12- семинар сабағы.

АКТ және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптар

Ақпараттық қауіпсіздікті қамтамасыз ету саласына қатысты біріңғай талаптар (БТ) ережелерін мемлекеттік органдар, жергілікті атқарушы органдар, мемлекеттік заңды тұлғалар, квазимемлекеттік сектор субъектілері, мемлекеттік органдардың ақпараттық жүйелерімен интеграцияланатын немесе мемлекеттік электрондық ақпараттық ресурстарды қалыптастыруға арналған мемлекеттік емес ақпараттық жүйелердің иелері және иеленушілері, сондай-ақ ақпараттық-коммуникациялық инфрақұрылымның өте маңызды объектілерінің иелері мен иеленушілері міндетті түрде қолдануы тиіс.

Ақпараттық қауіпсіздікті ұйымдастыруға қойылатын талаптар

Ұйымда АҚ ұйымдастыру, қамтамасыз ету және басқару кезінде "Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Ақпараттық қауіпсіздікті басқару құралдары туралы ережелер жиынтығы" ҚРҚР СТ ИСО/МЭК 27002-2015 стандартының ережелерін басшылыққа алынады.

29-1. Елдің қорғанысы мен мемлекеттің қауіпсіздігі үшін АЖ-ны қамтамасыз ету талаптарын орындау мақсатында тауарларды сатып алу ҚРмемлекеттік сатып алу туралы заңнамасына сәйкес сенім білдірілген бағдарламалық қамтылым мен электрондық өнеркәсіп өнімі тізілімінен жүзеге асырылады.

Бұл ретте сенім білдірілген бағдарламалық қамтылым мен электрондық өнеркәсіп өнімі тізілімінде қажетті өнім болмаған жағдайда, тауарларды ҚРмемлекеттік сатып алу туралы заңнамасына сәйкес сатып алуға жол беріледі.

30. АҚ қамтамасыз ету саласындағы жауапкершіліктің және функциялардың аражігін ажырату мақсатында ақпараттандыру объектілерін құру, сүйемелдеу және дамыту мәселелерімен айналысатын басқа құрылымдық бөлімшелерден оқшау құрылымдық бөлімше болып табылатын АҚ бөлімшесі құрылады немесе АҚ-ны қамтамасыз етуге жауапты лауазымды адам белгіленеді.

АҚ жеке құрылымдық бөлімшесін құру бойынша осы тармақтың талаптары арнаулы мемлекеттік органдарға қолданылмайды.

АҚ бөлімшелері немесе АҚ қамтамасыз етуге жауапты лауазымды адам:

1) АҚ ТҚ талаптарының орындалуын бақылауды;
2) АҚ құжаттық ресімделуін бақылауды;
3) АҚ қамтамасыз ету бөлігінде активтердің басқарылуын бақылауды;
4) БҚ пайдаланудың заңдылығын бақылауды;

5) АКТ саласындағы тәуекелдердің басқарылуын бақылауды;

6) АҚ оқиғаларының тіркелуін бақылауды;

7) АҚ ішкі аудитін жүргізуді;

8) АҚ сыртқы аудитінің ұйымдастырылуын бақылауды;

9) АКТ пайдаланатын бизнес-процестер үздіксіздігінің қамтамасыз етілуін бақылауды;

10) персоналды басқару кезінде АҚ талаптарының сақталуын бақылауды;

11) "электрондық үкіметтің" ақпараттандыру объектісі АҚ-сының жай-күйін бақылауды жүзеге асырады.

32. Ұйымның АҚ саясаты бірінші деңгейдегі құжат болып табылады және МО немесе ұйым күнделікті қызметінде басшылыққа алатын АҚ-ны қамтамасыз ету саласындағы мақсаттарды, міндеттерді, басшылық қағидаттары мен практикалық тәсілдерді айқындайды.

33. Екінші деңгейдегі құжаттар тізбесіне АҚ саясатының талаптарын нақтылайтын құжаттар кіреді, соның ішінде:

1) ақпараттық қауіпсіздік тәуекелдерін бағалау әдістемесі;

2) ақпаратты өңдеу құралдарымен байланысты активтерді сәйкестендіру, жіктеу және таңбалау қағидалары;

3) ақпаратты өңдеу құралдарымен байланысты активтердің үздіксіз жұмысын қамтамасыз ету жөніндегі қағидалар;

4) есептеу техникасы құралдарын, телекоммуникация жабдығын және бағдарламалық қамтылымды түгендеу мен паспорттау қағидалары;

5) ішкі АҚ аудитін жүргізу қағидалары;

6) ақпаратты криптографиялық қорғау құралдарын пайдалану тәртібі;

7) электрондық ақпараттық ресурстарға қол жеткізу құқығының аражігін ажырату қағидалары;

8) Интернет желісі мен электрондық поштаны пайдалану қағидалары;

9) аутентификациялау рәсімін ұйымдастыру қағидалары;

10) вирусқа қарсы бақылауды ұйымдастыру қағидалары;

11) мобильдік қондырғыларды және ақпаратты тасығыштарды пайдалану қағидалары;

12) ақпаратты өңдеу құралдарын нақты қорғауды және ақпараттық ресурстардың қауіпсіз қызмет ету ортасын ұйымдастыру қағидалары.

34. Үшінші деңгейдегі құжаттар АҚ-ны қамтамасыз ету процестері мен рәсімдерінің сипаттамаларын қамтиды, соның ішінде:

1) АҚ қатерлері (тәуекелдері) каталогы;

2) АҚ қатерлерін (тәуекелдерін) өңдеу жоспары;

3) ақпаратты резервтік көшіру және қалпына келтіру регламенті;

4) ақпаратты өңдеу құралдарымен байланысты активтердің үздіксіз жұмысын және жұмыс қабілеттілігін қалпына келтіруді қамтамасыз ету бойынша іс-шаралар жоспары;

5) әкімшінің ақпараттандыру объектісін сүйемелдеу жөніндегі басшылығы;

6) пайдаланушылардың АҚ инциденттеріне ден қою және штаттан тыс (дағдарысты) жағдайларда әрекет ету бойынша іс-қимыл тәртібі туралы нұсқаулық.

35. Төртінші деңгейдегі құжаттар тізбесі орындалған рәсімдер мен жұмыстарды тіркеу және растау үшін пайдаланылатын жұмыс нысандарын, журналдарды, өтінімдерді, хаттамаларды және электрондық құжаттарды қоса алғанда, басқа да құжаттарды қамтиды, соның ішінде:

1) АҚ инциденттерін тіркеу және штаттан тыс оқиғаларды есепке алу журналы;

2) серверлік үй-жайларға кіру журналы;

3) желілік ресурстардың осалдықтарын бағалауды жүргізу туралы есеп;

4) кабельдік қосылуларды есепке алу журналы;

5) резервтік көшірмелерді (резервтік көшірме, қайта қалпына келтіру), резервтік көшірмелерді тестілеуді есепке алу журналы;

6) жабдық конфигурациясының өзгеруін есепке алу, АЖ ЕБҚ мен ҚБҚ тестілеу және өзгерістерді есепке алу, БҚ осалдықтарын тіркеу және жою журналы;

7) серверлік үй-жайларға арналған дизель-генераторлық қондырғыларды және үздіксіз қуат беру көздерін тестілеу журналы;

8) серверлік үй-жайлардың микроклиматын, бейнебақылауды, өрт сөндіруді қамтамасыз ету жүйелерін тестілеу журналы.

36. Активтерді қорғауды қамтамасыз ету үшін:

1) активтерді түгендеу;

2) активтерді МО-да, ЖАО-да қабылданған сыныптау жүйесіне сәйкес сыныптау және таңбалау;

3) активтерді лауазымды тұлғаларға бекіту мен активтердің АҚ-сын басқару жөніндегі іс-шараларды іске асыру үшін олардың жауапкершілік көлемін белгілеу;

4) АҚ ТҚ-да:

активтерді қолдану мен қайтару;

активтерді сәйкестендіру, сыныптау мен таңбалау тәртібін реттеу жүргізіледі.

37. МО-да немесе ЖАО-да АКТ саласындағы тәуекелдерді басқару мақсатында:

1) ҚР СТ 31010-2010 "Тәуекел менеджменті. Тәуекелді бағалау әдістері" Қазақстан Республикасы стандартының ұсынымдарына сәйкес тәуекелдерді бағалау әдісін таңдау және тәуекелдерді талдау рәсімдерін әзірлеу;

2) сәйкестендірілген және сыныпталған активтердің тізбесіне қатысты тәуекелдерді сәйкестендіру жүзеге асырылады, ол мыналарды қамтиды:

АҚ қатерлерін және олардың көздерін айқындау;

қатерлердің іске асырылуына әкеп соғуы мүмкін осалдықтарды айқындау;

ақпараттың таралу арналарын анықтау;

бұзушы моделін қалыптастыру;

3) сәйкестендірілген тәуекелдерді қабылдау өлшемшарттарын таңдау;

4) мыналарды:

ҚР СТ ИСО/МЭК 27005-2013 "Ақпараттық технологиялар. Қауіпсіздікті қамтамасыз ету әдістері. Ақпараттық қауіпсіздік тәуекелі менеджменті" Қазақстан Республикасы стандартының талаптарына сәйкес сәйкестендірілген тәуекелдерді бағалауды (қайта бағалауды);

ықтимал нұқсанды айқындауды қамтитын АҚ қатерлері (тәуекелдері) каталогын қалыптастыру;

5) АҚ қатерлерін (тәуекелдерін) бейтараптандыру немесе төмендету жөніндегі іс-шараларды қамтитын оларды өңдеу жоспарын әзірлеу және бекіту жүзеге асырылады.

38. ... АҚ-ның бұзылу оқиғаларын бақылау мақсатында:

1) АҚ-ны бұзуға байланысты оқиғалар мониторингі мен мониторинг нәтижелерін талдау жүргізіледі;

2) АҚ-ның жай-күйіне байланысты оқиғалар тіркеліп, оқиғалар журналдарын, соның ішінде:

операциялық жүйелердің оқиғалар журналдарын;

дерекқорларды басқару жүйелерінің оқиғалар журналдарын;

вирусқа қарсы қорғау оқиғаларының журналдарын;

қолданбалы БҚ оқиғалар журналдарын;

телекоммуникациялық жабдықтың оқиғалар журналдарын;

шабуылдарды анықтау және алдын алу жүйелерінің оқиғалар журналдарын;

контентті басқару жүйесі оқиғаларының журналын талдау арқылы бұзушылықтар анықталады;

3) оқиғаларды тіркеу журналдарындағы уақытты уақыт көзінің инфрақұрылымымен үйлесімді ету қамтамасыз етіледі;

4) оқиғаларды тіркеу журналдары АҚ ТҚ-да көрсетілген, бірақ үш жылдан кем емес мерзім бойы сақталады және кем дегенде екі ай жедел қолжетімді болады;

Ақпараттық қауіпсіздікті қамтамасыз ету саласындағы уәкілетті орган ұлттық қауіпсіздік органдарымен келісу бойынша бекітетін "электрондық үкіметтің" ақпараттандыру объектілерінің және ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілерінің ақпараттық қауіпсіздігін қамтамасыз ету мониторингін жүргізу қағидаларында айқындалатын форматтар мен жазба түрлеріне сәйкес оқиғаларды тіркеу журналдары жүргізіледі;

6) оқиғаларды тіркеу журналдарын араласудан және авторланбаған қолжетімділіктен қорғау қамтамасыз етіледі. Жүйе әкімшілеріне журналдарды өзгертуге, жоюға және ажыратуға өкілеттік беруге жол берілмейді. Құпия АЖ үшін журналдардың резервтік қоймасын құру және оны жүргізу талап етіледі;

7) АҚ инциденттері туралы хабардар етудің және АҚ-ның инциденттеріне әрекет етудің формальді рәсімін енгізу қамтамасыз етіледі.

39. ...Ұйымның өте маңызды процестерін ішкі және сыртқы қатерлерден қорғау мақсатында:

1) ақпаратты өңдеу құралдарымен байланысты активтер жұмысының үздіксіздігін және жұмыс қабілеттілігін қалпына келтіруді қамтамасыз ету жөніндегі іс-шаралар жоспары әзірленеді, тестілеуден өтеді және іске асырылады;

2) пайдаланушылардың АҚ инциденттеріне және штаттан тыс (дағдарысты) жағдайларда әрекет етуі бойынша іс-қимыл тәртібі туралы нұсқаулық МО, ЖАО қызметшілерінің немесе ұйым жұмыскерлерінің назарына жеткізіледі.

Ақпаратты өңдеу құралдарымен байланысты активтер жұмысының үздіксіздігін және жұмыс қабілеттілігін қалпына келтіруді қамтамасыз ету жөніндегі іс-шаралар жоспары үнемі өзектілендіруге жатады.

40. ..Ұйым жұмыскерлерінің АҚ-ны қамтамасыз ету бойынша функционалдық міндеттері мен АҚ ТҚ талаптарын орындау бойынша міндеттемелері лауазымдық нұсқаулықтарға және (немесе) еңбек шартының талаптарына енгізіледі.

41. ЭАР, АЖ, АКИ ақпараттық қауіпсіздігін қамтамасыз етуге бөгде ұйымдарды тартқан жағдайда олардың иесі немесе иеленушісі аталған объектілермен жұмыс істеу, оларға қол жеткізу немесе пайдалану шарттары, сондай-ақ оларды бұзғаны үшін жауапкершілігі белгіленетін келісімдер жасайды.

42. АҚ-ны қамтамасыз ету саласында міндеттемелері бар МО, ЖАО қызметшілерін немесе ұйым жұмыскерлерін жұмыстан босатқан кездегі рәсімдердің мазмұны АҚ ТҚ-да белгіленеді.

43. Жұмыстан босатылған немесе еңбек шарты талаптарына өзгерістер енгізілген кезде МО, ЖАО қызметшісінің немесе ұйым қызметкерінің жеке және логикалық қолжетімділікті, қол жеткізу, қол қою сәйкестендіргіштерін және оны МО, ЖАО жұмыс істейтін қызметшісі немесе ұйым жұмыскері ретінде сәйкестендіретін құжаттаманы қамтитын ақпаратқа және ақпаратты өңдеу құралдарына қол жеткізу құқықтары оның еңбек шарты тоқтатылғаннан кейін жойылады немесе еңбек шартының талаптарына өзгерістер енгізілген кезде өзгертіледі.

44. Кадр қызметі МО, ЖАО қызметшілерін немесе ұйым жұмыскерлерін ақпараттандыру және АҚ-ны қамтамасыз ету саласында оқытуды ұйымдастырады және есебін жүргізеді.

46. Ақпараттандыру объектілерін пайдалану кезінде АҚ қамтамасыз ету мақсатында:

1) аутентификация тәсілдеріне;

2) қолданылатын АККҚ-ға;

3) қолжетімділікті және істен шығуының болмаушылығын қамтамасыз ету тәсілдеріне;

4) АҚ-ны қамтамасыз ету, қорғауды және қауіпсіз жұмыс істеуі мониторингіне;

5) АҚ қамтамасыз ету құралдары мен жүйелерін қолдануға;

6) куәландырушы орталықтардың тіркеу куәліктеріне қойылатын талаптар белгіленеді.

47. Сыныптауышқа сәйкес бірінші және екінші сыныптағы ақпараттандыру объектілеріне қол жеткізу кезінде көп факторлы, соның ішінде ЭЦҚ пайдаланыла отырып аутентификация қолданылады.

48. Құпия АЖ, құпия ЭАР және қолжетімділігі шектелген дербес деректерді қамтитын ЭАР қызметтік ақпаратын қорғау мақсатында ҚР СТ 1073-2007 "Ақпаратты криптографиялық қорғау құралдары. Жалпы техникалық талаптар" ҚРстандартына сәйкес АККҚ-ға қойылатын талаптарға сәйкес келетін мынадай параметрлері бар:

бірінші сыныптағы ақпараттандыру объектілері үшін сыныптауышқа сәйкес – үшінші қауіпсіздік деңгейінің;

екінші сыныптағы ақпараттандыру объектілері үшін сыныптауышқа сәйкес – екінші қауіпсіздік деңгейінің;

үшінші сыныптағы ақпараттандыру объектілері үшін сыныптауышқа сәйкес – бірінші қауіпсіздік деңгейінің АККҚ (бағдарламалық және аппараттық) қолданылады.

49. Қолжетімділікті және істен шығуының болмаушылығын қамтамасыз ету үшін ЭҮ ақпараттандыру объектілерінің иелері:

1) сыныптауышқа сәйкес бірінші және екінші сыныптағы ЭҮ ақпараттандыру объектілеріне арналған меншікті немесе жалға алынған резервті серверлік үй-жайдың болуын;

2) аппараттық-бағдарламалық деректерді өңдеу құралдарын, деректерді сақтау жүйелерін, деректерді сақтау желілерінің компоненттері мен деректерді беру арналарын, соның ішінде сыныптауышқа сәйкес:

бірінші сыныптағы ЭҮ ақпараттандыру объектілерін – резервтік серверлік үй-жайда жүктememен (жедел);

екінші сыныптағы ЭҮ ақпараттандыру объектілерін – резервтік серверлік үй-жайда жүктемесіз (іске қосылмаған);

үшінші сыныптағы ЭҮ ақпараттандыру объектілерін – негізгі серверлік үй-жайға жақын орналасқан қоймада сақтаумен резервтеуді қамтамасыз етеді.

50. Сыныптауышқа сәйкес бірінші және екінші сыныптағы ЭҮ ақпараттандыру объектілері оларды өндірістік пайдалануға енгізгеннен кейін бір жылдан кешіктірмей АҚ-ны қамтамасыз ету, қорғауды және қауіпсіз жұмыс істеуі мониторингі жүйесіне қосылады.

51. МО, ЖАО немесе ұйым:

пайдаланушылар мен персоналдың іс-қимылы;

ақпаратты өңдеу құралдарын қолдану мониторингін жүзеге асырады.

52. МО-да, ЖАО-да немесе ұйымда пайдаланушылар мен персонал іс-қимылының мониторингін жүзеге асыру шеңберінде:

1) пайдаланушылардың аномальді белсенділігі мен қасақана іс-қимылдары айқындалған кезде, мұндай іс-әрекеттер:

сыныптауышқа сәйкес бірінші сыныптағы ЭҮ ақпараттандыру объектілері үшін тіркеледі, бұғатталады және әкімшісі жедел хабардар етіледі;

сыныптауышқа сәйкес екінші сыныптағы ЭҮ ақпараттандыру объектілері үшін тіркеледі және бұғатталады;

сыныптауышқа сәйкес үшінші сыныптағы ЭҮ ақпараттандыру объектілері үшін тіркеледі;

2) қызмет көрсетуші персоналдың іс-қимылдарын АҚ бөлімшесі тіркейді және бақылайды.

53. АҚ оқиғалары мониторингін және оқиғалар журналын талдау нәтижелері бойынша құпиялылығы, қолжетімділігі мен тұтастығы үшін өте қатерлі болып сәйкестендірілген АҚ оқиғалары:

1) АҚ инциденттері ретінде анықталады;

2) АҚ қатерлері (тәуекелдері) каталогында есепке алынады;

3) мемлекеттік техникалық қызметтің компьютерлік инциденттерге әрекет ету қызметінде тіркеледі.

54. Ақпараттандыру объектілерін тәжірибелік және өнеркәсіптік пайдалану кезеңінде:

зиянды кодты анықтау мен алдын алу;

АҚ инциденттері мен оқиғаларын басқару;

басып кіруді анықтау және алдын алу;

ақпараттық инфрақұрылым мониторингі және оны басқару құралдары мен жүйелері пайдаланылады.

54-1. Локальды желілерде деректердің таралуын болдырмау жүйелерін (DLP) қолдануға жол беріледі. Бұл ретте:

іс-әрекеттерге жүргізілетін бақылау туралы пайдаланушыға визуалды хабарлау;

пайдаланушының іс-әрекеттеріне бақылауды жүзеге асыру үшін оның жазбаша келісімін алу;

басқару орталығын және деректердің таралуын болдырмау жүйесін локальды желі шегінде орналастыру қамтамасыз етіледі.

55. Қазақстан Республикасы негізгі куәландырушы орталығының тіркеу куәліктері ҚР СТ ИСО/МЭК 14888-1-2006 "Ақпараттық технология. Ақпаратты қорғау әдістері. Қосымшалары бар цифрлық қолтаңбалар. 1-бөлім. Жалпы ережелер", ҚР СТ ИСО/МЭК 14888-3-2006 "Ақпаратты қорғау әдістері. Қосымшалары бар цифрлық қолтаңбалар. 3-бөлім. Сертификатқа негізделген механизмдер", ГОСТ Р ИСО/МЭК 9594-8-98 "Ақпараттық технология. Ашық желілердің өзара байланысы. Анықтамалық. 8-бөлім. Аутентификация негіздері" стандарттарына сәйкес

аутентификация мақсаттарында әлемдік БҚ өндірушілер бағдарламалық өнімдерінің сенімді тізімдерінде тануға жатады.

56. ҚР негізгі куәландырушы орталығын қоспағанда, ҚРкуәландырушы орталықтары куәландырушы орталықтарды аккредиттеу қағидаларына сәйкес куәландырушы орталықты аккредиттеу жолымен әлемдік БҚ өндірушілер бағдарламалық өнімдерінің сенімді тізімдерінде танылады.

ҚР куәландырушы орталықтары шет елдердің аумағында Қазақстан Республикасы азаматтарының ЭЦҚ тексеруді қамтамасыз ету үшін өз тіркеу куәлігін ҚРсенім білдірілген үшінші тарапында орналастырады.

АКТжәне ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарды бекіту туралы

Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы № 832 қаулысынан үзінділер .