәйкестендіргіш, басып кіруді жүргізу үшін пайдаланылған хаттама туралы ақпаратты тіркеуді;

3) сигнатуралық және эвристикалық әдістерді пайдалана отырып, басып кірулерді айқындау мақсатында жиналған деректерді талдауды орындау мүмкіндігін;

4) эвристикалық талдаудың белгіленген деңгейінде желілік трафиктің ауытқуларын айқындау әдістеріне негізделген эвристикалық әдістерді пайдалана отырып, басып кірулерді айқындау мақсатында жиналған деректерді талдауды орындау мүмкіндігін;

5) ашық жүйелердің өзара іс-қимылының базалық эталондық моделінің желілік деңгейі хаттамаларының қызметтік ақпаратын талдау негізінде басып кірулерді айқындау мүмкіндігін;

6) басып кірулерді айқындау немесе қауіпсіздікті бұзу фактілерін аудит журналдарында тіркеу мүмкіндігін;

7) басқару консоліне тиісті хабарлама бейнелеу көмегімен АКИО-ның бақылаудағы тораптарына қатысты айқындалған басып кірулер мен қауіпсіздікті бұзулар туралы БАЖ әкімшісінің хабарламасын;

8) шешуші қағидалар базасын автоматты жаңарту мүмкіндігін;

9) БАЖ-дың қауіпсіздік функцияларын тестілеу (өзін-өзі тестілеу) мүмкіндігін;

10) уәкілетті әкімшілер тарапынан БАЖ-дың қауіпсіздік функцияларын орындау режимін басқару мүмкіндігін;

11) уәкілетті әкімшілер тарапынан БАЖ-дың деректерін басқару мүмкіндігін;

12) БАЖ-ға және олардың нақты БАЖ әкімшілері және АЖ пайдаланушыларымен байланысын қолдау;

13) БАЖ-ды әкімшілендіру мүмкіндігін;

14) ықтимал аудит жүргізілетін оқиғалар үшін аудит жазбаларын өндіру мүмкіндігін;

15) аудиттің әрбір оқиғасын оны бастамалаған субъектінің сәйкестендіргішімен байланыстыру мүмкіндігін;

16) ақпаратты аудит жазбаларынан оқуға мүмкіндік беру мүмкіндігін;

17) аудит жазбаларын оқуға қолжетімділікті шектеуді;

18) аудит деректерін іздеу, іріктеу, ретке кетіруді қамтамасыз етуі тиіс.

14. БАЖ архитектурасының жалпы түрі мынадай компоненттерді қамтиды:

1) АКИО-ның жұмыс істеуі туралы қажетті ақпаратты жинауға арналған БАЖ датчиктері (сенсорлар);

2) басып кірулерді айқындау мақсатында датчиктер жинаған деректерді талдауды орындайтын БАЖ талдағыштары;

3) оқиғалар, тіркелген басып кірулер туралы ақпаратты, сондай-ақ басып кірулердің сигнатуралары мен оның негізінде басып кірудің орын алатыны туралы шешім қабылданатын шешуші қағидалар базасының басқа ақпаратын сақтауды қамтамасыз ететін сақтау орны;

4) қауіпсіздік әкімшісіне БАЖ-ды конфигурациялауға, қорғалатын АКИО және БАЖ-дың жай-күйін бақылауға, талдағыш айқындаған инциденттерді қарауға мүмкіндік беретін БАЖ компоненттерін басқару консолі.

15. БАЖ-дың негізгі компоненттері БАЖ датчи(ктері)гі мен талдағыш(тар)ы болып табылады . Датчиктер АКИО-ға келіп түсетін желілік трафик туралы ақпаратты жинайды, бастапқы талдау жүргізеді және осы ақпаратты (деректерді) талдағышқа жібереді. Талдағыш жиналған деректерді талдауды орындайды, БАЖ әкімшілерін айқындалған басып кірулер туралы хабардар етеді, әрекет ету бойынша басқа іс-қимылдарды орындайды, жиналған ақпараттың (деректердің) негізінде есептерді өндіреді.

16. Желі деңгейінің датчиктері бақылаудағы АЖ сегментіндегі байланыс арнасының үзілген жеріне; порттарға АКИО желілік жабдығын қосу жолымен орнатылуы, сондай-ақ желіаралық экрандарға немесе АКИО-ның коммуникациялық жабдығына интеграцияланған болуы мүмкін.

17. Талдағыштың мынадай функционалдық мүмкіндіктері:

1) датчиктерден деректерді қабылдау;

2) басып кірулерді айқындау мақсатында деректерді өңдеу;

3) айқындалған басып кірулерге әрекет ету.

18. Әрекет етудің есептер құруды, хабарламаны басқару консолінде бейнелеу мен әрекет ету бойынша өзге мүмкіндіктерді қамтуына жол беріледі.

19. БАЖ басып кіруді айқындау туралы шешімді БАЖ сенсорлары БАЖ шешуші қағидалар базасын пайдалана отырып жинайтын ақпаратты талдау нәтижелеріне сәйкес қабылдайды.

20. БАЖ-ды әкімшілендіру қашықтықтан немесе локальдық тәсілдермен орындалуы мүмкін. Локальдық әкімшілендіру нақты БАЖ компоненті орнатылған тораптан, ал қашықтықтан – байланыс арналары бойынша жіберілетін командалар арқылы жүзеге асырылады.

21. Бұдан басқа, БАЖ-дың барлық компоненттерінің мынадай функционалдық мүмкіндіктері:

1) өзінің бағдарламалық және ақпараттық бөлігін араласудан қорғауды (жұмыс істеу ортасының механизмдерімен бірлесіп) жүзеге асыру;

2) өзінің параметрлерін қауіпсіздік әкімшісі тарапынан баптауға жол беру.

АКИО-да желі деңгейінің БАЖ қолданудың үлгілік схемасы осы ҚБ-ға 4-қосымшада беріледі.

22. БАЖ жұмыс істеуі БАЖ қауіпсіздігінің функционалдық талаптарында көрсетілген БАЖ-дың қауіпсіздік саясатына бағындырылған.

2-тарау. Бағалау объектісі қауіпсіздік ортасы

1-Параграф. Қауіпсіздік болжамдары

23. БАЖ-ды алдын ала белгілеп пайдалануға қатысты болжамдар:

1) 1-болжам.

БАЖ-ға өзінің функционалдық мүмкіндіктерін іске асыру үшін қажетті барлық АКИО-ға (бақылаудағы АКИО-ға) БАЖ-дың қолжетімділігі қамтамасыз етілуі;

2) 2-болжам.

Пайдалану құжаттамасына сәйкес БАЖ-ды орнату, конфигурациясы мен басқару;

3) 3-болжам.

БАЖ-дың ол бақылауды жүзеге асыратын АКИО-ның элементтерімен үйлесімділігі;

4) 4-болжам.

БАЖ-дың қауіпсіздік саясатын жүзеге асыру тұрғысынан аса маңызды БАЖ компоненттері орнатылған АКИО элементтерін физикалық қорғау қамтамасыз етілуі;

5) 5-болжам.

БАЖ компоненттері арасында, сондай-ақ БАЖ бен оның жұмыс істеу ортасы арасында уақыт бойынша синхрондау қамтамасыз етілуі;

6) 6-болжам.

БАЖ-дың жұмыс істеуіне жауапты персонал пайдалану құжаттамасын басшылыққа ала отырып, БАЖ-дың тиісінше жұмыс істеуін қамтамасыз етуі тиіс.

2-Параграф. Қатерлер

24. БО қарсы тұруы қатерлер:

1) 1-қатер:

қатердің сипаттау - халықаралық ақпарат алмасу желілерін қоса алғанда, сыртқы ақпараттық-телекоммуникациялық желілерден әрекет ететін сыртқы пайдаланушылар тарапынан ақпаратқа (ақпаратты тасығыштарға) қасақана рұқсатсыз қол жеткізу немесе арнайы әсер ету;

қатер көзі – сыртқы бұзушылар;

қатерді іске асыру тәсілі – АКИО ұсынатын штаттық құралдарды, сондай-ақ мамандандырылған аспаптық құралдарды пайдалана отырып,

АКИО-ның қауіпсіздік механизмдерін ескермеу;

пайдаланылатын осалдықтар – АКИО-да қолданылатын ақпаратты қорғау құралдарының кемшіліктері;

әлеуетті қатерге ұшырағыш ақпараттық ресурстардың түрі – пайдаланушылардың деректері, конфигурациялау деректері, АКИО-ның басқа ресурстары;

ақпараттық ресурстардың бұзылатын қауіпсіздік ерекшеліктері – құпиялылық, тұтастық, қолжетімділік;

қатерді іске асырудың ықтимал салдарлары – АКИО-ның жұмыс істеу режимдерін бұзулар, АКИО қорғау деңгейінің төмендеуі;

2) 2-қатер:

қатердің сипаттау - ақпараттық жүйедегі ақпаратқа қол жеткізу құқығы мен өкілеттіктері бар ішкі пайдаланушылар тарапынан ақпаратқа (ақпарат тасығыштарға) қасақана рұқсатсыз қол жеткізу немесе арнайы әсер ету;

қатер көзі – ішкі бұзушылар;

қатерді іске асыру тәсілі – АКИО ұсынатын штаттық құралдарды, сондай-ақ мамандандырылған аспаптық құралдарды пайдалана отырып, АКИО-ның қауіпсіздік механизмдерін ескермеу;

пайдаланылатын осалдықтар – АКИО-да қолданылатын ақпаратты қорғау құралдарының кемшіліктері;

әлеуетті қатерге ұшырағыш ақпараттық ресурстардың түрі – пайдаланушылардың деректері, конфигурациялау деректері, АКИО-ның басқа ресурстары;

ақпараттық ресурстардың бұзылатын қауіпсіздік ерекшеліктері – құпиялылық, тұтастық, қолжетімділік;

қатерді іске асырудың ықтимал салдарлары – АКИО-ның жұмыс істеу режимдерін бұзулар, АКИО қорғау деңгейінің төмендеуі.

25. БАЖ жұмыс істейтін орта қарсы тұруы қатерлер:

1) 1-орта қатері:

қатердің сипаттау - БАЖ жинаған немесе құрған деректердің (БАЖ деректерінің) тұтастығын бұзу;

қатер көзі – ішкі бұзушы, сыртқы бұзушы;

қатерді іске асыру тәсілі – штаттық және штаттық емес құралдарды пайдалана отырып, БАЖ деректеріне рұқсатсыз қол жеткізу;

пайдаланылатын осалдық – АКИО-да қолжетімділікті басқару, сеанстарды қорғау, жабдықты физикалық қорғау механизмдерінің жеткіліксіздігі; БАЖ аудитінің журналдарын қорғау механизмдерінің жеткіліксіздігі;

әлеуетті қатерге ұшырағыш ақпараттық ресурстардың түрі – БАЖ деректері;

ақпараттық ресурстардың бұзылатын қауіпсіздік ерекшеліктері –тұтастық, қолжетімділік;

қатерді іске асырудың ықтимал салдарлары – әрекет ету туралы шешімдер қабылдау үшін БАЖ жинаған ықтимал басып кірулер (шабуылдар) туралы ақпаратты пайдаланудың мүмкінсіздігі;

2) 2-орта қатері:

қатердің сипаттау - бұзушының БАЖ компоненттерін ажыратуы немесе бұғаттауы;

қатер көзі – ішкі бұзушы, сыртқы бұзушы;

қатерді іске асыру тәсілі – БАЖ компоненттеріне рұқсатсыз қол жеткізу;

пайдаланылатын осалдық – АКИО-да өкілеттіктердің аражігін ажырату рәсімдерінің жеткіліксіздігі, жобалау мен әзірлеу кезеңдерінде енгізілген БАЖ осалдықтары, АКИО бағдарламалық ортасын бақылаудың кемшіліктері;

әлеуетті қатерге ұшырағыш ақпараттық ресурстардың түрі – БАЖ бағдарламалық қамтылымы және шешуші қағидалар базасы;

ақпараттық ресурстардың бұзылатын қауіпсіздік ерекшеліктері –тұтастық, қолжетімділік;

қатерді іске асырудың ықтимал салдарлары – БАЖ-дың жұмыс істеу режимдерін бұзулар, АКИО-ға қатысты іске асырылатын басып кірулерді (шабуылдарды) айқындамау;

3) 3-орта қатері:

қатердің сипаттау - БАЖ конфигурациясын рұқсатсыз өзгерту;

қатер көзі – ішкі бұзушы, сыртқы бұзушы;

қатерді іске асыру тәсілі – БАЖ-дың конфигурациялау ақпаратына (баптауларына) рұқсатсыз қол жеткізу;

пайдаланылатын осалдық – АКИО-да өкілеттіктердің аражігін ажырату рәсімдерінің жеткіліксіздігі, БАЖ-бен өзара іс-қимыл жасайтын және БАЖ-дың жұмыс істеуіне әсер етуі мүмкін АКИО техникалық, бағдарламалық және бағдарламалық-техникалық құралдарының осалдықтары , АКИО-да қолжетімділікті басқару, сеанстарды қорғау, жабдықты физикалық қорғау механизмдерінің жеткіліксіздігі;

әлеуетті қатерге ұшырағыш ақпараттық ресурстардың түрі – БАЖ бағдарламалық қамтылымының баптаулары;

активтердің бұзылатын қауіпсіздік сипаттамалары –тұтастық;

қатерді іске асырудың ықтимал салдарлары – БАЖ-дың жұмыс істеу режимдерін бұзулар, АКИО-ға қатысты іске асырылатын енулерді (шабуылдарды) айқындамау;

4) 4-орта қатері:

қатердің сипаттау - шешуші қағидалар базасын жаңарту механизмі арқылы БАЖ-дың жұмыс істеу логикасына рұқсатсыз өзгерістер енгізу;

қатер көзі – ішкі бұзушылар, сыртқы бұзушылар;

қатерді іске асыру тәсілі – АКИО ұсынатын штаттық құралдарды, сондай-ақ мамандандырылған аспаптық құралдарды пайдалана отырып, рұқсат етілмеген іс-қимылдарды жүзеге асыру;

пайдаланылатын осалдық – БАЖ-дың шешуші қағидалар базасын жаңартуларды алудың сенім білдірілген арнасын қамтамасыз ету механизмдерінің кемшіліктері;

әлеуетті қатерге ұшырағыш ақпараттық ресурстардың түрі – БАЖ бағдарламалық қамтылымы және шешуші қағидалар базасы;

ақпараттық ресурстардың бұзылатын қауіпсіздік ерекшеліктері –тұтастық, қолжетімділік;

қатерді іске асырудың ықтимал салдарлары – БАЖ-дың жұмыс істеу режимдерін бұзу, АКИО-ға қатысты іске асырылатын басып кірулерді (шабуылдарды) айқындамау, әрекет ету туралы шешімдер қабылдау үшін БАЖ жинаған ықтимал басып кірулер (шабуылдар) туралы ақпаратты пайдаланудың мүмкінсіздігі.

3-Параграф. Ұйымның қауіпсіздік саясаты

26. БАЖ төменде келтірілген ұйымның қауіпсіздік саясаты қағидаларын сақтауы тиіс:

1) 1-қауіпсіздік саясаты.

БАЖ-дың қауіпсіздік функцияларын орындауына әсер ететін БАЖ параметрлерін басқаруды БАЖ әкімшілері ғана жүзеге асыру керек;

2) 2-қауіпсіздік саясаты.

БО желілік трафик туралы ақпаратты жинауды жүзеге асыруы тиіс;

3) 3-қауіпсіздік саясаты.

Басып кіруді айқындау туралы шешім шығару мақсатында бақылаудағы АКИО-ның жұмыс істеуі туралы БАЖ жинаған деректерді белгіленген әдістермен аналитикалық өңдеу жүзеге асырылуы тиіс ;

4) 4-қауіпсіздік саясаты.

БАЖ-дың айқындалған басып кірулерге әрекет етуі жүзеге асырылуы тиіс;

5) 5-қауіпсіздік саясаты.

БАЖ-дың уәкілетті әкімшілері тарапынан БАЖ-дың қауіпсіздік функцияларын орындау режимдерін басқару жүзеге асырылуы тиіс;

6) 6-қауіпсіздік саясаты.

Бақылау объектісі рұқсатсыз қолжетімділіктен және БАЖ-дың функциялары мен деректеріне қатысты бұзулардан қорғалған болуы тиіс;

7) 7-қауіпсіздік саясаты.

БАЖ қауіпсіздік функцияларының орындалуын тіркеу мен есебін жүргізу қамтамасыз етілуі;

8) 8-қауіпсіздік саясаты.

БАЖ бағдарламалық кодының тұтастығын бақылау қамтамасыз етілуі;

9) 9-қауіпсіздік саясаты.

Бақылау объектісінің әкімшілендіру интерфейсі.

10) 10-қауіпсіздік саясаты.

Бақылау объектісінің БАЖ-дың шешуші қағидалар базасын (бұдан әрі – ШҚБ) жаңартуларды (өзектілендіру) алу және орнату режимдерін басқару.

3-тарау. Қауіпсіздік мақсаттары

1-Параграф. Бағалау объектісіне арналған қауіпсіздік мақсаттары

27. БАЖ-ға арналған қауіпсіздік мақсаттарының сипаттамасы:

1) 1-қауіпсіздік мақсаты БАЖ параметрлерін басқару.

БАЖ-дың қауіпсіздік функцияларын орындауына әсер ететін БАЖ параметрлерін БАЖ-дың уәкілетті әкімшілері тарапынан басқару мүмкіндігін (БАЖ ШҚБ-дағы қағидалармен, БАЖ басқа деректерімен) БАЖ қамтамасыз етуі тиіс;

2) 2-қауіпсіздік мақсаты. Бақылаудағы АКИО оқиғалары мен белсенділік туралы деректерді жинау.

БАЖ желілік трафикті беру туралы ақпаратты жинауды жүзеге асыруы тиіс;

3) 3-қауіпсіздік мақсаты. БАЖ деректерін талдау.

БАЖ басып кіруді айқындау туралы шешім шығару мақсатында бақылаудағы АКИО-ның жұмыс істеуі туралы БАЖ жинаған деректерді белгіленген әдістермен аналитикалық өңдеуді жүзеге асыруы тиіс;

4) 4-қауіпсіздік мақсаты. БАЖ-дың әрекет етуі.

БАЖ айқындалған басып кірулерге әрекет етуді жүзеге асыруы тиіс;

5) 5-қауіпсіздік мақсаты. БАЖ-дың жұмысын басқару.

БАЖ уәкілетті әкімшілері тарапынан БАЖ-дың қауіпсіздік функцияларын орындау режимдерін басқаруды қамтамасыз етуі тиіс;

6) 6-қауіпсіздік мақсаты. БАЖ басқаруға қолжетімділіктің аражігін ажырату.

БАЖ әкімшілерінің негізінде БАЖ-ды басқаруға қолжетімділіктің аражігін ажыратуды БАЖ қамтамасыз етуі тиіс;

7) 7-қауіпсіздік мақсаты. БАЖ қауіпсіздік аудиті.

БАЖ қауіпсіздік функцияларының орындалуын тіркеу мен есебін БАЖ қамтамасыз етуі тиіс;

8) 8-қауіпсіздік мақсаты. БАЖ тұтастығын бақылау.

БАЖ бағдарламалық кодының тұтастығын бақылауды БАЖ қамтамасыз етуі тиіс;

9) 9-қауіпсіздік мақсаты. БАЖ интерфейсі.

БАЖ әкімшісіне әкімшілендіру интерфейсін БАЖ беруі тиіс;

10) 10-қауіпсіздік мақсаты. ЕАЖ ШҚБ жаңартуларын (өзектілендіруді) орнатуды басқару.

БАЖ ШҚБ жаңартуларды (өзектілендіру) алу және орнату режимдерін басқару мүмкіндігі БАЖ-да.

2-Параграф. Бағалау объектісі ортасына арналған қауіпсіздік мақсаттары

28. БАЖ-дың жұмыс істеу ортасына арналған қауіпсіздік мақсаттарының сипаттамасы:

1) БО-ның жұмыс істеу ортасына арналған 1-мақсат АКИО деректеріне қол жеткізу.

БАЖ-ға өзінің функционалдық міндеттерін (АКИО бақылаудағы объектілеріне) іске асыру үшін қажетті АКИО деректеріне БАЖ-дың қолжетімділігі қамтамасыз етілуі;

2) БО-ның жұмыс істеу ортасына арналған 2-мақсат. БАЖ-ды пайдалану.

Пайдалану құжаттамасына сәйкес БАЖ-ды орнату, конфигурациялау мен басқару қамтамасыз етілуі;

3) БО-ның жұмыс істеу ортасына арналған 3-мақсат. Үйлесімділік.

БАЖ-дың ол бақылауды жүзеге асыратын АКИО элементтерімен үйлесімділігі қамтамасыз етілуі;

4) БО-ның жұмыс істеу ортасына арналған 4-мақсат. БАЖ бөліктерін физикалық қорғау.

БАЖ-дың қауіпсіздік саясатын жүзеге асыру тұрғысынан аса маңызды БАЖ компоненттері орнатылған АКИО элементтерінің физикалық қорғауы қамтамасыз етілуі;

5) БО-ның жұмыс істеу ортасына арналған 5-мақсат. Сенімді байланыс.

БАЖ мен БАЖ-дың әкімшілері арасында сенімді байланыс (бағдар) қамтамасыз етілуі;

6) БО-ның жұмыс істеу ортасына арналған 6-мақсат. Аутентификация және сәйкестендіру механизмдері.

БАЖ-дың жұмыс істеуі БАЖ әкімшілерінің аутентификациясы мен сәйкестендіру механизмдерін ұсынатын жұмыс істеу ортасында жүзеге асырылуы тиіс;

7) БО-ның жұмыс істеу ортасына арналған 7-мақсат. Сенімді арна.

БАЖ ШҚБ жаңартуларын алудың сенімді арнасы қамтамасыз етілуі;

8) БО-ның жұмыс істеу ортасына арналған 8-мақсат. ОҚФ деректерін қорғау.

БАЖ қауіпсіздік функцияларын орындаудың қорғалған аясы қамтамасыз етілуі;

9) БО-ның жұмыс істеу ортасына арналған 9-мақсат. Уақыт бойынша синхрондау.

БАЖ компоненттері арасында, сондай-ақ БАЖ мен оның жұмыс істеу ортасы арасында тиісті уақыт белгілерінің көзі және уақыт бойынша синхрондау қамтамасыз етілуі;

10) БО-ның жұмыс істеу ортасына арналған 10-мақсат. Аудит деректерін сақтау.

Аудит журналын рұқсатсыз өзгерту мен жоюдан қорғау, сондай-ақ аудит деректерін сақтау аймақтарының шамадан тыс толуына әкелуі ықтимал оқиғаларды басқару мүмкіндігі қамтамасыз етілуі;

11) БО-ның жұмыс істеу ортасына арналған 11-мақсат. Қауіпсіздік атрибуттарын басқару.

БАЖ компоненттерінің және бақылаудағы АКИО объектілерінің қауіпсіздік атрибуттарын басқару мүмкіндігі уәкілетті рөлдерге (БАЖ және АКИО әкімшілерінің) ғана берілуі тиіс.

12) БО-ның жұмыс істеу ортасына арналған 12-мақсат Персоналға қойылатын талаптар.

БО жұмыс істеуіне жауапты персонал пайдалану құжаттамасын басшылыққа ала отырып, БО тиісінше жұмыс істеуін қамтамасыз етуі тиіс.

4-тарау. Негіздеме

1-Параграф. Бағалау объектісінің қауіпсіздік мақсаттарының негіздемесі

29. БО-ға арналған қауіпсіздік мақсаттарының ұйымның қауіпсіздік қатерлері мен саясатына осы ҚБ-ға 5-қосымшада әсері беріледі:

1) 1-қауіпсіздік мақсаты.

Бұл қауіпсіздік мақсатына қол жеткізу 1-қатер және 2-қатер қатерлеріне қарсы тұруға, сондай-ақ 1-қауіпсіздік саясаты қауіпсіздік саясатын іске асыру үшін қажет, себебі БАЖ-дың қауіпсіздік функцияларын орындауға әсер ететін БАЖ параметрлерін (БАЖ ШҚБ-дағы қағидалармен, БАЖ басқа деректерімен) БАЖ-дың уәкілетті әкімшілері тарапынан басқару мүмкіндігін қамтамасыз етеді;

2) 2-қауіпсіздік мақсаты.

Бұл қауіпсіздік мақсатына қол жеткізу 1-қатер және 2-қатер қатерлеріне қарсы тұруға, сондай-ақ 2-қауіпсіздік саясаты қауіпсіздік саясатын іске асыру үшін қажет, себебі желілік трафикті беру туралы ақпаратты жинауды қамтамасыз етеді;

3) 3-қауіпсіздік мақсаты.

Бұл қауіпсіздік мақсатына қол жеткізу 1-қатер және 2-қатер қатерлеріне қарсы тұруға, сондай-ақ 3-қауіпсіздік саясаты қауіпсіздік саясатын іске асыру үшін қажет, себебі басып кіруді айқындау туралы шешім шығару мақсатында бақылаудағы АКИО-ның жұмыс істеуі туралы БАЖ жинаған деректерді белгіленген әдістермен талдамалық өңдеуді жүзеге асыруды қамтамасыз етеді ;

4) 4-қауіпсіздік мақсаты.

Бұл қауіпсіздік мақсатына қол жеткізу 1-қатер және 2-қатер қатерлеріне қарсы тұруға, сондай-ақ 4-қауіпсіздік саясаты қауіпсіздік саясатын іске асыру үшін қажет, себебі айқындалған басып кірулерге әрекет етуді жүзеге асыруды қамтамасыз етеді;

5) 5-қауіпсіздік мақсаты.

Бұл қауіпсіздік мақсатына қол жеткізу 1-қатер және 2-қатер қатерлеріне қарсы тұруға, сондай-ақ 5-қауіпсіздік саясаты қауіпсіздік саясатын іске асыру үшін қажет, себебі БАЖ

қауіпсіздік функцияларын орындау режимдерін БАЖ-дың уәкілетті әкімшілері тарапынан басқаруды қамтамасыз етеді;

6) 6-қауіпсіздік мақсаты.

Бұл қауіпсіздік мақсатына қол жеткізу 1-қатер және 2-қатер қатерлеріне қарсы тұруға, сондай-ақ 6-қауіпсіздік саясаты қауіпсіздік саясатын іске асыру үшін қажет, себебі БАЖ-ды басқаруға қолжетімділіктің аражігін БАЖ әкімшілерінің негізінде ажыратуды қамтамасыз етеді;

7) 7-қауіпсіздік мақсаты.

Бұл қауіпсіздік мақсатына қол жеткізу 1-қатер және 2-қатер қатерлеріне қарсы тұруға, сондай-ақ 7-қауіпсіздік саясаты қауіпсіздік саясатын іске асыру үшін қажет, себебі БАЖ қауіпсіздік функцияларын тіркеу мен орындалуын есепке алуды қамтамасыз етеді;

8) 8-қауіпсіздік мақсаты.

Бұл қауіпсіздік мақсатына қол жеткізу 1-қатер және 2-қатер қатерлеріне қарсы тұруға, сондай-ақ 8-қауіпсіздік саясаты қауіпсіздік саясатын іске асыру үшін қажет, себебі бағдарламалық кодтың тұтастығын бақылауды қамтамасыз етеді;

9) 9-қауіпсіздік мақсаты.

Бұл қауіпсіздік мақсатына қол жеткізу 9- қауіпсіздік саясаты қауіпсіздік саясатын іске асыру үшін қажет, себебі әкімшілендіру интерфейсінің болуын қамтамасыз етеді;

10) 10-қауіпсіздік мақсаты.

Бұл қауіпсіздік мақсатына қол жеткізу 10-қауіпсіздік саясаты қауіпсіздік саясатын іске асыру үшін қажет, себебі БАЖ ШҚБ жаңартуларын (өзектілендіруді) алу және орнату режимдерін басқару мүмкіндігін қамтамасыз етеді.

2-Параграф. Бағалау объектісі ортасына арналған қауіпсіздік мақсаттарының негіздемесі

30. Ұйымның қауіпсіздік болжамдарына арналған қауіпсіздік мақсаттары ҚБ-ның 6-қосымшасында келтірілген, ұйымның қауіпсіздік ортасының қатерлеріне қауіпсіздік мақсаттары 7 -қосымшасында көрсетіледі:

1) БО-ның жұмыс істеу ортасына арналған 1-мақсат.

Бұл қауіпсіздік мақсатына қол жеткізу 1-болжам қауіпсіздік болжамын іске асыру үшін қажет, себебі БО өзінің функцияларын іске асыру үшін қажетті АКИО-ның барлық объектілеріне (бақылаудағы АКИО-ға) БАЖ-дың қолжетімділігін қамтамасыз етеді;

2) БО-ның жұмыс істеу ортасына арналған 2-мақсат.

Бұл қауіпсіздік мақсатына қол жеткізу 2-болжам қауіпсіздік болжамын іске асыру үшін қажет, себебі пайдалану құжаттамасына сәйкес БАЖ-ды орнатуды, конфигурациялау мен басқаруды қамтамасыз етеді;

3) БО-ның жұмыс істеу ортасына арналған 3-мақсат.

Бұл қауіпсіздік мақсатына қол жеткізу 3-болжам қауіпсіздік болжамын іске асыру үшін қажет, себебі БАЖ бақылауындағы АКИО элементтерімен үйлесімділікті қамтамасыз етеді;

4) БО-ның жұмыс істеу ортасына арналған 4-мақсат.

Бұл қауіпсіздік мақсатына қол жеткізу 4-болжам қауіпсіздік болжамын іске асыру мен 3-орта қатері ортаға арналған қатерге қарсы тұру үшін қажет, себебі БАЖ қауіпсіздік саясатын жүзеге асыру тұрғысынан аса маңызды БАЖ компоненттері орнатылған АКИО элементтерін физикалық қорғауды қамтамасыз етеді;

5) БО-ның жұмыс істеу ортасына арналған 5-мақсат.

Бұл қауіпсіздік мақсатына қол жеткізу 2-орта қатері ортаға арналған қауіпсіздік қатеріне қарсы тұру үшін қажет, себебі БАЖ және БАЖ әкімшілері арасында сенімді байланысты (бағдарды) қамтамасыз етеді;

6) БО-ның жұмыс істеу ортасына арналған 6-мақсат.

Бұл қауіпсіздік мақсатына қол жеткізу 1,2,3-орта қатерлері ортаға арналған қауіпсіздік қатерлеріне қарсы тұру үшін қажет, себебі БАЖ әкімшілерінің аутентификациясы мен сәйкестендіру механизмдерін ұсынатын жұмыс істеу ортасында БАЖ-дың жұмыс істеуін қамтамасыз етеді;

7) БО-ның жұмыс істеу ортасына арналған 7-мақсат.

Бұл қауіпсіздік мақсатына қол жеткізу 4-орта қатері ортаға арналған қауіпсіздік қатеріне қарсы тұру үшін қажет, себебі БАЖ ШҚБ жаңартуларын сенімді арна бойынша алуды қамтамасыз етеді;

8) БО-ның жұмыс істеу ортасына арналған 8-мақсат.

Бұл қауіпсіздік мақсатына қол жеткізу 1,2,3-орта қатерлері ортаға арналған қауіпсіздік қатерлеріне қарсы тұру үшін қажет, себебі БАЖ қауіпсіздік функцияларын орындауға арналған қорғалған аясы қамтамасыз етіледі;

9) БО-ның жұмыс істеу ортасына арналған 9-мақсат.

Бұл қауіпсіздік мақсатына қол жеткізу 5-болжам қауіпсіздік болжамын іске асыру үшін қажет, себебі БАЖ компоненттері мен БАЖ және олардың жұмыс істеу ортасы арасында уақыт белгілерінің тиісті көзін ұсыну мен уақыт бойынша синхрондау қамтамасыз етіледі;

10) БО-ның жұмыс істеу ортасына арналған 10-мақсат.

Бұл қауіпсіздік мақсатына қол жеткізу 1-орта қатері ортаға арналған қауіпсіздік қатеріне қарсы тұру үшін қажет, себебі аудит журналын рұқсатсыз өзгерту мен жоюдан қорғау, сондай-ақ аудит деректерін сақтау аймақтарының шамадан тыс толуына әкелуі ықтимал оқиғаларды басқару мүмкіндігі қамтамасыз етіледі;

11) БО-ның жұмыс істеу ортасына арналған 11-мақсат.

Бұл қауіпсіздік мақсатына қол жеткізу 2,3-орта қатерлері ортаға арналған қауіпсіздік қатерлеріне қарсы тұру үшін қажет, себебі БАЖ компоненттерінің және бақылаудағы АКИО ақпараттық қауіпсіздік компоненттерін басқару мүмкіндігін тек қана уәкілетті рөлдерге (БАЖ және АКИО әкімшілерінің) беру қамтамасыз етіледі;

12) БО-ның жұмыс істеу ортасына арналған 12-мақсат.

Бұл қауіпсіздік мақсатына қол жеткізу 5-болжам қауіпсіздік болжамын іске асыру үшін қажет, себебі БАЖ-дың жұмыс істеуіне жауапты персоналдың міндеттерді пайдалану құжаттамасын басшылыққа ала отырып орындауын қамтамасыз етеді.

	Жұмыс станцияларына және серверлерге арналған вирусқа қарсы қорғау құралдарының, сондай-ақ желі деңгейіне басып кіруді айқындау жүйелерінің қорғау бейіндеріне 1-қосымша

Вирусқа қарсы қорғау құралы пайдаланылатын ақпараттық-коммуникациялық инфрақұрылым объектілерін үлгілік схемасы

	Жұмыс станцияларына және серверлерге арналған вирусқа қарсы қорғау құралдарының, сондай-ақ желі деңгейіне басып кіруді айқындау жүйелерінің қорғау бейіндеріне 2-қосымша

Қауіпсіздік мақсаттарының ұйымның қауіпсіздік бағалау объектісі қатерлері мен саясатына әсері

	1-қауіпсіздік мақсаты	2-қауіпсіздік мақсаты	3-қауіпсіздік мақсаты	4-қауіпсіздік мақсаты	5-қауіпсіздік мақсаты	6-қауіпсіздік мақсаты	7-қауіпсіздік мақсаты
1-қатер	X	X	X				
2-қатер	X	X	X	X			
1-қауіпсіздік саясаты	X						
2-қауіпсіздік саясаты		X					
3-қауіпсіздік саясаты			X				
4-қауіпсіздік саясаты				X			
5-қауіпсіздік саясаты					X		

6-қауіпсіздік саясаты						X	
7-қауіпсіздік саясаты							X
8-қауіпсіздік саясаты							

	Жұмыс станцияларына және серверлерге арналған вирусқа қарсы қорғау құралдарының, сондай-ақ желі деңгейіне басып кіруді айқындау жүйелерінің қорғау бейіндеріне 3-қосымша

Ортаға арналған қауіпсіздік мақсаттарының қауіпсіздік болжамдарына, қауіпсіздік саясаты мен қатерлерге әсері

	БО-ның жұмыс істеу ортасына арналған 1-мақсат	БО-ның жұмыс істеу ортасына арналған 2-мақсат	БО-ның жұмыс істеу ортасына арналған 3-мақсат	БО-ның жұмыс істеу ортасына арналған 4-мақсат	БО-ның жұмыс істеу ортасына арналған 5-мақсат	БО-ның жұмыс істеу ортасына арналған 6-мақсат	БО-ның жұмыс істеу ортасына арналған 7-мақсат	БО-ның жұмыс істеу ортасына арналған 8-мақсат	БО-ның жұмыс істеу ортасына арналған 9-мақсат	БО-ның жұмыс істеу ортасына арналған 10-мақсат
1-болжам	X									
2-болжам		X								
3-болжам			X							
4-болжам				X						
5-болжам					X					
6-болжам						X				
7-болжам							X			
1-орта қатері					X				X	
2-орта қатері								X	X	
3-орта қатері										X

	Жұмыс станцияларына және

	серверлерге арналған вирусқа қарсы қорғау құралдарының, сондай-ақ желі деңгейіне басып кіруді айқындау жүйелерінің қорғау бейіндеріне 4-қосымша

Ақпараттық-коммуникациялық инфрақұрылым объектілері желі деңгейінің басып кірулерді айқындау жүйесі қолданудың үлгілік схемасы

	Жұмыс станцияларына және серверлерге арналған вирусқа қарсы қорғау құралдарының, сондай-ақ желі деңгейіне басып кіруді айқындау жүйелерінің қорғау бейіндеріне 5-қосымша

БО-ға арналған қауіпсіздік мақсаттарының ұйымның қауіпсіздік қатерлері мен саясатына әсері.

	1-қауіпсіздік мақсаты	2-қауіпсіздік мақсаты	3-қауіпсіздік мақсаты	4-қауіпсіздік мақсаты	5-қауіпсіздік мақсаты	6-қауіпсіздік мақсаты	7-қауіпсіздік мақсаты
1-қатер	X	X	X	X	X	X	X
2-қатер	X	X	X	X	X	X	X

1-қауіпсіздік саясаты	X						
2-қауіпсіздік саясаты		X					
3-қауіпсіздік саясаты			X				
4-қауіпсіздік саясаты				X			
5-қауіпсіздік саясаты					X		
6-қауіпсіздік саясаты						X	
7-қауіпсіздік саясаты							X
8-қауіпсіздік саясаты							
9-қауіпсіздік саясаты							
10-қауіпсіздік саясаты							

	Жұмыс станцияларына және серверлерге арналған вирусқа қарсы қорғау құралдарының, сондай-ақ желі деңгейіне басып кіруді айқындау жүйелерінің қорғау бейіндеріне 6-қосымша

Ортаға арналған қауіпсіздік мақсаттарының ұйымның қауіпсіздік болжамдарына, қауіпсіздік қатерлері мен саясатына әсері.

	БО-ның жұмыс істеу ортасына арналған 1-мақсат	БО-ның жұмыс істеу ортасына арналған 2-мақсат	БО-ның жұмыс істеу ортасына арналған 3-мақсат	БО-ның жұмыс істеу ортасына арналған 4-мақсат	БО-ның жұмыс істеу ортасына арналған 5-мақсат	БО-ның жұмыс істеу ортасына арналған 6-мақсат	БО-ның жұмыс істеу ортасына арналған 7-мақсат	БО-ның жұмыс істеу ортасына арналған 8-мақсат	БО-ның жұмыс істеу ортасына арналған 9-мақсат	БО-ның жұмыс істеу ортасына арналған 10-мақсат
1-болжам										
2-болжам										

3-болжам										
4-болжам										
5-болжам										
6-болжам										

	Жұмыс станцияларына және серверлерге арналған вирусқа қарсы қорғау құралдарының, сондай-ақ желі деңгейіне басып кіруді айқындау жүйелерінің қорғау бейіндеріне 7-қосымша

Ортаға арналған қауіпсіздік мақсаттарының ұйымның қауіпсіздік болжамдарына, қауіпсіздік қатерлері мен саясатына әсері.

	БО-ның жұмыс істеу ортасына арналған 1-мақсат	БО-ның жұмыс істеу ортасына арналған 2-мақсат	БО-ның жұмыс істеу ортасына арналған 3-мақсат	БО-ның жұмыс істеу ортасына арналған 4-мақсат	БО-ның жұмыс істеу ортасына арналған 5-мақсат	БО-ның жұмыс істеу ортасына арналған 6-мақсат	БО-ның жұмыс істеу ортасына арналған 7-мақсат	БО-ның жұмыс істеу ортасына арналған 8-мақсат	БО-ның жұмыс істеу ортасына арналған 9-мақсат	БО-ның жұмыс істеу ортасына арналған 10-мақсат
1-орта қатері										
2-орта қатері										
3-орта қатері										
4-орта қатері										

	Қазақстан Республикасы Қорғаныс және аэроғарыш өнеркәсібі министрінің 2018 жылғы 27 маусымдағы № 105/НҚ бұйрығына 2-қосымша

Қорғау бейіндерін әзірлеу әдістемесі

1-тарау. Жалпы ережелер

1. Осы Қорғау бейіндерін әзірлеу әдістемесі (бұдан әрі – Әдістеме) "Ақпараттандыру туралы" 2015 жылғы 24 қарашадағы Қазақстан Республикасының Заңы (бұдан әрі – Заң) 7-1-бабының 18) тармақшасына сәйкес әзірленді.

2. Әдістеме қорғау бейіндерін, ақпараттық-коммуникациялық инфрақұрылым объектілерін әзірлеу үшін арналған.

3. Осы Әдістемеде мынадай терминдер мен анықтамалар пайдаланылады:

1) ақпараттық-коммуникациялық инфрақұрылым объектілері (бұдан әрі – АКИО) – ақпараттық жүйелер, технологиялық платформалар, аппараттық-бағдарламалық кешендер, телекоммуникация желілері, сондай-ақ техникалық құралдардың үздіксіз жұмыс істеуін және ақпараттық қауіпсіздікті қамтамасыз ету жүйелері;

2) ақпараттық-коммуникациялық инфрақұрылым – электрондық ақпараттық ресурстарды қалыптастыру және оларға қолжетімділік беру мақсатында технологиялық ортаның жұмыс істеуін қамтамасыз етуге арналған ақпараттық-коммуникациялық инфрақұрылым объектілерінің жиынтығы;

3) бағалау объектісі (бұдан әрі – БО) – әкімші және пайдаланушы басшылықтары берілген АКИО-ның бағалауға жататын компоненттері;

4) қауіпсіздігі тұрғысынан сенімділік - АКИО компоненттерінің өзінің қауіпсіздік мақсаттарына жауап беретініне сенімді болудың негіздемесі;

5) қорғау бейіні (бұдан әрі – ҚБ) – ақпараттандыру объектілерінің компоненттері болып табылатын бағдарламалық және техникалық құралдардың қауіпсіздігіне қойылатын ең төменгі талаптардың тізілімі;

6) қауіпсіздік жөніндегі тапсырма – нақты АКИО-ны бағалаудың негізі ретінде пайдалануға арналған қауіпсіздік талаптары мен ерекшеліктер жиынтығы;

7) БО қауіпсіздік саясаты – активтерді басқаруды, оларды қорғауды және АКИО шегінде бөлуді реттейтін қағидалар жиынтығы;

8) ұйымның қауіпсіздік саясаты – ұйым өз қызметінде басшылыққа алатын қауіпсіздік саласындағы бір немесе бірнеше қағидалар, рәсімдер, практикалық тәсілдер немесе басшылық қағидаттары;

9) қауіпсіздік функциясы – БО қауіпсіздік саясатының өзара байланысты қағидаларының ішкі жиынтығын орындауды қамтамасыз ететін АКИО бөлігінің немесе бөліктерінің функционалдық мүмкіндіктері;

10) қауіпсіздік қатері (бұдан әрі – қатер) – АКИО немесе оның иесіне зиян келтіруге әкелуі ықтимал инциденттің туындауының әлеуетті немесе нақты орын алатын қауіп-қатерін айқындайтын шарттар мен факторлардың жиынтығы;

11) қауіпсіздік мақсаты – ұйымның анықталған қатерлерге қарсы тұру және/немесе белгіленген қауіпсіздік саясаты мен болжамдарды қанағаттандырудың жазылған ниеті.

2-тарау. Қорғау бейіндеріне қойылатын талаптар

4. ҚБ қауіпсіздік талаптарының АКИО компоненттерінің сыныптау санаты қанағаттандыруы тиіс үлгілік (стандартталған) жинағын білдіреді.

5. ҚБ:

1) АКИО компоненттерін пайдаланушылардың қауіпсіздікті қамтамасыз етуге мұқтаждығының сипаттамасын;

2) ұйымның қауіпсіздік саясатының және АКИО компоненттерінің қауіпсіздік ортасының ол туғызатын ықтимал қатерлері ескерілген сипаттамасын;

3) АКИО компоненттерінің олардың қауіпсіздік ортасының сипаттамасына негізделген қауіпсіздік мақсаттарын, сондай-ақ оны қамтамасыз етуге арналған шарларды;

4) АКИО компоненттерінің олардың қауіпсіздік проблемасын шешуге бағытталған қауіпсіздіктің функционалдық талаптары мен қауіпсіздігіне қойылатын сенімділік талаптарын;

5) қауіпсіздік проблемаларының (қатерлердің, болжамдар мен қауіпсіздік саясатының ережелері терминдерінде) және олардың шешімдерінің сипаттамасын;

6) ҚБ-да берілген АКИО компоненттерін пайдаланушылардың олардың қауіпсіз болу мұқтаждығын қанағаттандыруға арналған қауіпсіздіктің функционалдық талаптары мен қауіпсіздігіне қойылатын сенімділік талаптары жеткіліктігінің негіздемесін қамтиды.

3-тарау. Қорғау бейінінің құрылымы мен мазмұны

6. Қорғау бейіні мына тараулардан тұрады:

1) Жалпы ережелер;

2) Бағалау объектісі қауіпсіздік ортасы;

3) Қауіпсіздік мақсаттары;

4) Негіздеме.

7. "Жалпы ережелер" тарауында ҚБ туралы деректер сипатталады, ҚБ сәйкестендіріледі және ҚБ каталогтары мен тізілімдеріне енгізу үшін ең қолайлы нысанда оның аннотациясы беріледі.

8. "Бағалау объектісінің қауіпсіздік ортасы" тарауына АКИО компонентінің (БО-ны білдіретін) оны пайдалану болжамдалатын қауіпсіздік ортасы аспектілерінің сипаттамасы, сондай-ақ аталған АКИО компонентін пайдалану тәсілі енгізіледі.

Бұл тарау мына параграфтарды қамтиды:

1) Қауіпсіздік болжамдары (АКИО компонентінің мақсаты мен оны пайдалану ортасы туралы болжамдар);

2) Қатерлер (АКИО компонентінің қауіпсіз жұмыс істеуне төнетін қатерлер);

3) Ұйымның қауіпсіздік саясаты (ұйымның АКИО компоненті қанағаттандыруы тиіс қауіпсіздік саясаты).

9. "Қауіпсіздік мақсаттары" тарауына БО қауіпсіздік мақсаттарының (АКИО компонентінің қауіпсіз жұмыс істеуне төнетін қатерлерге қарсы тұру бойынша қалыптастырған шешімдер) және БО ортасына арналған қауіпсіздік мақсаттарының (АКИО компонентінің ортасына арналған қауіпсіздік қатерлеріне қарсы тұру бойынша қалыптастырған шешімдер) сипаттамасы енгізіледі.

Бұл тарау мына параграфтарды қамтиды:

1) Бағалау объектісіне арналған қауіпсіздік мақсаттары;

2) Бағалау объектісі ортасына арналған қауіпсіздік мақсаттары.

10. "Негіздеме" тарауына қауіпсіздік мақсаттарының және қауіпсіздік талаптарының, соның ішінде:

АКИО компоненті мен оның ортасына арналған функционалдық талаптар мен қауіпсіздігіне қойылатын сенімділік талаптары қауіпсіздік мақсаттарына сәйкес келетіні;

қауіпсіздік талаптарының бір-біріне қайшы еместігі;

қауіпсіздік талаптарын таңдау негізделген болып табылатыны;

АКИО компоненті функцияларының оның қауіпсіздік мақсаттарына үйлесімділігі туралы логикалық негіздемесі енгізіледі.

Бұл тарау мына параграфтарды қамтиды:

1) Бағалау объектісі қауіпсіздік мақсаттарының негіздемесі;

2) Бағалау объектісі ортасына арналған қауіпсіздік мақсаттарының негіздемесі.