ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

АЛМАТЫ ЭНЕРГЕТИКА ЖӘНЕ БАЙЛАНЫС УНИВЕРСИТЕТІ

Байкенов Б.С. Оразалиева С.К.

АҚПАРАТ ҚАУІПСІЗДІГІ МЕН ҚОРҒАНЫС ҚЫЗМЕТІН ҰЙЫМДАСТЫРУ ЖӘНЕ БАСҚАРУ

Оқу құралы

Алматы 2014

УДК 004.384 (075-8)

ББК 32.973я73

Б18 Ақпарат қауіпсіздігі мен қорғаныс қызметін ұйымдастыру және басқару:

Оқу құралы/ Байкенов Б.С. Оразалиева С.К.; АЭжБУ. Алматы, 2012. – 68б.

ISBN 6978-601-7327-50-7

Оқу құралында ақпарат қауіпсіздігі мен қорғаныс қызметінің жұмысын талдауға байланысты негізгі ұғымдар келтірілген. Жүйелердің ақпараттық тәуекелдері мәселелері қарастырылған. Ақпараттың қауіпсіздік жүйесі үшін қауіптерді залалсыздандыру мәселелері талқыланады. Оқу құралы компанияның ақпараттық қауіпсіздігін қамтамасыз ету мәселелерін оқып үйренетін студенттерге арналған.

Кесте. 7, сур. 4 , әдеб. көрсеткіші- 9 атау.

УДК 004.384 (075-8)

ББК 32.973я73

ПІКІРБЕРУШІЛЕР: ҚазҰТУ, тех.ғыл.кан., доцент Н.А. Сейлова.

ҚазҰТУ, тех.ғыл.кан., ассоц. профессор Ж.Т. Жұмашева.

АЭжБУ, тех.ғыл.док., профессор Ш.А. Бахтаев.

Алматы энергетика және байланыс университетінің Ғылыми кеңесі басуға ұсынды (28. 01. 2014ж. №5 хаттама).

ISBN 6978-601-7327-50-7

Мазмұны

Кіріспе 4
1 Ақпараттық қауіпсіздік қызметінің жұмысы және мақсаттары 9
1.1 Кәсіпорынның ақпараттық қауіпсіздігі (АҚ) 9
1.2 Ақпараттық қауіпсіздікті қамтамасыз етудің негізгі бағыттары 11
1.3 АҚ қызметін ұйымдастыру мақсаттары және қағидалары 12
1.4 Ақпараттық қауіпсіздік қызметінің тиімділігін бағалау 14
1.5 Қауіпсіздік қызметінің жасалуы 14
2 Ақпараттық жүйелердің түгенделуі және жіктелуі 20
2.1 Ақпараттық жүйелерді түгендеу 20
2.2 Ақпараттық жүйенің (АЖ) жіктелуі 22
2.3 Субъекттерді жіктеу үлгісі 24
3 Физикалық рұқсатты бақылау жүйелері 29
3.1 Физикалық рұқсатты бақылау механизмдері 29
3.2 Потенциалдық бұзушының тәртіп моделі 30
3.3 Қарапайым қорғаныс моделі 32
3.4 Аймақты күзету жүйесі 34
3.5 Кіруге рұқсатты басқару жүйесі 35
4 Қауіпсіздік жүйесі шектерінде жұмысшылармен (персоналмен) және құрылғымен жұмыс жасау 38
4.1 Қызметкерлермен айналысу 38
4.2 Қызметкерлермен әдістемелік жұмыс 41
4.3 Кәсіпорынның бұрынғы кадрлық қызметкерлері 42
4.4 Құрылғымен жұмыс 42
5 Тәукелдерді басқару 44
5.1 Кәсіпорынның ақпараттық қауіпсіздігі мәселесі 44
5.2 Негізгі ұғымдар 46
5.3 Тәуекелді басқарудың жалпы әдістемесі 47
5.4 Сапалы бағалау моделі 48
5.5 Тәуекелдің сандық моделі 49
5.6 Миордың құндық нәтижелерінің жалпы моделі 51
5.7 Ақпараттық қауіпсіздік шығындары 54
6 Апаттық жоспар және келеңсіз жағдайда жұмыс істеу 57
6.1 Апаттық жоспар қағидалары 57
6.2 Апаттық жоспардың құрылымы 58
6.3 Апат жоспарының мысалы 60
7 Зерттеу жүргізу 62
7.1 Алдын алу шаралары 62
7.2 Мақсаттар және зерттеу есептерін анықтау 63
7.3 Жедел әрекеттер 64
Қорытынды 65
Әдебиеттер тізімі 68

Кіріспе

Құнды мәліметтерді қорғау мәселесі адамзат қоғамын ертеректен мазалады. Соңғы уақытта бұл мәселе көптеген кәсіпорын басшылары мен техникалық мамандарды мазалап отыр. Аз уақыт бұрын құнды мәліметтерді сақтаудың ең тиімді шешімі ретінде мыналар есептелді: құжаттарды өртенбейтін сейфке, одан дұрысы жауапкершілікті басқалардың мойнына жүктеп банк ұяшығына салу. Қазіргі уақытта ақпаратты сақтаудың ең сенімді тәсілі келесі түрде (қалжың): ақпарат бір ғана данада брондалған сейфте орналасқан компьютерде болуы керек және ол компьютер барлық желілерден ажыратылған болуы керек.

Қазіргі заманғы ақпараттық қоғамда ақпарат өте құнды. Ақпараттың нақты немесе потенциалдық иесі қандай да бір ұтыс алуға, материалдық, саяси, әскери және т.б. мүмкіндік беретін ақпарат құнды болады.

Ақпаратты алумен әр кезде арнайы қызметтегілер айналысатын. Соңғы жылдары бүкіл әлем арнайы қызметкерлерінің аз көлемдегі арнайы технологиялық ақпаратқа деген қызығушылықтары артып отыр. Бұл бірнеше фактормен байланысты. Бір жағынан, соңғы жылдары мемлекеттік инновация құны өсті және ірі корпорациялар зерттеушілік қызметке көп қаржы салуға мәжбүр.

Бір жағынан инновациялар жылдам ескіру қабілетіне ие. Сонымен бірге, алдыңғы қатарлы елдерде фундаментальды ғылым ірі бизнеспен тығыз байланысуда. Осының нәтижесінде инвесторларға экономикалық жағынан инновациялық қызметке емес, ондағы ақпарат алу жөніндегі инфраструктураға ақша салу тиімдірек.

Сарапшылар мәліметі бойынша, бүкіл әлемнің тыңшылары биотехнология, аэроғарыштық технология, телекоммуникация, компьютерлік технология және бағдарламалық қамтамасыздандыру, осы заманғы транспорттық жүйелер, алдыңғы қатарлы конструкциялық материалдар, энергетикалық өнімдер, жартылай өткізгіштер өндірісі сияқты салаларға көп қызығушылық танытып отыр.

ФБР мәліметтеріне сүйенсек, АҚШ-та өндірістік тыңшылық бабы бойынша жасалған қылмыс саны соңғы бірнеше жыл ішінде жасалған қылмыс саны 320 пайызға өсті. Өндірістік алаяқтықтың басты обьектісі саналатын технологиялық дамыған елдерде тыңшылардың экономикаға ауысуы ұлттық қызығушылыққа үлкен әсер етеді.

АҚШта арнайы қоғамдық бірлестік құрылды (Индустриалды қауіпсіздіктің Американдық қоғамы). Және де бұл қоғам осы тыңшылық актіден зардап шеккен үлкен американдық корпорациялардың жыл сайынғы санының артуын көрсетті. Тыңшылық ақпаратты алу мақсаттары әртүрлі сипатта болуы мүмкін. АҚШ ФБР-інің мұрағатында келесі оқиғалар тіркелген:

- оңтүстік кореялық тыңшылар байқаусызда американдық зертханаларда галстуктерінің ұштарын сұйықтыққа батырып отырған;

- қытайлық және жапондық тыңшылар кейбір цехтерде және ғылыми институттарда шаң үлгілерін алу мақсатында өздерінің аппақ қол орамалдарын жерге түсіріп алған.

Кейбір елдерде өндірістік тыңшылықтың нақты бейресми философиясы ойлап табылды. Жапонияда (авторлар қатарының пайымдауы бойынша) философия мынадай: он жыл және миллиард долларды зерттеулерге жұмсаудың не қажеті бар, осындай нәтижелерге бәсекелес фирманың инженеріне бір миллион пара беру арқылы тез әрі әсерлі түрде қол жеткізуге болады. Сол себепті, бизнес үшін өндірістік тыңшылық тек қана бәсекелестіктің бір түрі. Өндірістік тыңшылықтың субъектісі ретінде жеке кәсіпкер, фирма, яғни, жеке немесе заңды тұлға болып табылады.

Ақпараттың жойылуы апат және авария салдарынан болуы мүмкін.

Ақпараттық жүйенің пайда болуынан бастап қауіпсіздік мәселесі техникалық мамандарды қатты толғандыра бастады. Осыған байланысты мамандардың көмегімен осы саладағы құнды ақпаратты сақтау мақсатында ақпаратпен ауысу қағидалары ойлап табылды:

- ақпарат ақпараттық жүйеден тыс сақталған және бұзылған болып бөлінеді;
- резервті көшірмелер бір емес, бірнеше данада жасалады;
- резервті көшірмелер жасау кезінде сенімді ақпарат тасушылар қолданылады;
- резервті көшірмелердің сенімді сақталуы қамтамасыз етіледі. Алғашқы ақпарат тасушыдан алыста орналасқан бөлек ғимаратта;
- резервті көшірмелердің сапасы және олардың қайта қалпына келулігі үнемі бақылауда болады.

Ақпаратты қорғаудың негізгі қағидаларын қолдану кезінде шектен шығушылық болған бірнеше классикалық үлгі бар. Олардың нәтижесінде үлкен материалдық және моральдық мәселелер туындады. Олардың біреуі – барлық жүйелік әкімшілік оқулықтарында келтірілген мысал: Бүкіл әлемдік сауда орталығының ақпараттық жүйесінің алғашқы апаты негізгі серверлік ғимаратта сақталған мәліметтердің резервті көшірмесінің лентасы террористтік акт және кейінгі өрт нәтижесінде басқа серверлік құрылғылармен бірге балқып кеткен кезде орын алды.

Резервті көшірмелерді орындап жатқан кезде адам факторын ойламауға болмайды. Көп жағдайда фирма басшылары ақпараттық жүйенің сенімділігіне деген негізгі қажеттілігінің маңызын жақсы елестете алмайды. Және де осы жүйенің сенімділік деңгейін дұрыс анықтамайды. Жүйе сенімділігінің деңгейін анықтау кезінде келесі фактоларды ескерген жөн: мәліметтердің маңыздылығының деңгейі, жүйенің жұмыс жасауының уақыттық графигі және мүмкін болатын тоқтап қалу уақыты, резервтеу стратегияларының болуы, апаттық жауап бермеудің ықтималдығы, мәліметтерді қорғаудың жөніндегі алғашқы іс-шаралардың болуы (сервердің таза қоректенуі, сервер ғимаратының желдету жүйесі, осы ғимаратта су және жылу құбырларының

болуы, серверлік ғимаратта терезелердің болуы, көшірмелерді сақтауға жағдай жасалуы).

1 кесте – АҚ қызметі үшін бюджет статистикасы

Ұйым %	АҚ-ке қатысты АТ бюджетінің %
1-5	46
5-10	31
10-15	7
15-20	6
20-25	3
25-30	3
30-35	0
35-40	2
40-45	0
45-50	2

Ақпаратты қорғаудың сапасын жақсарту жөніндегі барлық маңызды шешімдер белгілі және міндетті ережелер ретінде көрсетілген, бірақ іс жүзінде бұл ережелер сақталмайды. Бұл шарттарда компания басшыларына ақпаратты жіктеу және өте маңызды ақпаратты бөліп көрсету қажет: өнім өндірісі технологиясына өте маңызды себеп, ғылыми зерттеу жұмыстарын өткізу, қаржылық операцияларды іске асыру және маркетингтік стратегияны жүзеге асыру. Бұл ақпарат сенімді қауіпсіздіктің кепіл болу керек. Және де компания басшылары қауіпсіздік қаупінің бар екенін әркез естен шығармай, оны қамтамасыз ету үшін барлық шараларды қодануы керек. Компания тыңшылық қызметтің, бәсекелестердің, қылмыстық ұйымдар немесе хакерлердің басты қызығушылық обьектісі болмаған жағдайда да бағындырған белестерді тұрақты түрде ұстап тұруға көмек көрсетеді.

Қазіргі кездегі өндірістік тыңшылықтың негізгі әдістерін екі негізгі топқа бөлуге болады: құрбан болу мақсатында фирмаға кіруді талап етушілер және ондайды талап етпеушілер. Бірінші топқа келесі әдістер: құпия мәліметтерге электронды рұхсат, кабельді желілерге жалғану арқылы тыңдау, офисте тыңдайтын аппаратураны орнату, ұялы телефон қоңырауларын тарту; желіге кіру арқылы компьютерлік жүйеге рұқсат алмай кіру, ақпараттық немесе жабдықтық қамтамасыздандыруды бұзу; құпия мәліметтерге қол жеткізу; жасырын визуалды бақылауларды, сурет немесе бейне түсірілімдерін қолдану; құжаттарда, сызбаларда, дискета немесе компакт дисктердегі ақпаратты ұрлау; «отырғызылған үйрек» әдісін қолдану (фирма қызметкерлерімен құпия ақпаратты алу мақсатында тығыз байланыс орната алатын әйел немесе ер кісі); фирма қызметкерлерін сатып алу; фирма қызметкерлерінің біліктілік деңгейін тексерген сыңай танытып, құпия ақпаратты алу.

Әдістердің екінші тобы тыңшылық техникаға жатпайды, яғни ол тек қана ресми қол жететін ақпаратты қолдану болып табылады.

Ақпаратты қорғаудың қажетті деңгейін қамтамасыз ету мәселесі өте қиын болды. Өз шешімін табу үшін жай ғана кейбір ғылыми, ғылыми техникалық және ұйымдастыру іс шаралары, арнайы әдістер мен құралдарды қолданудың қосындысы емес, ұйымдастырушылық іс шаралар жүйесін толығымен құру және ақпаратты қорғау үшін арнайы құралдар мен әдістерді қолдану болып табылады.

Қоғамдағы айналыстағы ақпарат көлемі тұрақты түрде өсіп келеді. Бүкіл әлемдік желі Интернеттің әйгілілігі соңғы жылдары ақпараттың әр жылда екі есе ұлғаюына септігін тигізіп отыр. Жаңа мыңжылдық қарсаңында адамзат ақпараттық өркениетті құрды. Ақпаратты өңдеу әдісінің жақсы жұмыс істеуінен адамзаттың амандығы және осы қалпында қалуы байланысты. Осы уақытта болған өзгрістерді келесі түрде сипаттауға болады:

- жарты ғасыр ішінде өңделетін ақпарат көлемі бірнеше есе өсті;
- белгілі мәліметтерге қол жеткізушілік айтарлықтай материалды және қаржылық құндылықтарды бақылауға мүмкіндік береді; ақпараттың құны бар, оны есептеуге де болады;
- өңделетін мәліметтер сипаты жағынан әртүрлі және де тек мәтіндік мәліметтер түрінде ғана емес;
- ақпарат түгелімен «жүзінен айырылды», яғни, оның материалды ерекшеліктері өзінің мәнін жоғалтты (өткен ғасыр хаты мен қазіргі замандағы электронды почтадан жіберілген жолдаманы салыстырыңыз);
- ақпараттық қарым қатынастардың сипаты өте қиындай түсті. Мәтіндік хабарламалардың рұқсат етілмеген оқылуы және бұзылуы сияқты қорғаныстың классикалық мақсатымен қатар ақпаратты қорғаудың жаңа мақсаттары пайда болды. Олар қолданылып жүрген «қағаздық» технологияның алдында тұрған және шешіліп жатқан мәселелері болатын, мысалы, электронды құжаттың астынан қол қою;
- ақпараттық процесстердің субъектілері ретінде тек адамдар емес, олардың өздерімен жасалған дайындалған бағдарлама бойынша жұмыс жасайтын автоматтық жүйелер;

қазіргі заман компьютерлерінің есептеу қабілеттері бұл уақытқа дейін өзінің жоғары қиындығына байланысты арман болып есептелген шифрларды іске асыру және аналитиктердің оларды бұзу мүмкіндіктері мүлдем жаңа деңгейге көтерілді.

1 Ақпараттық қауіпсіздік қызметінің жұмысы және мақсаттары

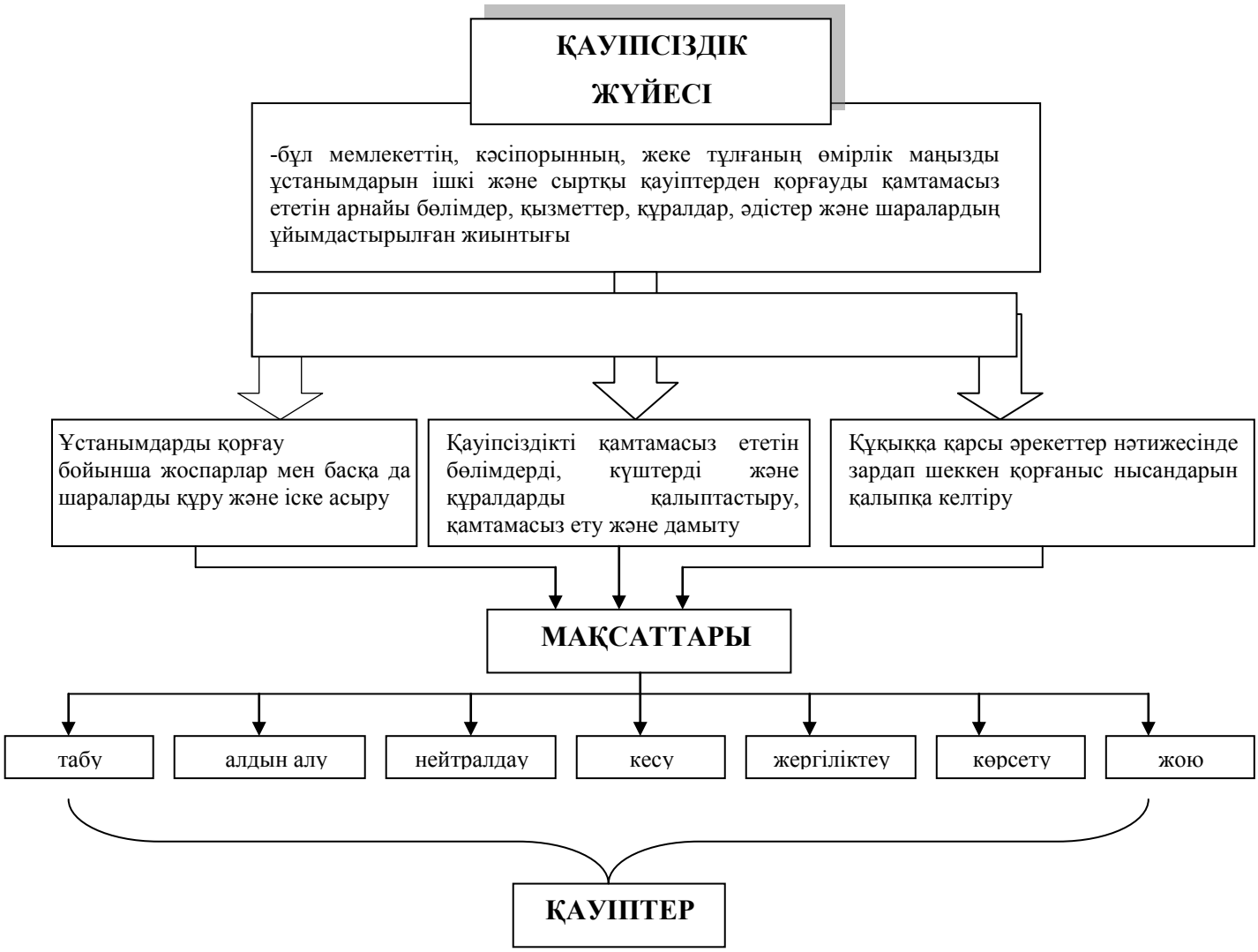
1.1 Кәсіпорынның ақпараттық қауіпсіздігі (АҚ)

1.1.1 АҚ мақсаты. АҚ-ның мақсаты келесі мәселелерді шешу үшін кәсіпорынды іс шаралар кешенімен қамтамасыз ету болып табылады:

- құпиялылықпен қамтамасыз ету – ақпаратпен (өлшемі емес, маңыздылығы бар мәліметтер) танысу мүмкіндігі тек қана құқығы бар адамдарда бар;
- бүтіндігін қамтамасыз ету – ақпаратқа өзгерістер енгізу мүмкіндігі тек қана құқығы бар адамдарда ғана болу керек;
- қол жетушілікті қамтамасыз ету – жұмыс уақытында арнайы құқығы бар адам қол жеткізе алу мүмкіндігі.

Бұл сұлбада шешілуі керек қосымша факторлар.

Ұйым ішінде қойылған мақсаттарға қол жеткізу үшін келесі баптар бойынша қосымша алдын ала келісім орындалуы керек:



1 сурет –Қорғаныс жүйесінің сұлбасы және қауіптер

- есеп, яғни, барлық рұқсат етілген әрекеттер жазылуы және болжануы қажет (яғни, бас штабта барлығы «қалың» дәптерде тіркелуі керек);
- бас тартпаушылық (егер ұйымда электронды ақпаратпен ауысу жүзеге асса), яғни, бір адамға ақпарат берген адам бұл фактіден бас тартпауы керек.

1.1.2 АҚ механизмі. Ақпараттық қауіпсіздік, кәсіпорын өмір сүруінің бір мақсаты ретінде, қамтамасыз етіледі, егер белгілі шарттардың барлығы орындалса (қағидалар немесе механизмдер). «Бас штаб және оған сәйкес барлау басқармасы» келесі механизмдерді қолдануын қарастыруы тиіс:

- идентификация – АҚ түсінігі қолданылмас бұрын ақпараттық қарым-қатынастың әрбір қатысушысын тану;
- аудентификация – әрбір қатысушының көрсеткен идентификатор иесі екендігіне сенімділік қамтамасыз ету;
- қол жеткізушілікті бақылау – әрбір қатысушыға қол жеткізушілікке рұқсат және қол жектізушілік деңгейін анықтайтын ережелерді ойлап табу және қолдау;
- авторизация – бақылау ережелерінен ақпараттық ауысу құқығының тұрпатының қалыптасуы;
- аудит және мониторинг – барлық іс шараларды күнделікті бақылау;
- жайсыз жайларға назар аудару – АҚ-ның бұзылуы кезінде болатын барлық іс шаралардың қосындысы;
- конфигурацияны басқару – АҚ талаптарына сәйкес функционалды ортаны сақтап отыру;
- тұтынушыларды басқару – ақпараттық ауысу ортасында тұтынушыларға жұмыс жағдайымен қамтамасыз ету;
- тәуекелділікті басқару және тұрақтылықты сақтаумен қамтамасыз ету – АҚ-ның істен шығуына байланысты мүмкін болатын жоғалтулар және қауіпсіздік құралдарының қуаты арасындағы сәйкестікті қамтамасыз ету (оларды құруға кеткен шығындар).

1.1.3 АҚ құралдары. Жоғарыда айталған механизм іске асуы мүмкін болатын құралдарды қарастырайық. Және де «тауар неғұрлым жақсы болса, оның бағасы соғұрлым жоғары» дегенді есімізден шығармайық (біздің жағдайда құрал-сайман неғұрлым қымбат, соғұрлым жүйеміз берік):

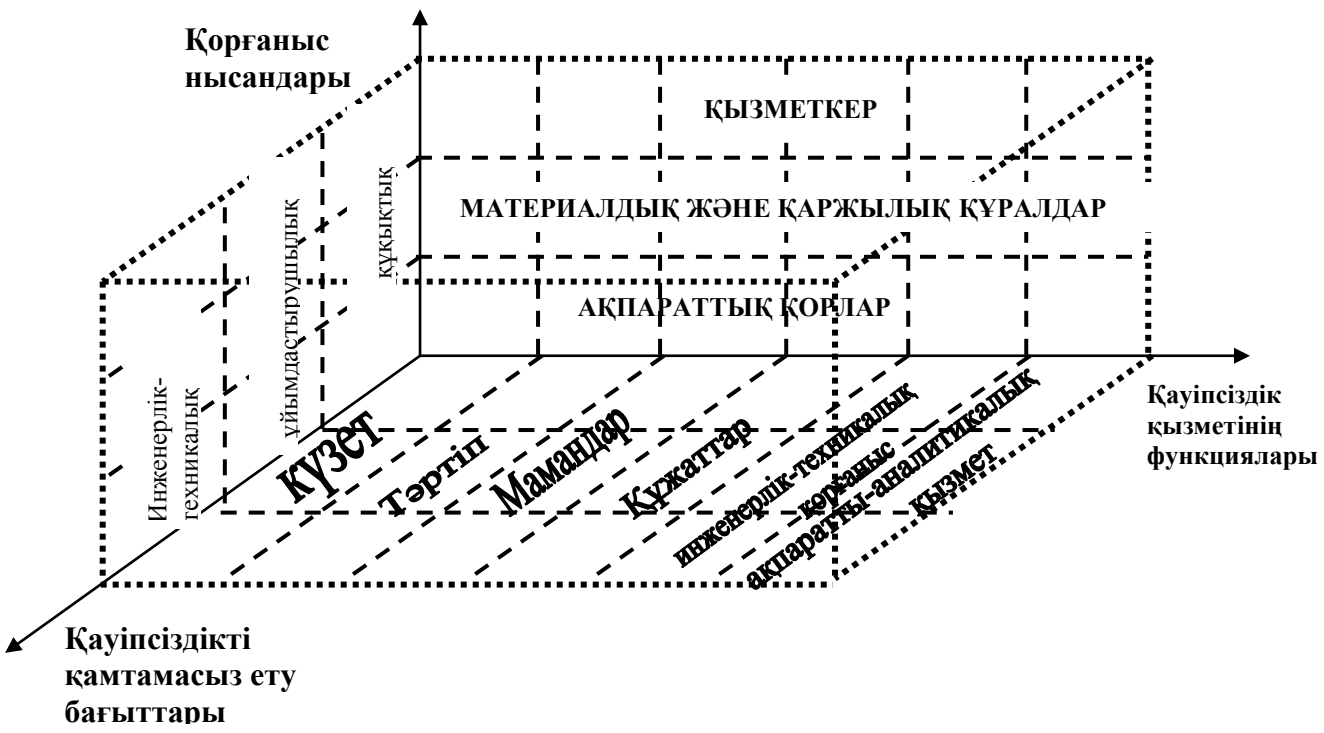
- қызметкер – АҚ-ны өңдеу жолымен, орналастыру, қолдау көрсету, бақылау және орындауды қамтамасыз ететін адамдар;
- құқықтық жазықтықпен қамтамасыз ететін нормативті қамтамасыздандыру (құжаттар);
- қауіпсіздік модельдері – берілген нақты ақпараттық жүйеге орналастырылған сұлбалары және АҚ-ның қамтамасыздандыру механизмдері.

Қауіпсіздік модельдері келесі элементтерден тұруы мүмкін:

- криптография – ақпаратты рұқсат етілмеген амалдарды орындауға қиындық туғызатын түрлерге түрлендіру әдістері мен құралдары;
- желі аралық экрандар – бір ақпараттық желіден екіншісіне өтуді бақылау құрылғысы;

- антивирустық қамтамасыз ету – қауіпті кодты анықтау және жою үшін қолданылатын құралдар;
- қауіпсіздік сканерлері – қауіпсіздік моделінің сапасын бақылау құралы;
- шабуылдарды табу жүйесі – ақпараттық ортада белсенділік мониторингінің құралы;
- резервті көшірме резервтеу – ақпараттық қорлардың артық көшірмелерінің сақталуы;
- қайталау (сақтау) - талғаулы құрылғылардың жасалуы;
- апат жоспары - егер оқиға ережеде көрсетілгендей емес, басқаша пайда болғанда қолдануға арналған шаралардың жиыны.
- қолданушыларды үйрету – АҚ-ті қамтамасыз ету шарттарында жұмыс істеуге арналған ақпараттық ортаның белсенді қатысушыларын әзірлеу.

АҚ үлгілерін көрсететін тағы да басқа жолдар болады. 1.2 суретте сондай үлгі көрсетілген.



2 сурет – Қауіпсіздік қызметі нобайының сұлбасы

1.2 Ақпараттық қауіпсіздікті қамтамасыз етудің негізгі бағыттары

Бұл бағыттардың бар болғаны екеу:

- физикалық қауіпсіздік;
- компьютерлік қауіпсіздік.

Физикалық қауіпсіздік - ақпараттық ортаны функционалдауға арналған құрылғының өзінің қолайлылығын қамтамасыз ету, осы құрылғыға

адамдардың рұқсатын бақылау. Бұдан басқа, мұнда қаскүнемдердің физикалық әсерінен ақпараттық ортаның қолданушыларын қорғау ұғымы, сонымен қатар виртуалды емес сипаттағы ақпараттарды қорғау жатады (қатты көшірмелер, қызмет телефоны, анықтамалар, бұзылған сыртқы сақтаушылар, қызметкерлердің мекен – жайлары).

Компьютер қауіпсіздігі (желілік қауіпсіздік, телекоммуникациялық қауіпсіздік, мәліметтердің қауіпсіздігі).

Компьютер қауіпсіздіктерін қамтамасыз ететін адамдардың көзқарасынан келесілерді ерекшелеуге болады:

– мәліметтердің қауіпсіздігі қызметі;
– желінің қауіпсіздігі қызметі.

1.3 АҚ қызметін ұйымдастыру мақсаттары және қағидалары

Сізге жаңа кәсіпорынның қауіпсіздік қызметін ұйымдастыру тапсырмасы берілді делік және бұл салада осы тапсырманы сізден басқа ешкім орындай алмайтын болсын.

Ақпараттың қарастырылатын бір бөлігі қызмет құрастыруының бюрократтық процестері үшін немесе осы қызметтерді дамыту стратегиясымен шұғылданатындар үшін "жеп отырған наны" болып табылады. Ең алдымен талдау қажет, мүмкін сұрақтардың келесі топтарын ерекшелейік:

– қауіпсіздік қызметін қайда орналастыру (қабат, қажетті аумақ);
– оның басқа қызметтермен өзара әрекеттесуі;
– бағыну иерархиясы.

Бұл сұрақтардың жауаптары бойынша көптеген ұсыныстар бар. Қатты регламенттеулердің болуы мүмкін емес, кәсіпорынның ішкі құрылымының құрастырылуына байланысты жауаптарды құрастыра аламыз және оларды келесі сұрақтарға жауап беру арқылы да ала аламыз.

Қауіпсіздік қызметі (ҚҚ) немен айналысуы керек?

– қауіпсіздіктің бар құралдарын басқару (тораралық перделер, антивирустік пакеттер, шабуылдарды табу жүйесі);
– ақпаратты қорғаудың сұлбалары мен үлгілерін ойлап табу, жаңа құралдар сатып алу;
– ақпараттық кеңістіктің қолданушыларының жұмысын басқару;
– ҚҚ-ның негізгі назарын қайта бағыттауды анықтау – ішкі қолданушыларға ма, әлде сыртқы кеңістіктің рұқсатынан қорғауға ма.

Бұл есептер әр кәсіпорында әртүрлі шешілуі мүмкін: есептердің бір бөлігі жұмыстың ортақ стратегиясында ескеріледі, ал қалғаны ҚҚ-ның жұмысында ерекшеленеді. Жоғарыда құрастырылған бұл сұрақтарға жауап беру үшін, жұмысты ұйымдастырудың әртүрлі жолдарын, сонымен қатар қарастырылып отырған жолдарға сәйкес кемшіліктерді қарастырайық.

Желі және жүйенің администрациясы әсер еткен кезде қандай нұсқалар бар болады?

– әкім жүйесінің құқығымен тең АҚ мамандары ақпараттық жүйенің үстінен толық бақылай алады;

– жүйені әкімшіліктеу кезінде АҚ мамандары жартылай қатыса алады, мысалы, қолданушылардың құқықтарын баптауда;

– АҚ мамандарының барлық нысандарға арналған рұқсаты болады, бірақ тек қана олар туралы мәліметтерді оқып отыруға ғана құқығы бар;

– АҚ мамандарының жүйеге рұқсаты болмайды, олар бақылау үшін тіркеу журналын, конфигурацияны, есептеу нәтижелерін және т.б. қолданады.

АҚ сұрақтары бойынша шешім қабылдаудың неше баспалдағы болуы керек?

– Егер АҚ қызметінің жетекшісі кәсіпорынның директорына тікелей бағынса және шешімдердің жобаларын тікелей енгізсе, онда бұл өз жағдайын теріс пайдалану мүмкіндігін береді (өйткені топ-менеджер ақпараттық технологияларда онша құзырлы емес және "қауіпсіздік" деген сөзге құжаттарға дереу белгі соғады).

– Егер шешім қабылдау жетекшілер бойынша тым бөлініп берілсе, онда тіршілікке маңызды шешімдер үлкен кешігумен қабылданады деген тәуекел болады. Осы жағдайда, мамандарымен қатар жетекшілері де болатын қауіпсіздік бойынша комитетке ҚҚ бағындыру орынды болып табылады.

Ақпараттық жүйелердің қамту аумағы қандай?

Бұл сұрақты басқаша да құрастыруға болады: ҚҚ-ның басқа да бөлімшелерін ерекшелеуге бола ма? Қызметті екі бөлімшеге бөлуге болады:

– қолданбалы қауіпсіздіктің бөлімшесі;

– жүйелік қауіпсіздіктің бөлімшесі (яғни осы жүйенің басқалармен өзара әрекеттесуі кезіндегі қауіпсіздік).

Сонымен қатар келесі мәселелермен қай бөлімшелердің айналысатынын да ойлану керек:

– кім телефон байланысы қауіпсіздігі жайлы сұрақтарды ұйымдастырады және жоспарлайды (ұялы байланыс, мини-АТС, факс)?

– кім кәсіпорынның қағаз есептеу нәтижелерін жою жайлы сұрақтарды және электр энергиясы көзін қорғау жайлы сұрақтарды ұйымдастырады және жоспарлайды?

Қызметкерлерді қамту аумағы қандай?

Ол барлығын қамту керек, бірақ барлығы үшін талап бірдей бол ма? Мысалы, электрондық поштаның хаттарына рұқсат. Бұл жерде мынандай сұрақ туындайды, ҚҚ-ның уәкіл қызметкерлері кәсіпорын қызметкерлерінің, соның ішінде жетекшілердің де электрондық поштасын қарауына бола ма? Бұл даулы сұрақ, және осы мәселе байланысты ортақ ережелерді бұзбас үшін,

келісім шарт болу керек. Негізінде ҚҚ-да жұмыстан шығару, жұмысқа қабылдау, демалыстар жайлы ақпарат болу керек.

Жобалардың қамту аумағы қандай?

Ұйым немесе кәсіпорынның мәліметі бойынша жобалардың өзгертілуі кезінде ҚҚ қатысу керек. Сонымен бірге АҚ бойынша әрбір жаңа есеп қосымша заттық және адамдық қорларды талап етеді.

1.4 Ақпараттық қауіпсіздік қызметінің тиімділігін бағалау

Бұл сұрақ ерте ме, кеш пе әйтеуір басқарушыларды қызықтыруы тиіс. Егер де АҚ қызметімен әрқайсысының қаупі 20 мың доллар потенциалдық қауіпі бар 10 шабуыл жасалатыны туралы дәлел көрсету мүмкін болғанда, онда қорытындылар түсінікті болар еді. Ал егер де ешқандай жайсыз жайлар болмаса ше?

ҚҚ-ның нәтижелік бағасы әдісінің бірі тәуекелдерді басқару технологиясына негізделген.

АҚ қызметінің жұмысын басқарғысы келетіндерге ең алдымен кәсіпорынның құрылымымен және ондағы ҚҚ-ның алатын орнымен танысуы қажет. Және де басқару кезінде жоғарыда сипатталған сұрақтарға жауап беруге тиіс: ҚҚ қандай құрылым шеңберінде жұмыс істейді, ақпараттық жобаларды жасауға араласада ма, дәрежені қалай басқарады және т.б.

1.5 Қауіпсіздік қызметінің жасалуы

Қызметті жасау қажеттілігінің белгілері. Бұл қызмет қажет болатынын уақытты қалай анықтаймыз? Бұл көптеген себептер мен шарттарға байланысты, мысалы, бірінші кезең келесі баптардың үйлесімділігімен анықтала алады:

– сіздің ұйымыңызда әртүрлі бөлмелер бойынша таралған компьютелер саны 10-нан көп;

– сіздің ұйымыңыз жергілікті жүйеге қосылған;

– сіздің ұйымыңыздағы компьютердің біреуі модеммен жалғанған;

– сіздің компьютеріңізде таралуы залал әкелетін ақпарат сақталған.

Неге жоғары да аталған пунктің кез келгені назар аударуды талап етеді?

а) егер компьютерлер көп болса, онда ол жабдықтың сақталуы туралы ойлану керек. Қолда бар бағалар бойынша, компьютерлік құраушылар қатарының салмақ/баға қатынасын алтынның салмақ/баға қатынасымен салыстырайық. Бұл демек, олар өздерін қаскүнемдерге арналған нысана ретінде көрсетеді. Мысалы, қылмыстың бір үлгідегі сценарийін көрсетуге болады: жедел жадтың 128 немесе 256 М/байтының жартысы (немесе 1/4) ұрланады. Қызметкерлердің көпшілігі компьютерді қоскқанда жүктелетін процесті қадағаламайтыны және жедел жадтың қысқартылғанын анықтауға

қабілетсіз болатыны айдан анық. Егер тек қана мерзімді уақытта қосылатын компьютерлер болса, онда мұндай жоғалуды біраз күн өткеннен кейін ғана анықтауға болады.

б) Егер сізде жергілікті жүйе пайда болса, онда бұл сіздің компьютерлерді өндірістік процесте пайдаланғаныңызды білдіреді. Сіздің желіңізде ешқандай да маңызды мәлімет жоқ деп болжайық. Егер қызметкерлердің біреуі қарақшы дисктен ойынды өз компьютеріне іске қосқан кезде сіздің компьютерлеріңіздің ешқайсысы басқару жүйесіндегі ақау салдарынан қосыла алмаса, сіз өзіңізді қалай сезінер едіңіз?

в) Сізде модем пайда болса – онда оны компьютерлердің біреуіне бірден қосып көреді. Сіздің қызметкерлеріңіздің біреуі өз баласына үйіне компьютер сатып алсын делік және ол хакерлік файлдары бар программа жүктеп алсын. Бұл кезде де жағдай тура алдыңғы жағдайда сипатталғандай болады.

г) Сіз өз компьютеріңізде өте маңызды мәліметті сақтадыңыз (жалпы тіпті ол жергілікті желіге де қосылмаған) және ол мәлімет қорғалып тұр деп ойлайсыз, өйткені сіздің компьютеріңіз құпия сөзбен қорғалған, ал компьютеріңіз сіздің дербес кабинетіңізде орналасқан болсын. Ал, құпия сөз - бұл, сіздің үй телефоныңыздың нөмірі емес пе?

Егер сіз бұл сұрақтар жайлы ойланған болсаңыз, демек сіз тиісті қызмет құруға немесе олармен айналысатын қызметкерлерді жалдауға дайынсыз.

Ақпараттық қауіпсіздік қызметінің құрамы.

"Нөлден" мұндай қызметті қалай жасауға болады және оның құрамына кімдер кіру керек? Әрине, бұл сұрақтарға жауап ұйымның өзіне, оның мақсаттарына, шарттарына және тағы басқа факторларға тәуелді болады. Үлгі ретінде сипатталатын есептері және АҚ қызметінің әртүрлі жұмысшылары арасында үлестіріліп бере алатын функциялары бар барынша үлкен кәсіпорын қарастырылады. Сыпайы серіктестіктер үшін әртүрлі рөлдер қызметкерлердің кіші санымен немесе біреуімен біріктірілуі мүмкін.

1 кесте – АҚ қызметінің сертификациясы

Квалификациялық жеке куәлік	Орташа, %	Азиялық-Тынық мұхиттық аудан,%'	Еуропа, Шығыс, Африка %	Американдық континент, %
АҚ қауіпсіздігі бойынша сертификацияланған маман	8	3 3	8 8	14
«Ақпараттық қауіпсізідк» мамандығы бойынша университет дипломы	5	4 4	5 5	7

1 кестенің жалғасы				
Қорғау өнімдірін шығарушының сертификациясы	7	6 6	8 8	7
Басқа да құжатар	7	3	9	8

Қызметтің құрамы.

Жекеменшік қызметтің *жетекшісі* болу керек – оның ортақ стратегиясы мен тактикасын анықтау, басшылыққа есеп беру, жедел шешім қабылдау және олар үшін жауапкершілікте болу үшін керек. Бұл маман өте даярланған болу керек және ол міндетті:

а) қолданылатын ақпараттық қамтамасыз етудің техникалық ерекшеліктерінің ортақ сипатын білу керек (аппараттық және программалық қамтамасыз етулерді, кәсіпорынның ақпараттық кеңістіктегі қабылданған жұмыстың де-юре және де-факто әдістемесін). Әйтпесе ол өзінің қол астындағылардың не істеп жатқанын түсінбейтін болады, ал олар өз кезегінде жетекшілерін қолданатын болады;

б) көптеген қауіпсіздік механизмдердің енгізілуі жобалық жұмысты қажет еткендіктен жобаларды басқару және қадағалау функцияларын формализацияланған функциялар ретінде қолдану (мысалға, техникалық шешімдерді қабылдау және енгізу сияқты);

в) қызметкерлердің психологиясын білу, дауларды шеше білу керек (өйткені ҚҚ- ның өзі жиі жазалау немесе шектеуші әсерге арналған негізбен қызмет етеді). Ұйымдағы қызметкерлердің әлсіз немесе күшті жағын қолдануы да мүмкін;

г) қазіргі заңның негізін білу. Мүмкін, "Мәліметке деген жеке меншік", "Айғақ және дәлел", "куәлік қағаз" және т.б. құқығы бар ұғымдары бар тергеу жүргізуге тура келеді;

д) басқа да ұйымдардағы әріптестерімен байланысты түзету, соның ішінде тиісті салаға сәйкес өз серіктестігінің мүдделерін қорғайтын жоғарғы ұйымдармен де;

е) басқарушылардың сеніміне кіру , өйткені қалаған кезде мынадай жағдай құруға болады, ҚҚ да көп нәрсе түйық болғанда ҚҚ-ның жетекшісі өзінің дәрежесін өзінің жекебасының қызығушылығына қолданатындай мүмкіндік береді. Жоғарыда айтылған "Тамаша" жетекшілердің қол астындағылары әртүрлі мүмкін белгілер бойынша жиналған мамандар болады. Ең алдымен олар орындауға тиісті функциялардың сипатын ескеру керек:

– Операциялық. Мұндай желі мониторингі және жеке сервистердің (қосымшалардың) күнделікті шараларын орындау, қолданушылардың нұсқаулығы және тіркелуі, шараларды орындауды бақылау (мысалы, резервті көшіру) тергеулерді өткізуді және т.б. жатқызуға болады.

– Зерттеу. Жалпы дүниеде ең жақын ақпараттық кеңістіктің ағымдағы жағдайын, жаңа мүмкіндіктер және осалдықтарды талдау осыған кіреді.

– Әдістемелік. Функцияларының осы жиыны бірінші және екінші функцияларды өзара байланыстырушы болып табылады. Технологияларды енгізу бойынша бітірілген жоба ескілікті іс күн сайынғы жұмыс жасаудың тәртібіне орнату керек, яғни тиісті процедуралармен, реттермен, нормативтік және техникалық құжаттамамен қамтамасыз ету керек. Бұл топтар тәуекелдерге талдау да жасай алады.

Жетекшілер және мамандар таңдалғаннан кейін, жұмысты бастай беруге болады, дұрысы - жұмысқа әзірлікті бастай беруге болады. Сонымен бірге мыналарды анықтау керек:

– сіздің қорғауыңыздың стратегиясы және тактикасын;
– сіздің қалай қорғайтыныңыз және неден;
– ол үшін қажет құралдар;
– қажетті нормативтік кеңістік.

2 кесте – ҚҚ мәселелеріне жетекшілерді енгізу дәрежесі

Ұйым қызметінің бағыттары	Енгізу дәрежесі, %
Қаржы саласы	60
Өндірістік және сауда саттық	43
Коммуникация және қызмет саласы	52
Мемлекеттік сала және инфрақұрылым	42

Мамандардың әзірлену деңгейі.

Жетекшілер және қызметкерлердің оларға жүктелген есептерді орындауда жеткілікті дайындалған дайындалмағанын қалай анықтауға болады?

Білікті қызыметшілермен қамтамасыз ететін қызмет орындарына маман тәжірибесін сұрау туралы кеңес бере аламыз. "Information security" кілттік сұранысы арқылы жұмысқа орналастыру бойынша бірнеше ірі агенттіктерге кіріп-шығу жеткілікті (мысалы, олардың интернет сайттары) және де кандидаттарға қойылған талаптардың тізімінен "CISSP preferred" деген тіркесті жиі байқауға болады.

Бұл сөз Information Systems Security Certification Consortium, Ins (Ақпараттық қауіпсізік облысындағы сертификация бойынша Халықаралық консорциум) деген, АҚ мамандарын серитификациялаумен және тестілеумен айналысатын арнайы ұйымның атауын білдіреді, ал CISSP - бұл Certified Information Systems Security Professional (Ақпараттық қауіпсіздік

облысындағы сертификацияланған маман). Сертификация жүргізілетін басқа бір категория, ол - SSCP - Systems Security Certified Practitioner (жүйелердің қауіпсіздігі бойынша сертификацияланған тәжірибеленуші маман).

Тестілеу жүргізілетін тізімді қысқаша қарап шығайық:

- рұқсат етуді басқару жүйесі, әдістеме;
- телекоммуникациялар және желілік қауіпсіздік;
- қауіпсіздікті тәжірибелік басқару;
- қосымшалар және жүйелерді өңдеудегі қауіпсіздік;
- криптография;
- архитектура және қауіпсіздіктің үлгісі; операциялардың қауіпсіздігі;
- өндірістік қызмет жалғасының жоспарлануы және апаттан кейін қайта құру;
- тергеуді өткізудегі заңдылық және әдеп;
- физикалық қауіпсіздік.

Мамандарды таңдау: теория және практика.

Осыған орай, маманында сертификаттың бар болуы, теориялық тұрғыларда көрсетілген тақырыптың меңгергені, емтихан тапсыра алғанын білдіреді. Ол дайындалмаған маманға қарағанда, практикалық сұрақтардың шешімін қажетті әдебиеттер, уақыт және техникалық базада қарастыруға мүмкіндік береді. Негізінен, мұндай теориялық білімдер тәжірибелерден ерекшеленеді, мысалы, жағдайды қиын түсіндіретін, біліксіз қолданушының сөйлесу кезіндегі мәселелердің маңызын түсіну қабілеттілігін қосады.

Мамандарды жеткілікті бағалау белгілері келесі екі факторлардың бар болуымен қызмет көрсете алады:

а) осы облыста сертификаты бар– бұл теориялық білімдердің растауы;

б) қажетті салаға сәйкес тәжірибелік жұмыстағы қызметі жайындағы құжат.

4 кесте – Әртүрлі мекемедегі АҚ қызметінің жұмысшылар саны

Жұмысшылардың жалпы саны, адам	АҚ қызметіндегі адамдардың орташа саны
< 1000	4,89
1001-10 000	9,38
10 000- 50 000	20,76
>50 000	39,21

5 кесте – АҚ штат қызметіндегі сату көлемі

Сату көлемі, млн. долл.	АҚ қызметіндегі адамдардың орташа саны
50-100	5,5
101-500	10,02
> 500	20,55

Мамандарды таңдау процесін бақылау.

Бөлімнің мазмұны, арнаулы штаттарды, қызметшінің қателерін, ұрлықтар, алаяқтық немесе қорлардың заңсыз қолдануының белгісін кішірейтуге бағытталған. Бұл бөлім ендігәрі бөлімдер және ақпараттық қауіпсіздіктің қызметтері үшін қолданушылар және басшылыққа алынатын құжаттардың лауазымды нұсқауларын құрастыру үшін қолданылады. Бұл құжаттарға келесі тармақтарды қосу керек:

- қызыметшінің жұмысқа қабылдауының тексеру ережелері;
- ақпараттық қорларға қарағанда міндеттер және қолданушылардың құқығы;
- қолданушылардың ақпараттық қорларына міндеті мен құқықтары;
- қолданушылардың оқуы мен ақпараттық қорларының жұмысына жіберілу тәртібі;
- әкімшіліктің құқығы мен міндеті;
- төлемдерді салу міндеті.

Алғашқы бірнеше тармақты қарап шығу. Бірінші тармаққа мінездемені қабылдау жөніндегі ереже, қажетті құжаттар, түйіндеме формасы, ұсынулар және тағы басқалары кіреді. Одан басқа, әртүрлі дәрежедегі жұмысшылармен тәртіп мен форма жөнінде әңгімелесу туралы анықталады.

Екінші тармақта қолданушылардың өз жұмыс орнындағы қызмет көрсетуі бойынша міндеттері мен ақпаратты қорлармен жұмыс істеуі суреттеледі. Бұл тармақ үшінші тармақпен тығыз байланысты, өйткені қолданушылардың қажетті білімдерін анықтайды.

Үшінші тармақ әртүрлі дәрежедегі жұмысшылардың қажетті білімдерін анықтайды, ақпаратты қорларды қолданудағы нұсқаудың өткізу тәртібі: (вирусқа қарсы базалары, программалар пакеттері бар жұмыс және тағы басқа жүйелерін теңестіру, құпия сөздің ауысымы және т.б.). Бұдан басқа, қосылу тәртібі суреттеледі.

2 Ақпараттық жүйелердің түгенделуі және жіктелуі

2.1 Ақпараттық жүйелерді түгендеу

2.1.1 Ақпараттық жүйелерді хаттаудың ортақ мезеттері. Түгендеу – осы жағдайда жүйелердің тізімінің құрастыруы, яғни ақпараттық кеңістік мәлімет іске қосылған субъекттердің қорғауларына жататын, және жүйенің ақпараттық қорғауларына ықпал ететін объектілер. Осыған орай, тізімді жай құрастырмай, жүйенің басқа да ерекшеліктер қатарын көрсету, яғни АҚ көзқарасымен қысқаша сипаттау. Бастапқы кезеңдегі бұл бөлімді қаншалықты толығырақ жасасақ, соншалықты өндіруді анықтау және қорғау үлгісі жеңілдеу болады. Жұмыстың осы бөлігі әдетте ҚҚ-да басталады, бірақ басқа қызметтердің мамандарының тартуымен орындалады. Бұл жүйенің әкімі немесе оның белсенді қолданушылары желінің үлгісінің жұмысы туралы білімдермен толығырақ ие болатынына байланысты. Мұндай түгендеуді өткізудің әдістері әртүрлі бола алады. Маманға өз нұсқасын меншікті жасауға мүмкіндік беретін мысал.

Түгендеуді өткізудің қағидалары:

- объективтіктің қағидасы – нысанды шектік талдау кезінде АҚ бағалау тұрғысынан қарастыруды білдіреді;
- көп деңгейлік қағидасы – нысанды бірнеше құрама бөліктерге бөлу арқылы қарастырады (аппаратты қамтамасыз ету, программалық қамтамасыз ету және тағы басқалар);
- түйісу қағидасы – ақпарат қандай жүйелерден берілгенге келіп түседі және берілгеннен қандай жүйелерге бағытталатынын білдіреді.

Түгендеуді өткізудің бағыттары:

- физикалық – жүйенің географиялық орналастыруын суреттейді;
- технологиялық – қолданылатын техникалық құралдарды суреттейді;
- функционалдық – өндірістік процестегі жүйенің орынын және атқарылатын есептерін суреттейді;
- ұйымдастыруышылық – жүйе және оның міндетінің жұмысы іске қосылған қызыметшіні суреттейді;
- нормативтілік – жүйенің жұмысын регламенттейтін құжаттарды суреттейді;
- ақпараттық (мәліметтер ретінде) – жүйе жұмыс істейтін мәліметтің өндірістік немесе іскерлік сипатын суреттейді.

Осындай тексерулерді өткізу келесі сұлба бойынша іске асады:

- жүйемен ортақ танысу, нақты орналастыруды көз мөлшерімен тексеру, және жеке компоненттер;
- жүйенің жұмыс жасауының бағыт-бағдары туралы әкіммен алдын ала әңгімелесу;

- ақпараттық жүйе бойынша құжаттармен танысу және АҚ тұрғысынан жүйенің сипаттамасын құру;

- құжаттар және шақырылған мамандармен жұмыс істеу негізінде жүйенің сипаттамасын.

Келешекте сапалы жұмыс істеу үшін көрсетілген сипаттамаларды мысалы, келесі параметрлер бойынша жақсылап құрамдастыру қажет:

- ақпараттық жүйенің жабдықтық қамтамасыз етілуі (компьютерлер, модемдер, көпірлер, қайталауыштар және т.б. енгізу-шығару құрылғылары);

- желілік қамтамасыз ету (желілік кәбілдер, ажыратқыштар, коннекторлар тағы сол сияқтылар);

- жүйелік бағдарламалық қамтамасыз ету (операциондық жүйе, резервтік көшірме бағдарламасы, немесе ДҚБЖ);

- қолданбалы бағдарламалық қамтамасыз ету, яғни өндірістік, көмекші және өндіріске қатысты функцияларды орындайтын бағдарламалар;

- ұйымдастыруды қамтамасыз етуі, яғни жүйенің пайдаланушылары немесе субъектілері және олардың жүйедегі қызметтік міндеттері;

- нормативтік қамтамасыз етуі – жүйемен жұмыс жасау ережелері және нұсқаулықтары;

- мәліметтер – оның өндірістік мәніндегі жүйенің жұмысында қолданылатын ақпарат.

Бұдан басқа қорғауға жататын жүйенің жеке объектісі деп нені санауға болатынын анықтау қажет? Жеке компьютер әлде жеке логикалық модуль ма? Мысалы, егер (клиент - қосымшалардың сервері - мәліметтердің сервері) үш архитектурасы бар жүйені мысал ретінде алса, онда жіктелу әртүрлі бола алады. Біртұтас объектпен барлық жүйеге есептеуге болады, әрбір буынды (үш объект) бөлек қарауға болады.

2.1.2 Түгендеудің басталуы. Қауіпсіздік бойынша маманның өз күштеріндегі күшті бағытының жанында осалдықтар және байбаламдардың жүйелерінің қолданушылары үшін анық болмайтын және бола алатын есептеу нәтижесін жұмыста толық емес оңай қолдануға тәуекел етеді. Мысалы, қорғауы құпия сөз бойынша авторландырумен және рөлдердің үлестірілуі бар рұқсатты бақылауға негізделген жүйе сипатталған. Құпия сөзді пайдалану жүйесі, XYZ- деңгей бойынша сертификатталған, барынша сенімді. Ортақ қорытынды – жүйе жеткілікті сенімді. Бірақ та, құпия сөзді жүйенің пайдаланушысы өзі таңдамайды, оған оны әкім тағайындайды, және сонымен бірге құпия сөзді нысанның бөлімше бастығына да хабарлайды. Мұндай жүйе жеткілікті сенімді ме? Жауап көп факторларға тәуелді болады.

Егер АЖ тізімін жай ғана санап шықсақ және менеджерлерге, қолданушыларға оның айқындығын берсе, керекті мөлшерде мәліметтер алуға болады, тек қажетсіз. Мысалы, кәсіпорынның кілттік есептемелерін сақтау жүйесі бойынша мәлімет керек болсын. Менеджерлер сипаттама ретінде есептеу нәтижелерін, экрандық формалардың барлық түрлерін, рұқсаттың жылдамдығын және тағы басқалар туралы мәліметті ала алады, бірақ

қауіпсіздіктің ішкі жүйесінің жұмысы барлық схемада өте күрделі екенін көрсетеді. Сондықтан, түгендеуді бастамас бұрын тексеру ретін және әдістемесін құрып, келісіп және бекіту қажет. Бұл құжатта тексеруді өткізудің мақсаттары мен қағидалары келтірілуі керек, себебі процеске қатысушылар үшін мөлдір болуы керек. Кәсіпорын басшысымен түгендеу жүргізетін қызметтің өкілеттігін және қатысушылар тізімін бекіту керек.

Құжаттың әдістемелік бөлігінде өз жұмысын орындау үшін тартылған мамандарға жасауы керек болатын жұмыстар сипатталуы керек. Құжатты қосымша ретінде сауалнамамен толықтырған жөн болар.

2.2 Ақпараттық жүйенің (АЖ) жіктелуі

АЖ-нің жіктелуі мақсаты келесілерге тіреледі:

- нысандар – кәсіпорын үшін олардың маңыздылығының дәрежелері бойынша;
- мәліметпен жұмыс жасайтын құралдар – олардың АҚ-нің белгілі бір деңгейін ұстап тұру қабілеттілігі;
- субъектілер – не бір нысанмен жұмыс жасау үшін олардың рұқсатының дәрежесі бойынша.

Жіктелім толық өткізілгенде, тек қана үш құраушыны сәйкестікке келтіру керек – сезімталдықтың берілген категориясының нысаны тек сенімділіктің сәйкесінше категориясының құралымен және енудің сәйкесінше категориясының субъектісімен өңделеді. Егер тиісті деңгейдің құралы немесе субъектісі табылмаса, онда жаңарту жүргізу керек немесе құрал сатып алу керек және жаңа пайдаланушыларды жұмысқа алып оқыту керек.

Нақтылық осы сұрақта күрделірек болып келеді (Субъектілерді кеңес кәсіпорындарының тәртібі бойынша бөлімдердің жинаған тәжірибесін есепке ала отырып жіктеу қарапайым). Бірақ қазіргі ақпараттық кеңістікте қолданушылардың сенімділігінің ортақ деңгейімен қатар келесі факторларды да есепке алу керек:

- ортақ біліктілік немесе ақпараттық жүйеде адам факторы салдарынан жаңылуларды кіргізбей жұмыс істеу қабілеттілігі. Ақпараттық қауіпсіздіктің бұзушылықтарының санағы белгілі. Нақты цифрлар туралы айтпай-ақ, бір ұйым үшін 1% бұзушылықтар ешнәрсені өзгертпесе, ал басқа ұйым үшін келеңсіз жай болып табылатынын есте сақтау керек;
- АҚ саласында пайдаланушыларды әзірлеуі.

2.2.1 Негізгі регламент жіктелуі. Жүйенің қауіпсіздік деңгейінің өте белгілі белгілері:

- АҚШ қорғаныс министрлігі шығарған қызғылт сары кітап – компьютерлік жүйелердің қауіпсіздік деңгейін бағалау белгісі;
- қызыл кітап – ақпараттық желідегі компьютерлік жүйелердің қолданылуы жағдайлары үшін бұл белгілердің кеңейуі.

Егер "Жүйе С2 сыныбы бойынша сертификатталған" деген термин қолданылса, онда бұл, осы белгілер бойынша ақпараттық қауіпсіздіктің деңгейін көрсететін термин.

Осы жағдайдағы нысандардың жіктелуін, яғни мәліметті қарастырайық. Қағаз құжаттарының дәуірінде кеңінен қолданылатын жіктелу – қызметтік пайдалануға арналған құпия және ашық, электрондық мәліметтің ғасырына да көшірілді. Осы жіктелу жеткілікті болып табылмайды және тек қана оңашалықтың тұрғысын жуықтап қамти алады. Табысты жұмыс үшін бүтіндіктің ұғымын, сонымен бірге мәліметтің ашықтығын қамту керек.

Ақпараттық объектілердің жіктелімі

"Құпия-оңаша - ашық" градациясы нысанның дөрекі нобайы болып табылады.

1-ші мысал. Барлау қызметі немесе қорғаныс министрлігі секілді жабық түрдегі мемлекеттік мекеме. Мұндай мекемелер үшін бірінші орында әдетте құпиялылық ұғымы тұрады, сондықтан ақпараттың таралуына қарағанда оның бұзылу немесе жойылу мүмкіндігі жіберіледі.

2-ші мысал. Банк. Егер нысан ретінде клиенттің есебіндегі қаражаттар сомасының мәні тұрса, онда банктің негізгі мақсаты оның (бүтіндік) рұқсат етілмеген өзгерісінің мүмкін еместігін қамтамасыз ету. Төтенше жағдайларда мәліметтердің ашылуы немесе есепке уақытша рұқсаттың жоқтығын көрсетуге болады.

3-ші мысал. Интернет қызметтердің жабдықтаушысы (тегін пошталық сервер). Мұндай мекеме үшін қолданушылардың серверге тұрақты рұқсатының болуы мүмкіндігін қамтамасыз ету өте маңызды. Құпиялылық пен бүтіндік маңызды болып қала береді, бірақ әрдайым бірінші дәрежелі талап емес.

2.2.2 Нысандарды жіктеу нобайының үлгісі. Ақпараттық нысандарды жіктеу үшін келесі үлгіні ұсынуға болады. Категория сыныбына кейінгі сілтемелерді көрсету ыңғайлы болу үшін бірден әріптік - цифрлы белгі енгізуге кеңес береміз (КЦД сыныбы үшін "Д" бедербелгісі қолжетімділікті, "К"-құпиялылықты, "Ц"-бүтіндікті білдіреді).

Болуына байланысты қолжетімділік:

- шектік – онсыз субъектінің жұмысы тоқтап тұрады (Д0);
- өте маңыздысы – онсыз жұмыс істеуге болады, бірақ өте қысқа уақыт мерзімінде (Д1);
- маңыздысы –онсыз аз уақыт жұмыс істеуге болады, бірақ ол ерте ме, кеш пе әйтеуір керек болады (Д2);
- мағыналысы – онсыз жұмыс істеуге болады, бірақ ол қолдану қорларды үнемдейді (Д3);
- мардымсыз – субъектінің жұмысына ықпал етпейтін ескірген немесе пайдаланылмайтын (Д4);
- зиянды – оның бар болуы өңдеуді талап етеді, ал өңдеу нәтижесіз немесе залал келтіріп қорлардың шығынына әкеледі (Д5).

Рұқсат етілмеген түрлендірулері бойынша (бүтіндік):

- шектік – оның рұқсат етілмеген өзгерісі толық субъектінің немесе оның бөлігінің дұрыс жұмыс жасамауына әкеліп соғады: түрлендірудің салдары (Ц0) қайтымсыз болады;
- өте маңызды – оның рұқсат етілмеген өзгерісі субъектінің бөлігінің дұрыс жұмыс жасамауына бірнеше уақыттан соң әкеліп соғады, егер әрекеттер жасалмаса; түрлендірудің салдары (Ц1) қайтымсыз;
- маңызды – оның рұқсат етілмеген өзгерісі субъектінің дұрыс жұмыс жасамауына бірнеше уақыттан соң әкеліп соғады, егер әрекеттер жасалмаса; түрлендірудің салдары (Ц1) қайтымсыз;
- мағыналы – оның рұқсат етілмеген өзгерісі субъектінің дұрыс жұмыс жасамауына әкеліп соғады; түрлендірудің салдары (Ц2) қайтымды;
- маңызыды емес –оның рұқсат етілмеген өзгерісі (Ц4) жүйенің жұмысына әсер етпейді.

Таралуы бойынша:

- шектік – ақпараттың таралуы субъекттің жұмысының күйреуіне немесе (К0) айтарлықтай материалдық шығындарға әкеледі;
- өте маңызды – ақпараттың таралуы айтарлықтай материалдық шығындарға әкеледі, егер кейбір әрекеттер орындалмаса (К1);
- маңызды – ақпараттың таралуы айтарлықтай материалдық немесе моральдік шығындарға әкеледі, егер кейбір әрекеттер орындалмаса (К2);
- мағыналы – әдетте моралдік нұқсан келтіреді, тек қана белгілі бір жағдайларда қолдануға болады (К3);
- мардымсыз – өте сирек жағдайларда моральдық нұқсан келтіреді (К4);
- маңыздылығы жоқ – субъектінің жұмысына ықпал етпейді (К5).

2.3 Субъектілерді жіктеу үлгісі

Ақпараттық кеңістіктің субъектісі ретінде ақпараттық кеңістікте ақпараттық жүйеге қатысты белсенді жұмыс атқаратын, ақпаратпен жұмыс істеу құралдарын, процестерін және адамдарды қарастырамыз.

Құқықтар мен жауапкершілікті үлестіру қағидалары.

Мұндай үлестірудің негізінде екі іргелі қағидалар жатады.

Таралған жауапкершіліктің қағидасы. Бұл қағида жүйеде қауіпсіздікке залал келтіре алатын амалды басынан аяғына дейін өз бетімен орындай алатын субъект болмауы керек екендігін білдіреді. Мысалы, егер А пайдаланушы жүйе үшін маңызды мән болатын кейбір транзакцияны орындаса, онда ол тиісті күшіне, тек оны Б пайдаланушысы тексеріп, түзулілігін растағаннан соң енеді. Сонымен, осы транзакцияны А пайдаланушысы да, Б пайдаланушысы да жеке дара жасай алмас еді, біреуі мәліметтерді қалыптастырып, екіншісі мәліметті тіркейді.

Егер жүйедегі нақты операция екі қолданушылардың арасындағы бөлігіне алмай құрастырылса, демек оның кризистік маңыздылығының

жанында, қолданушымен орындауы керек. Мысалы, бұл функцияны іске қосылатын қолданушы аутентификациясына паролінің бөлінуімен (немесе көп) екі бөлікте жете алады. Бұл қағида кейде "Төрт көзде" деп аталады. Егер мағыналы операциялардың қатары объективті түрде бір-ақ адаммен орындалуы керек болса, онда оның әсерлерінің нәтижелері түзетуге рұқсаты болмайтын журналдарға тіркелуі керек. Бұл журналдар басқа адаммен үнемі талдауы керек.

Кәсіпорындағы рөлдердің саясатының мақсаты - беруді бір ізге салып ықшамдасын қызметкерлерге дұрыс айтуы. Жиын оны және міндеттердің әрбір жаңадан келген қызметкері үшін қажеттіліктің ұқсас схемасының өңдеулерінен кейін құрап және есептік жазуларды жүздікті күйіне келтіру. Басқа да жұмысшылардың жабдықтарының редакциялау пішінін көрсетсе жеткілікті.

Артықшылықтардың минимизациялау қағидасы. Бұл қағида қолданушыға жұмыс жасау үшін керек, бірақ тек қана оқу, және де барлық мәліметке рұқсат алуы керек, яғни қолданушының міндетінде егер мәліметтердің барлық базасы бойынша есептеу нәтижелерінің құрастыруының дұрыс екенін білдіреді.

2.3.1 Субьектілерді жіктеудің қарапайым моделі.

Субьект жіктелімінің қарапайым моделін қарастырайық. Ақпараттық кеңістікте мекемелерде келесі түрдегі субьектілер болады:

- нысанды құрушылар;
- нысанды қолданушылар;
- нысанды басқарушылар (яғни басқа субьектілердің обьектілерінің жұмыс ортасын қамтамасыз етушілер);
- нысандарды субьект ретінде қолдануды басқарушылар.

Кез келген нақты субьекті өзінің бойында келтірілген жіктеме негіздердің бірнешеуін немесе барлығын жинақтауы мүмкін.

Ақпаратпен жұмыс жасау тәсіліне байланысты келесі топтарды анықтайық.

А тобы. Бір субьекті ақпаратқа ие болып, оны басқа субьектке жібермей-ақ, өз бетінше өңдейді. Бұл жағдайда ол ақпараттың жіктелуі мен жұмыс тәсілдерін өзі басқара алады.

Б тобы. Бір субьекті ақпаратқа ие болып, оны басқа субьекті не субьектілер тобы қолдануы үшін таратады. Бұл жағдайда ол ақпарат жіктелімін жүзеге асыруы, оның қолданылу ережелерін анықтауы және тұтынушыларды сол ережелермен таныстырып немесе осы әрекеттерді орындайтын басқа субьектіні тағайындап қоюы қажет.

В тобы. Субьектілер тобы дәл сол ақпараттық обьектіні немесе бір субьектіні иелену құқығы жоқ обьектілердің жиынтығын қолданады. Бұл жағдайда субьектілер заң берушілік кеңістік аумағындағы иесімен анықталған ақпаратты қолдану ережелеріне бағынады.

Д тобы. Субьектілер тобы кең және анықталмаған рұқсатты ақпараттық обьектілерді қолданады. Бұл жағдайда заң берушілік кеңістік аумағында обьектілермен жұмыс шектеусіз жүргізіледі.

Бізге үлкен қызығушылықты тудыратын Б тобы болып саналады. Аталған топтарға сәйкес ақпараттық өмірлік стадиясы бойынша субьектілердің келесі міндеттерін ажыратамыз.

Әкімгер-субьектілер (ары қарай жай ғана әкімгерлер) қолданушы субьектілермен (ары қарай жай ғана қолданушылар) анықталған тапсырмаларға сәйкес нысандарды құру, таратуын қолдану және сақтау шарттарын қамтамасыз етуі керек, және де әкімгерлер жағынан сияқты бақылаушы субьектілерінің (ары қарай жай ғана бақылаушылар) жағынан да қолданушылардың іс-әрекеттеріне бақылау жасау үшін шарттарды құру. Әкімшілер өз жұмысында қолданушылардың нысандарымен жұмыс істейтін құрылған ережелерімен жүруі керек. Сонымен бірге олар ақпараттық нысандарды жіктеп, қолданушылардың ережелермен және жіктелумен танысуын қамтамасыз етіп, және де осы ережелердің орындалуын бақылауы тиіс.

2.3.2 Субъектілерді жіктеудің толық моделі.

Ақпарат иесі – мекеменің ақпараттық белсенділігіне жауапты бизнес менеджер. Міндеттері келесі түрдегідей:

- ақпараттың біріншілік жіктелуін орнату және осы жіктелудің өндірістік тапсырмаларға жауап бере алу мүмкіндігін периодты түрде тексеру;
- жіктелу негізінде жұмыс механизмінің қауіпсіздігін анықтау;
- ақпараттық белсенділікке рұқсат құқығының мәнін талдау;
- келесі амалдарды орындау немесе орындаушыны тағайындау: басқа бизнес-бөлімшелерден рұқсат сұранысын бекіту, резервті көшіру, мәліметтерді қалпына келтіру, қауіпсіздіктің бұзылу фактілері бойынша әртүрлі іс-әрекеттерді бекіту.

Ақпарат сақтаушы – әдетте негізгі тапсырмасы – мәліметтерді резервті көшіру мен қалпына келтіру болып табылатын ақпараттық технология маманы. Міндеттері келесі түрдегідей:

- орнатылған ақпарат иесінің талабына сәйкес резервті көшіруді жүзеге асыру;
- қажет жағдайда жоғалған не бүлінген мәліметтерді қалпына келтіру;
- резервтік көшірме мәліметтерінің сақталуы мен қолжетімді болуын қамтамасыз ететін міндетті шараларды жүзеге асыру;
- ақпарат иесінің талаптарына сәйкес тіркемелердің сақталуын қамтамасыз ету.

Үстеме (приложения) иесі – үстememен қызмет көрсетілетін өндірістік және де басқа да функциялардың орындалуына толығымен жауапты бизнес-бөлімше басқарушысы.

Міндеттері келесі түрдегідей:

- тұтынушылардың рұқсат (доступ) критерийлерін орнату және үстеме үшін рұқсаттылықты талап ету;
- қосымшаның қауіпсіздік механизмін қолданатын барлық құралдарды басқару;
- келесілерді орындау, не бұйрық беру:
  1) күнделікті қауіпсіздікті басқару;
  2) жеке рұқсат (доступ) сұраныстарын қарастыру;
  3) қауіпсіздік бұзылған жағдайда талдау жасау;
  4) нақты жүйеге орнатылғанға дейін қосымша өзгерістерін қарастыру және растау;
  5) қосымшалар аясында тұтынушылардың рұқсат құқығының өзектілігін растау.

Тұтынушылар әкімшісі – жұмысшылардан тыс басқарушы. Оның толық жауапкершіліктері – тұтынушының тіркеме мәліметтері және мекеме жұмысшыларының ақпараттық қорлары (яғни жүйелер, үстемелер, мәліметтер т.б). Міндеттері:

- тұтынушының босатылуы жөнінде оның тіркеме жазбасын өшіру, сөндіру немесе уақытша бекіту (блокирования) үшін қауіпсіздік әкімшісіне хабарлау;
- тұтынушының қызметтік орнын ауыстыруы жөнінде егер ол рұқсат құқығының не формасының өзгерісіне алып келетін болса, қауіпсіздік әкімшісіне хабарлау;
- ИБ жүйесіне барлық қауіпсіздік оқиғалары жөнінде немесе осындай оқиғаларға күмән болған жағдайда есеп беру;
- жаңа тұтынушылар үшін біріншілік парольдерді ұсыну және форматтау;
- қауіпсіздік саясатының сұрақтарымен тұтынушыларға сабақ жүргізу.

Қауіпсіздік әкімшісі – рұқсат басқару жүйесінде сәйкес мүмкіндіктерге ие болатын мекеме жұмысшысы. Ол қауіпсіздік механизмін орнатады, тұтынушылардың тіркеме жазбаларын және ақпараттық қор рұқсатына құқығын басқарады. Ол не бизнес-бөлімшеге, не ИБ жүйесіне есеп береді. Келесі міндеттерге ие болады:

- әртүрлі орталарда мәліметтерді өңдеу және нәтижесінде оларға деген рұқсаттылықты ұсынуды талдайды;
- рұқсат сұраныстарының қауіпсіздік ережелері мен ақпаратты қолданудың жалпы жолымен сәйкес келу дерегін бақылап отыру;
- рұқсат құқығының ақпарат иесі құрған критерийлермен сәйкес келуін басқару;
- тұтынушылар әкімгері орнатқан тұтынушылардың тіркеме жазбаларын құру және өшіру;
- функционалдық міндеттер мен өз жұмысының аумағындағы жүйені басқару;
- қауіпсіздік жағдайы бұзылғаны туралы есеп берулерді зерттеу;

- жаңа тұтынушылардың бастапқы құпия сөздерін олардың бастығы арқылы бағыттау.

Қауіпсіздік талдаушысы – ақпаратты бақылау және қорғау ақпарат маңыздылығына, компрометация мен жоғалу тәуекеліне негізделген сенімді қамтамасыз етілу мәліметтерінің (стратегиялар, процедуралар, ережелер) қауіпсіздігінің дамуын анықтауға жауапты қызметші. Міндеттері:

- ақпаратты басқару процедурасының қауіпсіздігінің жетекшілігін көрсету;
- ақпараттық негіздегі жұмыстың негізгі принциптерінің түсінігін қамтамасыз ету;
- мәліметтерді қорғау жүйесінде орындалған талдауды және кеңес беруді қамтамасыз ету.

Басқару модификациясының талдаушысы – АҚ модификация инфрақұрылымының сұранысына жауапты қызметші.

Мәліметтер талдаушысы – мәліметтер құрылымының орындалу бизнес талаптарына талдау жасайды, мәліметтер стандарты мен оларға тән физикалық платформаларды ұсынады. Міндеттері:

- бизнес талаптарына сәйкес мәліметтер құрылымын жасау;
- мәліметтер базасының физикалық құрылымын жасау;
- бизнес талабы негізінде мәліметтердің логикалық моделін құру және қолдау;
- мәліметтер архитектурасы жасалу кезінде ақпарат иесін техникалық қолдауды қамтамасыз ету;
- метамәліметтерді (мәліметтердің сақталуы туралы) мәліметтер кітапханасына жазу;
- мәліметтерді тиімді тарату үшін метамәліметтерді құру, қолдану және қолдау.

Шешімдер провайдері – шешімдерді құруда және бизнес шешімдерді айналдыру процесінде қатысатын қызметші, әртүрлі ақпараттық жүйелерде интегратор, қосымша құрушылар, ақпараттық технология провайдері деп аталады.

Міндеттері:

- қосымшалар мен мәліметтердің бірлесіп жұмыс істеуіне сенімділікті қамтамасыз ету үшін мәліметтер талдаушысымен жұмыс істеу;
- мәліметтер талдаушысына техникалық талап жіберу.

Соңғы тұтынушы – өз жұмысы аумағында ақпараттық жүйелер мен қорларды қолданатын мекеменің иесі немесе келісім шартпен жұмыс жасайтын жұмысшы. Міндеттері:

- рұқсат құпия сөздерін жасырын сақтау;
- ақпарат қауіпсіздігі оның күтімі болатынын түсіну;
- белгілі басшылықты мекеменің бизнес активтері мен ақпараттық қорларын пайдалану;

- АҚ стандартында саясат қауіпсіздігінің, іс шараның барлық аспектілерін бақылау;
- АҚ-пен байланысты іс-шара есеп берулерін басшылық сұранысы бойынша таныстыру.

Процесс иесі – белгілі өндіріс мұқтаждықтарына сәйкес процестің тұрақты жақсартылуына, басқарылуына және ендірілуіне жауапты қызметші.

3 Физикалық рұқсатты бақылау жүйелері

Ұйым қызметінің қауіпсіздігіне сәйкес шеткі көрсетілімдерді де ұсынатын әртүрлі сұлбалар болуы мүмкін.

Мекемеге өту бірнеше өткізу орындарымен жүзеге асады; компьютерлер орналасқан бөлмелер, бірнеше құлыппен жабылады да тек директор не күзетшілер бастығы болғанда ғана ашылады, кейде тіпті компьютерлерді де сейфке салады. Ұйым үшін критикалық маңызға ие барлық мәліметтерді өзінде сақтаған компьютер тұрақты түрде интернетке не жай ғана модемге қосылады, және кез келген ең минималды бағдарламалық қорғау әдістері болмайды, ал компьютерге кіру паролі – «123» болады.

Мекеме желісі тек HTTP, SMTP, DNS хаттамаларын ғана өткізетін қуатты желіаралық экранмен қорғалған. Әрбір жұмыс станциясында тұрақты түрде (тіпті кейде тұтынушы жұмысында шығын болса да) антивирустық сканерлер жіберіледі. Желі шабуылды анықтайтын агенттік жүйесімен түсірілген, ал тұтынушының әрбір әрекеті әртүрлі электрондық регистрациялық журналдарда көрсетіледі. Желінің орталық сервері клиенттермен жұмыс жасау залының бұрышында және жұмыс күні аяқталар уақытта тазалаушылар шай ішетін жерде орналасқан.

Әрине, бұл шектік мысалдар, алайда бұл немесе басқа жағдайдағы нұсқалар іс жүзінде кездеседі.

Қауіпсіздікті қамтамасыз ету үшін 5 кілттік мезет бар:

- офис есіктері жабық;
- столдар мен шкафтар жабық;
- жұмыс станциялары қауіпсіздікте;
- дискеталар қауіпсіздікте;
- мекеме ақпараттары қауіпсіздікте (басып шығарулар, қағаз құжаттар).

3.1 Физикалық рұқсатты бақылау механизмдері

3.1.1 Жалпы мағлұматтар. Физикалық рұқсат бақылауын қамтамасыз ететін механизмдер басқа да АҚ механизмдеріне ұқсас, атап айтқанда субъекті нысанға ену үшін тіркелген, авторластырған болуы керек. Бұл жағдайда субъектінің нысанмен электрондық жұмыс жасауынан ерекшелігі, ол адамның әрекеттері уақыт бойынша барынша таралуы және құқыққа қарсы

әрекеттер болған мезетте қауіпсіздік қызметінің келгенге дейінгі нақты уақыт шамасына жуық тәртіпте адамдармен бақылануы.

Физикалық рұқсат бақылауының қазіргі заманғы әдістерін әдетте мынадай топтарға бөлінеді:

- периметрді қорғау жүйелері;
- рұқсатты басқару және бақылау жүйелері;
- бейнебақылау жүйелері;
- күзеттік сигнализация жүйелері (бұл жүйе периметрді қорғау жүйесімен қосылған болуы мүмкін);
- сақтау жүйелері (сейфтер). Егер нысан қауіпсіздігін қамтамасыз етуге бөлінетін қаражат жетсе, онда келтірілген жүйелерді ғимаратты басқару жүйесі деп аталатын бірлік жүйеге топтастыруға болады.

Барлық зияткерлік ғимараттардың осындай жүйелерін енгізу және жобалау жұмыстары айтарлықтай күрделі және әдетте басқа компаниялармен атқарылады.

3.2 Потенциалдық бұзушының тәртіп моделі

Қасақана рұқсатсыз енудің болған уақытын және орнын білу мүмкін емес, сондықтан ең қауіпті жағдайларды жорамалдап, потенциалдық бұзушының тәртіп моделін келесі түрде елестету орынды:

а) бұзушы автоматты жүйенің периметрінің кез келген жерінде және кез келген уақытта пайда болуы мүмкін;

б) бұзушының біліктілігі мен хабардарлығы берілген жүйені жасаушының деңгейінде болуы мүмкін;

в) жұмыс жүйесінің принципі туралы тұрақты сақтаулы және құпиялы ақпарат бұзушыға белгілі;

г) өзінің мақсатына жету үшін бұзушы қорғануына барынша осал буынды таңдайды;

д) бұзушы тек бөгде тұлға емес, сонымен қатар жүйенің заңды тұтынушысы болуы мүмкін;

е) бұзушы жалғыз әрекет жасайды.

Берілген модель қорғануды құру үшін бастапқы мәліметтермен анықталуға және оның негізгі құрылу принципін белгілеуге рұқсат береді.

«а» пунктіне сәйкес, міндетті түрде қорғалатын заттың айналасында тұрақты әрекет ететін тұйық контурын тұрғызу керек.

«б» пунктіне сәйкес, қорғанысты құратын бөгеттің құрамы мүмкіндігінше бұзушының күтілетін біліктілігі мен хабардарлығына сәйкес болуы керек.

«в» пунктіне сәйкес, заңды тұтынушының жүйеге кіруі үшін тек оған белгілі өзгермелі құпиялы ақпарат керек.

«г» пунктіне сәйкес, қорғаныс контурының қорытынды төзімділігі оның осал буынымен анықталады.

«д» пунктіне сәйкес, бірнеше заңды тұтынушылардың орындалатын функциялары мен өкілеттілігіне сәйкес олардың ақпаратқа рұқсатын шек қоюын қамтамасыз еткен пайдалы, сонымен қоса егер олардың ішіндегі біреуінің жауапсыз орны болған жағдайда шығынды шегеру мақсатымен әрбір тұтынушының аз хабарлылығының принципін растау. Осыдан, қорғаныстың беріктілік есебі бұзушының екі мүмкін бастапқы жағдайы үшін шығарылуы керек: бақыланатын шекарадан тыс және соның ішінде.

«е» пунктіне сәйкес сонымен бірге әдетте бастапқы алғышарт ретінде бұзушыны жалғыз деп санайды, өйткені бұзушылар тобынан қорғаныс – келесі зерттеу сатысының тапсырмасы. Алайда бұл осы текті тапсырманың айтарлықтай қиындығына қарамастан бұл жағдай түрінен ұсынылған әдістер мен амалдар арқылы қорғану мүмкіндігін жоққа шығармайды. Осының арқасында бұзушылар тобының негізімен жалпы басшылықпен бір тапсырманы орындайтын тұлғалар тобы түсіндіріледі.

Алайда, өндірілетін ақпарат құндылығының әртүрлі тағайындалған қорғаныс жүйесінде «қауіпті» потенциалдық бұзушының тәртіп моделі де әртүрлі болуы мүмкін. Яғни әскери жүйе үшін – кәсіби барлаушы деңгейі, ал коммерциялық жүйе үшін – маманданған тұтынушы деңгейі.

Айтылғандар негізінде бұзушының бастапқы тәртіп моделін таңдау үшін дифференциалдық әдіс орынды. Сондықтан потенциалдық бұзушының мамандануы – қауіпсіздіктің төрт класы негізінде қабылдау мүмкіндігіне қатысты түсінік:

1-ші класс тұтынушы үшін өмірлік маңызды ақпараттарды үлкен жоғалтуларға алып келетін модификация, қирату, жоғалудан қорғау үшін ұсынылады.

2-ші класс бірнеше тұтынушылардың жұмысы кезінде әртүрлі мәліметтер массивіне рұқсаты бар, басқа тұтынушылар үшін қол жетімсіз құнды ақпараттарға қатысты қорғанысты қолдануды ұсынады. Қорғаныс беріктілігі кәсіби бұзып түсуші ұрыға емес, жоғары маманданған бұзушыға есептелініп жасалуы керек.

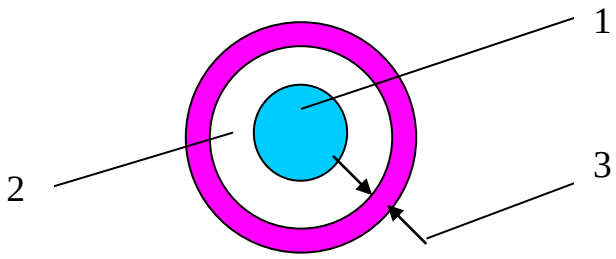
3-ші класс құнды ақпаратқа қатысты қорғануды ұсынады, тұрақты бекітілмеген рұқсат жолы өте құнды ақпараттардың жоғалуына алып келуі мүмкін. Мұнда да қорғаныс беріктілігі профессионал бұзып түсуші ұрыға емес, жоғары маманданған бұзушыға қатысты есептелініп жасалынған.

4-ші класс маңызды бұзушылар үшін қызуғышылық тудырмайтын қарапайым ақпараттарды қорғау үшін ұсынылады.

Келтірілген қауіпсіздік деңгейлердің іске асырылуы потенциалдық бұзушының күтілетін класымен сәйкес бекітілмеген рұқсаттың мүмкін каналдарының белгілі санын жабатын қорғаныс әдістеріне сәйкес жиынтығымен қамтамасыз етілуі керек. Класс ішіндегі қорғаныс қауіпсіздігінің деңгейі қорытындысы төменде келтірілген, есептеу формуласымен анықталатын қорған беріктігінің сандық бағасымен қамтамасыз етіледі.

3.3 Қарапайым қорғаныс моделі

Қорғаныс заты бөгет деп аталатын тұйық және біртекті қорғаныс қабығында орналасқан.



1 – қорғаныс заты; 2 - бөгет; 3-бөгеттің беріктік параметрі.
3 сурет – Қарапайым қорғаныс нобайы

Қорғаныс беріктілігі бөгет құрамына тәуелді. Бөгеттің қағидалық рөлді ойнайтын әрекетке қарсы тұру мүмкіндігі – оның иесі мен бұзушыны еліктіру мүмкіндігі. Қорғаныс нысанының тартымдылығы оның бағасында. Қорғаныс затының бұл ерекшелігі есептеуіш жүйелерде және ақпаратты қорғау бағасында кең қолданылады. Сондықтан, егер потенциалдық бұзушының игеретін күтілетін шығын құны қорғалатын ақпарат құнынан асып кетсе, онда құрылған бөгеттің беріктілігі жеткілікті деп есептелінеді. Алайда басқалай да әдіс болуы мүмкін.

Уақыт өте келе ақпарат өзінің тартымдылығын жоғалтып ескіретіні белгілі, ал жеке жағдайда оның бағасы нөлге дейін түсуі мүмкін. Ақпараттың өмір сүру уақыты кезінде қорғаныстың жеткілікті шарты үшін бұзушының бұзушының бөгетті игеруіне кеткен уақытын өсіру керек. Егер бұзушының бөгетті игеру ықтималдығын $P_{сзи}$ деп, ақпарат өмірінің уақытын $t_ж$, ал бұзушының бөгетті игеруінің күтілетін уақытын $t_н$, және бұзушының бөгетті орағытып өту ықтималдығын $P_{обх}$ десек, онда ақпараттың ескіру жағдайы үшін қорғаныстың жеткіліктік шартын келесі қатынас түрінде аламыз:

$P_{сзи}$ =1, егер $t_ж < t_н$ және $P_{обх}$ =0.

$P_{обх}$ =0, нольге теңдігі, қорғаныс затының айналасында бөгеттің тұйықталуының қажеттілігін көрсетеді. Егер $t_ж > t_н$, ал $P_{обх}$ =0, онда

$P_{сзи}$ =(1- $P_{нр}$),

мұндағы $P_{нр}$-$t_ж$ уақытынан аз уақытта бұзушының бөгетке төтеп беру ықтималдығы.

Шынайы жағдай үшін $t_ж>t_н$ және $P_{обх}>0$, қорғау төзімділігі келесі түрде

$P_{сзи}=(1-P_{нр})(1-P_{обх})$.

Бірақ бұл жағдай бұзушы екеу болғанда әділетті, яғни біреуі бөгетке төтеп береді, ал екіншісі оны айналып өтеді. Біз бұзушы біреу деп шарт қойғандықтан, бөгетті өтудің бір әдісін – ең оңайын таңдайды. Сонда жоғарыда көрсетілген формулада «немесе» формуласын қолданамыз:

$P_{сзи}=(1-P_{нр})^{\vee}(1-P_{обх})$,

мұндағы $\vee$ - «немесе» белгісі.

Демек, бөгеттің төзімділігі $(1-P_{нр})^{\vee}(1-P_{обх})$ шамаларын анықтау мен салыстырғаннан кейін оның ең аз мәніне тең болады.

Қарапайым қорғау мысалы ретінде, бірінші формуламен есептелетін ақпаратты криптографиялық қорғауды атауға болады, онда $P_{нр}$ шамасы кілт кодын таңдау ықтималдығын бағалаумен анықталады, ол арқылы осы жолмен жабық ақпаратты келесі формуланы қолданып, дешифрлеуге болады:

$$P_{нр}=\frac{n}{A^{S}},$$

мұндағы n – кілтті таңдау әрекетінің саны;

A – кілт кодының таңдалынған алфавитіндегі белгі саны;

S – белгі санындағы кілт кодының ұзындығы.

$P_{обх}$ шамасы таңдалынған шифрлеу тәсілі, қолдану амалынан, ақпарат мәтінінің жабылу енінен, криптоталдау тәсілінің бар-жоғынан, сондай-ақ кілт кодының шын мәнін сақтау жолы және оны иеленушісінде жаңаға ауыстыру периодына тәуелді.

$P_{обх}$ белгілі мәнін таңдау мен анықтауды алғашқыда мамандардың тәжірибесінің негізінде өткізуге болады. $P_{обх}$ шамасы 0 мен 1 аралығында болады. $P_{обх=1}$ болғанда қорғау барлық мағынасын жоғалтады. Қорғауға жататын ақпарат ескірмесе немеес периодты түрде жаңарып тұрса, яғни $t_{ж}>t_{н}$ теңсіздігі тұрақты немесе $t_{н}>t_{ж}$ теңсіздігін қамтамасыз ету мүмкін емес болса, онда әдетте объектіні қорғау немесе затқа бұзушыны көріп калу және кіруді рұқсат етпейтін бөгет тұрақты түрде қолданылады. Бұндай қорғау ретінде адам немесе адам басқаратын көріп қалу арнайы автоматтандырылған жүйесі қолданылады.

Бөгетке рұқсатсыз енуді көріп қалу және оны тоқтату қабілеттілігі – есептеу формуласындағы $(1-P_{нр})$-дің орнына $P_{обл}$ – рұқсатсыз енуді көріп қалу және оны тоқтату ықтималдығын енгізу жолымен төзімділігін бағалау кезінде ескерілу қажет.

Автоматтандырылған бөгеттің жұмыс істеу принципі бұзушыны көріп қалу көрсеткіші периодты бақылау түрінде басқару блогымен жүргізіледі. Бақылау нәтижесі адаммен бақыланады. Автоматпен сұралатын көрсеткіш периодтылығы секундтың мыңнан бір бөлігіне дейін жете алады. Бұл жағдайда бұзушының бөгетке төтеп беру күтілетін уақыты көрсеткіштің сұраныс периодынан едеуір асып кетеді. Сондықтан жиі мұндай бақылауды тұрақты деп атайды. Бірақ бақылауды автоматты басқаратын адамға бұзушыны анықтау үшін көрсеткіштің аз периодты сұранысы аздық етеді. Сондай-ақ үрейлі сигнал беруді өндіретін сигналға уақыт керек. Әдетте

бұзушының әрекеттерін тоқтату үшін үрей сигналы да жеткілікті екенін тәжірибе көрсетті.

Бұзушының жүйенің көріп қалу және бітеуден айналып өтудің бір жолы – жасырын түрде көріп қалу жүйесін өшіру (мысалы, бақылау тізбектерін үзу немесе тұйықтау, бақылау сигналына ұқсас сигналды қосу, сигналды жинау бағдарламасын жинау). Бұндай оқиғаның болу ықтималдығы жүйенің жұмысы мен құрылу принципін талдау негізінде баға беру әдісімен 0 мен 1 аралығында анықталады.

3.4 Аймақты күзету жүйесі

Қай жерді күзет ету және онда нысандардың қандай түрі болу керек екенін анықтау үшін субъекті табу тәртібін анықтау керек. Мысал ретінде, дуалмен қоршалған ғимаратты, оның ішінде серверлік бөлмесі бар техникалық қабаты бар. Әрине, дуал сыртында кез келген адам болуы мүмкін, бірақ дуалға өте жақын келгенде және мекеменің сыртында бөтен адамдар тек өте шектеулі уақыт қана (жанынан өткенде) болуы мүмкін – басқа жағдайлар қауіпсіздік қызметінің назарын аудартуы тиіс.

3.4.1 Күзетудің дәстүрлі жүйесі. Бұл жүйелер терезе әйнегі мен есік ойығында (коммутациялық жүйелер) орналасқан түйіндерге тартылған, ток өткізетін желілерде немесе сейф бұзуы, сөре, төбенің, қабырғаның сынуы туралы сигнал беретін дыбыстық қысым көрсеткішінде, не болмаса күзетілетін нысанға адам жақындағанын сезетін сыйымдылықты көрсеткіштерде жүзеге асады.

Тек жұмыс уақытында, айталық, 8.00-ден 18.00-ге дейін уақытта ғана дуал сыртына (күзетілетін аймақ) ұйымның қызметкерлері мен оларды шығарып салушы адам ғана шыға алады. Ғимаратқа сағат 8.00-ден 18.00-ге дейін жұмысшылар ғана арнайы жіберу қағазымен ғана кіре алды, 22.00-ге дейін шығуы тиіс, ал субъектілер тек 16-ға дейін кіріп, 18-ге дейін қатаң түрде шығуы тиіс. Техникалық қабатқа тек техникалық бөлім қызметкерлері ғана тек жұмыс уақытында ғана көтеріле алады, ал серверлік бөлмеге тек жүйелік оператор (администратор) ғана қауіпсіздік бөлімін хабарландырғаннан кейін ғана кіре кіре алады.

Енді тұжырымдалған тапсырмаларды шешу үшін қандай механизмдер пайдалану керектігін анықтауға болады. Дуалдың толық өтуге болмайтын болуы дұрыс (қазуы немесе ұшып өту мүмкіндігін қоспағанда кәсіпорын режимділігіне тәуелді), сондай-ақ дуалға жақындауын бақылау үшін видеобақылау камераларымен жабдықталғаны дұрыс. Бір жағынан дуалды сыртынан айналып өткен субъектілерін көріп қалу, ал екінші жағынан дуалға ұйым қызметкерлерінің жақындауының алдын алу үшін дуалдың ішкі жағында қозғалыс көрсеткіші орнатылуы мүмкін. Дуал (ғимарат) қабырғасында қабырға сындыру затына вибрация көрсеткішінің орнатылуына рұқсат бар. Дуал қақпаларында құжаттарды тексеру қауіпсіздігі үшін

қызметкердің көзбен шолу бақылауы, сондай-ақ алып кіретін заттарды тексеру үшін жарық түсіруші және/немесе металл іздеуші құрылғының болуы жеткілікті.

3.5 Кіруге рұқсатты басқару жүйесі

Кіруге рұқсат басқаруын шартты түрде екіге бөлуге болады – күзетілетін аумаққа алғашқы өтуді басқару және күзетілетін аумақ бойынша орын ауысуды басқару. Егер күзетілетін аймақ ішінде басқасы болса және ол бұдан қатаңырақ күзетілсе, онда сәйкесінше бөліну саны екі еселенеді.

Алғашқы бақылаудың тапсырмасы – авторлау ережелерін қолдануға болмайтындарға, яғни аумаққа кіруге ешқандай құқығы жоқтарды кесіп тастау; аумаққа тыйым салынған заттарды алып кірмеуін, сондай-ақ алдын ала тәртіппен белгіленген басқа функцияларды қамтамасыз ету. Берілген жағдайда келесі механизмдер пайдаланылуы мүмкін:

- адамдар тобының бөлінуін қамтамасыз ететін турникеттер мен металл қақпалар;
- шығарып салушы адамның авторланған қызметкерді бақылау қақпалары арқылы бірге кіруге мәжбүр ету мүмкіндігінсіз, қатаң түрде тек 1 адам ғана өтетін шлюзді кабиналар;
- кілттер будасын пышақтан айыру үшін алып кіретін заттардың габариттін икемдеу мүмкіндігі бар металл іздеушілер;
- жарық шығаратын құрылғылар – бұл құрылғы жарыққа және металлға сезімтал материалдарға қауіпсіз немесе керісінше осындай материалдарға істен шығаратынын анықтауға ғана керек;
- егер кіріс/шығыс қашық жерде жүзеге асатын болса, қолданылатын келіссөздер құрылғысы (бұнда домофондар, бейнедомофондар, интерфондар жатады).

Аталғандардан бөлек, кірістерде қалған территорияларда барлық бақыланатын аумақтарда рұқсат ету параметрлерінің оқу құрылғылары тұруы мүмкін.

Орын ауысу бақылауының тапсырмасы – кіруге рұқсат сұрайтын субъектіні идентификациялау/аудентификациялау және оған авторланған ережелерді қолданып, оны өткізіп жіберу немесе өтуге тыйым салу.

Субъектінің идентификациялану/аутентификациялануы стандартты принциптер негізінде жүзеге асады:

- субъекті білетін бір нәрсе. Әдетте бұл бір АИН (арнайы идентификациялық нөмір) немесе құлыпты ауыстырғанда терілетін код;
- субъектіде бар зат. Бұл кәдімгі есектің кілті немесе токен – магниттік жолағы бар карточка, смарт-карта немесе тағы басқа зат болуы мүмкін;
- субъектіден физикалық немесе психикалық түрде бөлінбейтін нәрсе. Бұл әдетте субъектінің денесінің биометриялық параметрлері.

Адам тұлғасының өзгешілігін ескере отырып, кодты теруге арналған кіруге рұқсат бақылау жүйесі айтуға болады, себебі тіпті АИН-дердің жалпы кіру кодын айтпағанда біраз уақыттан соң кең танымал бір жақтылығы (тенденциясы) бар. Токенді таңдау кезінде қосымша келесі параметрлерді ескерген жөн:

- тозық (көп пайдаланғанда карточкадан магнитті жолақтың өшірілуі, энерготәуелді элементтердің шектелген пайдалану уақыты бар);
- өту жылдамдығы (салыстырып оқылуға элементті қосу біраз уақыт алады);
- бағасы;
- токенге иеленушінің суреттерді енгізу мүмкіндігі;
- мүмкін болатын сынуға төзімділік.

Аутентификацияның биометрикалық құралдарының құрамында жиі кездесетіндер – саусақ дағы, көз тор қабыры, алақан суреті, қол геометриясы, бет пішіні, дауыс параметрлері. Бірақ сол немесе басқа құралды иелену туралы шешім қабылдаудың алдында биометрияның берілген түр үшін жалған жұмыс істеу және жалған қабыл алмау бойынша статистикамен танысу керек. Бұдан басқа, кейбір адамдардың мәдениетті дәстүрлер мен жеке әдеттерін, алдында бірнеше жүздеген адам қолын тигізген беттерге қол тигізу мүмкін емес.

Орын ауыстыру бақылау жүйесін жоспарлағанда аймақтың қай бөлігінде рұқсат сұралынып жатқанда тәуелсіз субъектіге кіру бірыңғай саясатын қолдану қажеттілігі туады. Бұл біріншіден, қолданудың бірізділігін қамтамасыз ету үшін саясат бір орында жасалуы мен сақталуы керек, ал екіншіден, саясаттың орталық сервердің қатардан шығып қалу кезінде жұмысты жалғастыру үшін бірыңғай саясат бірнеше құрылғыға бөліп таралуы керек. Қосымша электрондық журналда субъектінің орын ауысуын тіркеу форматы мен басқа журналдармен интеграция мүмкіндігін алдын ала ескеру керек.

Егер өту есігі өтуге керекті уақыттан көп уақытқа аралық уақытқа ашық қалса, кезекші қызметкердің экранына жария етуді алдын ала қарастыру керек.

Саясатты өзгертуді келесі көпшілік құбылыстарда қарастырған жөн – тыйым салуды ақиқат ретінде елемеу және өрт жағдайында есіктерді ашу немесе рұқсатты шындық ретінде елемеу және қаскүнемді байқап қалған жағдайда есіктерді жабу.

Басқа жағынан, жүйенің жаңылу жағдайында шебер-кілттер (шартсыз өту кілттері) қол астында болуы тиіс, бірақ басқа жағынан, олардың сақталу және қолдануын қатаң есепке алу керек. Тек кіріс шектелген, ал шығыс кіргендердің барлықтарына рұқсат етілген бөлме үшін шығысында салыстырып оқушы емес, жай ғана есікті ашу пернесін қондыру қажет.

3.5.1 Видеобақылау жүйесі. Ең алдымен бұндай жүйе үшін келесі мақсаттарды анықтау қажет: аймаққа жақындау бақылау, өтулерді, бөлмедегі

жұмысшылардың жүріс-тұрысы. Жүйедегі тапсырмаларға тәуелді видеобақылау үшін камералардың бірнеше түрі және басқа құрылғылар қажет болады. Сонан соң анықтау керек:

- ашық орта жағынан бақылау камерасына әсері (жаңбыр, қар, жел, шаң);
- аймақтың ашықтығы, ауданы, жарық түсірілуі (мүмкін, қосымша көздерді орнатуға тура келеді, потенциалды паналарды бөлектеу);
- ашық немесе жабық камераларды қолдану);
- оның айналуы байқала ма?
- объектілердің тек жалпы контурларын ғана көру керек пе, әлде бөлшектерін де көру керек пе (суреттерді ұлғайту)?
- ақ-қара суреттер жеткілікті ме, әлде түсті суреттер де керек пе?
- егер камера қолжетімді жерде болса, ұрлау объектісі болмай ма?
- камерадан суреттер қалай көрінеді: барлығы бірге ме, әлде кезекпен бе?
- суретті жазып алу және оны сақтау жүргізіле ме?

Суреттерді жазып алу керек болса, онда қосымша сұрақтарға жауап жазу керек:

- суреттер барлық камералардан ба, әлде біреуінен ғана жазыла ма?
- жазу әрқашан жүргізіле ме, әлде тек дабыл сигналы жұмыс жасағанда ғана жүргізіле ме?
- жазу үзіліссіз бола ма, әлде дискретті жазу бола ма?
- суретке күні/уақытын жазу керек пе?
- дыбыс жазудың қажеті бар ам?
- жазу аналогты немесе цифрлы бола ма?

3.5.2 Күзет (өрт) сигнал беру жүйесі. Күзет сигнал беру түрін таңдау үшін дабыл сигналын беруге қандай оқиға керек екенін анықтап алу қажет. Мүмкін, ол – дуал мен қабырғалардың сілкінуі немесе сынуы, шарбақ үшін жанасу немесе жақындау, терезелер үшін тұтастықтың бұзылуы, жабық кеңістік үшін көлемнің өзгеруі, есіктің ашылу/жабылуы, күзетілетін территорияның әр түрлі учаскілері үшін қозғалыс. Өрт көрсеткіштері үшін жұмыс жасау белгілері – бөлмеде түтін шыға бастауы және/немесе температураның көтерілуі. Инфрақызыл сәулелену бойынша оттың көзін анықтайтын жалын детекторы қымбат, бірақ жеткілікті түрде сенімді шешім болады.

Көрсеткіштің белгілі бір түрін иемденудің алдында құрылғының жұмыс сапасы статистикасымен – әсіресе бөгеттерде жалған жұмыс жасау мен шынайы бұзылу кезіндегі жұмыс жасамауының процентімен танысу керек. Бұл сипаттамаларды алу үшін, мүмкін, ұйымның СБ мамандарының өздеріне орындауға тура келеді. Күзет сигнал беру жүйесін жобалау кезінде қауіпсіздіктің бүкіл жүйесінің жүріс-тұрысының белгілі бір сценарийге байланысты дабыл сигналының жұмыс жасауын бірден байланыстырып қою керек. Мысалы, қозғалыс көрсеткішінің түнгі уақытта жұмыс жасауы бір

уақытта камераның көрсеткіш жағына бұрылуы, жазу режимін дискреттіден үзіліссіз режимге өтуі, өту есіктерін бұғаттау ауысым күзет сигнал беруінің пультіндегі сигналды қоздырады. Өрт көрсеткіштерін өрт өшіру жүйесі мен жұмысшыларға қатты байланыс арқылы жария етуді бірден байланыстыру керек.

3.5.3 Сақтау жүйесі. Сақтау жүйесі (материалды құндылықтарды сақтау) ұйымның түріне өте қатты тәуелді. Қолма-қол ақшамен операциялар жүргізетін банктер үшін сейфтердің бір түрі, ал бағдарламалық қамтамасыз етуді шығаратын компанияларға басқа түрі қажет екені айдан анық. Кез келген жағдайда сақталатын объектілердің физикалық көлемі, физикалық немесе электрондық бұзуға деген сақтау орнының тұрақтылығы, өртке тұрақтылығы, алып жүру қабілеті, монтаж жасырылынуын анықтап алу керек.

3.5.4 Бақылау жүйесінің тұрақтылығы. Физикалық тұрақтылық жүйесінің барлық компоненттерінің интеграциясы туралы сұрақ әрбір жағдай үшін бөлек шешіледі және ортақ шешім болмайды. Бұл сұрақтың бөлек жағдайлардағы оң шешімі пайда емес, зиян әкелуі мүмкін. Шынында, шынайы жағдайларда әрқашан орны бар бөлек көрсеткіштер мен тұтас жүйенің аймақтық таралуы байланыс мәселесін көтереді. Мысалы, көрсеткіштің өзін алдағаннан гөрі бұзушы болып табылатын аймаққа кірген қызметкер үшін орталық сигнал беру мен көрсеткіштің байланыс жүйесін қатардан шығару оңайырақ.

Көрсеткіштердің біреуін немесе байланыс жүйесін қатардан шығарудың бір нұсқасын таңдау жүйенің пішін үйлесіміне тәуелді. Ең оңай мысал – өткелді ашу көрсеткіші. Егер көрсеткіш (немесе байланыс желісі) қызмет көрсетуден бас тартса, құлып не істеуі қажет? Жауап анық сияқты – көрсеткішті жөндегенше өткелді бұғаттау – жер сілкіну немесе өрт кезінде өлердей қауіп тудыруы мүмкін (адамдар бұғатталып қалады). Осылайша, шешім ұйымның, ғимараттың және тағы басқа параметрлердің жұмыс ерекшелігін есептеу қажет.

4 Қауіпсіздік жүйесі шектерінде жұмысшылармен (персоналмен) және құрылғымен жұмыс жасау

Қолданылатын құрылғының барлық қызметтерін мұқият зерттеу және жұмысшылармен әдістемелік жұмыс жасау ақпараттық қауіпсіздікте өте маңызды сақтандыратын шара болып табылады.

4.1 Қызметкерлермен айналысу

Жұмысшылардың қауіпсіздігі туралы сөз қозғағанда, екі түсінікті түсіну керек – ақпараттық ресурс және адам ретінде жұмысшылар қауіпсіздігін және

бастау ретінде жұмысшылардан қорғау немесе ақпараттық жүйелерде қаскүнемдік әсерлер негізі.

Апат жағдайында жұмысшыларды қорғау сұрағына бөлек назар аударылады. Қаскүнемдердің жұмысшыларға шабуыл, қауіп-қатер, бопсалау және т.с.с. әсерлері – бұл қылмыстық құқық нысаны және ол өкілетті мемлекеттік органдардың қызмет бабында, олар кез келген жағдайда екінші дәрежелі рөлді ойнайтын АҚ қызметімен бірге жұмыс істей алады. Белгілі бір жағдайды ұйымдастыру үшін басқаша болуы мүмкін және мұндай сұрақтар өзіндік қауіпсіздік қызметімен шешіледі, бірақ бұл жағдайда барлық шаралар өтетін курстың шегінен шығып кетеді.

Басқа көзқарасты жұмысшыларға ақпараттық жүйелерге деген қаскүнемдік әсерлердің көзі ретінде тарату керек немесе жұмысшылардың жете білмеушілік, қате, немқұрайлық немесе басқа ықпалдары ұйымның қауіпсіздігіне қатер болып табылады.

Жұмысшылар талдаудың басы жұмысқа қабылдаудан басталады. Жұмысшылармен айналысатын бөлімшеде адамдарды қабылдауда өзіндік талаптары бар, бірақ ҚҚ белсенді қатысуы керек. Бұл кезде қабылданатын адамның мүмкін бағасы екі бөлімнен тұруы керек – алдыңғы тәжірибесінен және қазіргі ақпараттан.

Алдыңғы тәжирибесі туралы ақпаратты жинау жүйесі (кәсіптік тәжірибе, білім, жеке қасиеттер, алдыңғы жұмыс орнынан ресми және ресми емес мінездемелер), мүмкіндігінше, үміттенушінің алдыңғы жұмыс орнынан СБ қызметтерімен байланыстары; ақпаратты талдау – қандай қасиеттер оң, ал қандай қасиеттер теріс болып табылады. Айталық, үміттенушінің алдыңғы жұмыс орнында ұйымның өндіру ерекшеліктерімен бөлісу. Бұл оң мінездеме ме, әлде теріс пе? Бір жағынан, ол барлық жиған-терген тәжірибесін жаңа жұмыс орнында қолданады деп күтіледі, ал екінші жағынан, келесіде жұмыс ауыстырғанда жұмыс істеген ұйымы туралы айтып бермейтініне кепіл жоқ.

Үміттенушінің қазіргі статусы оның техникалық дайындығы және ақпараттық жүйелермен жұмыс жасай алу қабілеті жағынан тексерілуі керек, сондай-ақ тұлғаның дамуы барысында психологиялық құрылымы мен мінез-құлығының дамуы (соның ішінде ұжымда қатынас кезінде ыңғайсыздықтар, жауыздық ниеттер). Бұл процеске психологтың қатысуы мүмкін.

Үміттенушінің қабілеттерін тексеру тестінің бірі болып құпия сөзге тест болып табылады. Ақпараттық жүйелерде парольді енгізуге шақыруды боямалайтын бағдарламалық қамтамасыз ету болып табылады, ол парольді сақтайды және қауіпсіздік қызметінің өкіліне көрсетуі мүмкін. Үміттенушіге сынақ алдында пайдаланушылар парольдеріне деген ұйымның талаптарымен танысуы мүмкін. Ары қарай үміткерге өзі ойлап тауып, парольді енгізу ұсынылады (мысалы, себеп ретінде жүйеде тесттік жұмыс мүмкіндігі көрсетіледі). Парольді енгізгеннен кейін үміткерден жүйеге қайта кіруін сұрауы мүмкін. Бұл кезде жүйе оған қате, қауіпсіздік қызметінен көмек сұрауы туралы немесе жаңа ғана жасалған кіруі соңғы жасалған кіруіне сәйкес

келмейтіні туралы немесе соңғы кіруден кейінгі парольді екі-үш рет енгізу дұрыс болмағаны туралы хабар шығарады. Бұл жағдайдағы сақ болу факторлары төмендегідей:

- Құпия сөз ойлап табу бойынша өте ұзақ ойлау. Жұмыс тәжірибесі бар пайдаланушы құпия сөзді 30-60 секундта ойлап табады.
- «Құпия сөз таңдауға көмектесіңізші» деген сияқты сұраныстары. Бұл-тұтынушының құпия сөздің құпияда сақталуы қажетінің маңыздылығын аңғармайтынын көрсетеді.
- Құпия сөз мақұлдау кезіндегі қателер. Егер тұтынушы екі рет 10 символдан тұратын парольді қатесіз енгізуге шамасы жетпесе бұл негативті белгі.
- Өте қарапайым енгізілген құпия сөз. Егер үміткер ұйымның құпия сөзге деген талабымен таныса отырып, бәрібір оларды орындамаса бұл – жағымсыз тенденция.
- Жүйеге қайта кірген кездегі дабыл хабарламаларына реакцияның жоқ болуы. Егер жүйе тұтынушыға қателік жайында ақпарат беріп, кейін оны жіберіп соңғы кіруінің дұрыс емес уақыты мен күнін берсе, онда қауіпсіздік қызметіне хабарлау керек.

Егер кандидат жұмысқа қабылданып және тұтынушы – ақпараттық кеңістік субъектісі болса, онда ақпараттық қауіпсіздік қызметі өзіне осы тұтынушыны бақылап, қателіктерін ескере алатындай деңгейде құқықтық кеңістік құруы тиіс. Ол үшін келесі шараларды орындау керек:

- ақпараттық қауіпсіздік саласындағы бар нормативтермен таныстырып, кейін олардың білмегеніне сілтеме жасамайтындай жағдай жасап, қолхат алған дұрыс; егер үміткер ұйыммен келісім шартқа отырған болса, онда ақпараттық қауіпсіздіктің бірнеше пункті қосылуы тиіс. Мысалы, субъекті меңгерушінің цифрлық қолын қағаздағыдай етіп мойындауға міндеттенеді;
- егер ұйым өз ақпаратының конфиденциалдылығын алға тартса, субъекті қол қоятын қосымшалар тізіміне енгізген жөн. Алайда мемлекет заңдарының сақталуында қадағалаған жөн, себебі, субъектіге жүктелетін міндеттер оның коституциялық құқықтарын бұзбауы тиіс;
- егер ұйым қызметкердің жұмыс барысына араласқысы келсе, мысалы, элетронды поштасын тексеру, интернет сайттарында болуы т.с.с., онда қызметкер ол жайында ескертілуі тиіс;
- егер қызметкер құзырына бір персоналды компьютер берілсе, онда оған бұл бірлік ұйым меншігі және оны қолдану саясатын ұйымның анықтайтынын жеткізу керек. Осында компьютерге оқу бағдарламалары, музыка және ойындардың орнатылуы ұйым мақсаттарына сәйкес емес. Ал осы қызметкер берілген компьютерге жауапты болғандықтан нормативтерге сәйкестігін және ақпараттық қауіпсіздіктің сақталуын орындауы тиіс;

- егер бұл компьютерде екі немесе одан да көп адам жұмыс істесе, берілген компьютердегі ақпараттық қауіпсіздіктің сақталуы талаптарын орындауға бір жауапты адамды қойған дұрыс.

4.2 Қызметкерлермен әдістемелік жұмыс

Кәсіпорынның ақпараттық кеңістігі бір орында тұрмайтындықтан, қызметкерлерді жаңа ақпараттық жүйелер жұмысына және сол жүйелердегі қауіпсіздік шараларына ұдайы оқытуды талап етеді. Сондай-ақ, қастандық ойлаушылар қолданатын технологиялардың дамуы тұтынушылардан шабуылдар жайында қосымша, анағұрлым жетік білім талап етуі мүмкін. Бұл қызметкерлерге осы тақырыпта әрдайым семинарлар өткізіп, қажетті іс-шаралар жайында оперативті хабарлау жүйесін ойластыру керек дегенді білдіреді. Үлкен тармақталған корпорациялар үшін осындай әдістемелік материалдарды дайындап, сол материалдармен қызметкерлердің міндетті түрдегі танысуы әдісін қолданған жөн.

Қызметкерлердің жұмысының сапасына қарамастан олардың жұмысын периодты түрде тексеріп отыру керек. Тексерулер «таңдамалы» болуы мүмкін. Тексеру көлемінің диапазоны әртүрлі болуы мүмкін. Осындай тексерулер барысында, тұтынушылардың жұмысындағы қандай да бір қателіктер, соның ішінде тұтынушы күнәсінен болмайтын қателіктер, табылуы мүмкін. Инциденттердің зерттелуі қалай жүргізілетіндігін кейінірек қарастырамыз. Қандай болмасын бұзушылықтағы тұтынушының күнә деңгейін және жазалау көлемін нақты ұйымның құзырлы өкілдері анықтау керек. Кішкентай қателік үшін әрдайым үлкен жаза беру - әрдайым мәселенің жақсы шешімі бола бермейді. Мынандай мазмұндағы электрондық хат жақсы профилактика болуы мүмкін: «Сіз кеше WWW.XXX.COM сайтында болып онда жұмыс уақытының 42 минутын жұмсадыңыз. Жағымсыздықтар болмас үшін сіздің жұмысыңызға қатысы жоқ сайттарды қолданбауыңызға кеңес береміз. Қауіпсіздік қызметі». – осындай хат жақсы профилактика болады.

Алайда, осындай инцидент формальды түрде «кешірілсе» де, ол қандай да бір «қара тізімде» белгіленуі керек.

Қызметкерлермен жұмыс істеген кездегі ең басты сұрақтардың бірі өзара қарым-қатынас кезіндегі жұмысшыны идентификациялау. Бірнеше ондаған адамы бар ұйымда, қауіпсіздік қызметкері әр қызметкерді жеке білуі мүмкін, ал бірақ персонал саны 1000 және одан да көп болатын үлкен ұйымдарда, әсіресе жаңа қызметкерлер үшін тұлғаны тану сұрағы қауіпсіздік қызметі жұмысында қолданылуы мүмкін осал тұстары болып табылады. Мысалы, телефонмен тұтынушының парольды ауыстыру жайындағы өтініші. Шын тұтынушы мен аталған есім арасындағы сәйкестікті қалай тексеруге болады? Мұндай кезде уақытша парольдар жүйесін қолдануға болады, Интернетте мәселенің екі шешім жолы ұсынылады:

- Тексеру сұрағы. Тұтынушының тіркеу жазбасын тіркеген кезде, рұқсат тек қана әкімшіде ғана бар, сұрақ және соған сәйкес жауап, жауабын тек қана тұтынушы біледі, енгізіледі. Сондай жағдайда құпия сөзді ауыстыру алдында әкімші тұтынушыны тексеру сұрағына берген жауабы бойынша аутентификациялайды.
- Балама кері байланыс. Тұтынушы қоңырауынан кейін әкімші телефон нөмірін тіркеп, оның дұрыстығын тексереді және тұтынушыға өзі қоңырау соғады.

Уақытша құпия сөздің ерекше болғанының маңыздылығын ескерген жөн.

4.3 Кәсіпорынның бұрынғы кадрлық қызметкерлері

Ұйымнан кеткелі жүрген қызметкермен қарым-қатынас мәселесі маңызды сұрақ күйінде қалып отыр. Осындай жағдайда, қызметкердің тіркеу нөмірін берілген ақпараттық жүйенің тұтынушысы ретінде блоктау мен өшіру мәселелері бойынша біраз техникалық іс-шаралар өткізілуі тиіс. Бірақ ол үшін ақпараттық қауіпсіздік қызметі (АҚҚ) кемінде осы қызметшінің жұмыстан шығатыны жайында ақпараттану керек. Содай-ақ, осы жағдайда қызметкерлермен жұмыс жайындағы бөлімшемен байланысу керек.

Жұмыстан кеттін біраз және барлық қызметкерлер үшін ұйымдағы қызметі мен оған артылған міндеттердің жалғастырылуы жайында әңгімелесу өткізген жөн. Жұмыстан кететін қызметкердің ұйымда қандай болмасын қосымша мүддесі қалуы мүмкін. Қандай жағдай болса да, жұмыстан кететін қызметкер мен ұйым арасындағы жақсы қарым-қатынастарды сақтаған жөн. Ұйымның қауіпсіздік қызметі жаңа жерге жұмысқа орналасатын бұрынғы қызметкерлердің мінездеме сұраныстарымен не істеу керектігін шешуі тиіс. Ондай мәліметті бермесе де болады, алайда мұндай жағдайда басқай ұйымдардың өз сұраныстарына жауап беруін күтпеген жөн. Осындай жағдайда кәсіпорынның қауіпсіздік қызметі алдын ала сала бойынша берілетін мәліметтердің тізімін жасауы керек.

4.4 Құрылғымен жұмыс

Құрылғының қауіпсіздігі мынандай нұсқалардан құрылады: құрылғы өзі қауіпті болып табылады немесе құрылғыға қауіп бағытталуы мүмкін.

Ақпараттық технологиялар құрылғысын сатып алған ұйым оған сенуге мәжбүр, себебі көп жағдайда бұл ұйым күрделі аппараттың құжатталмаған кемшіліктерін анықтауға арналған техникалық мүмкіндіктерінің болмауымен байланысты. Мұндай кемшіліктердің болуының басты себебі – кәсіпорындар арасындағы бәсекелестік және кейбір елдердің саясатымен байланысты. Ұйымда жоғарғы мамандандырылған ақпараттық технологиялар немесе ақпараттық қауіпсіздік мамандары болған кезде де, олар аппаратық

кемшіліктердің барын немесе жоғын мақұлдай бермейді. Ақпараттық кемшіліктерді анықтауда арнайы әдістер мен құралдардан басқа жоғары арнайы мамандандаырылған мамандары бар зертханалар қажет.

Осы себепті құрылғыларды мемлекеттің құзырлы орындары сертификаттағаннан кейін сатып алған дұрыс, алайда ондай орын жоқ болған жағдайда, өз беделі үшін жұмыс істейтін және апаттың дұрыс істемеуіне байланысты дау-жанжалдарды қаламайтын белгілі өндірушілерден (брэнд) сатып алған дұрыс. Берілген жағдайдағы тауар бағасының өсуі - кәсіпорын ішіндегі «бесінші коллоннасы» болмағандықтан төленетін кепілдік деп түсінген дұрыс.

Егер құрылғының ішінде қасақана оймен істелінген жиынтықталмаған мүмкіндіктері жоқ деп есептегеннің өзінде, ақпараттық қауіпсіздікте әлсіз тұсы да болуы мүмкін. Осындай әлсіздікке әдетте ПЭМИН (БЭСЖБ) – бөгде электромагниттік сәулелену және бағыттау терминін қолданады. Бұл құбылыс құрылғы өз жұмысы барысында қоршаған ортаға бақылаусыз түрде қандай да бір түрде ақпарат бөлуіне негізделеді және сол ақпаратты қағып алуға, өңдеуге және заңсыз түрде қолдануға болады. Тұтынушылардың мониторлары жұмыс істеп тұрғандағы генерацияланатын және деректерді беру ортасында (желілер, сымдар, кабельдер және т.б.) пайда болатын БЭСЖБ ақпараттық технологияларда үлкен назар аудартып отыр. Алайда, БЭСЖБ-дан қорғау үшін күрделі және қымбат құрылғыны сатып алмастан бұрын, тәуекелдерге талдау жүргізу керек:

- байланыс желілерімен беру кезінде деректерді шифрлау жеткілікті болуы мүмкін. Осы жағдайда электромагнитті бағыттауларды қағып алатын күрделі жабдық түгіл, қастандық ойлаушының тікелей пакеттерді қағып алушыны енгізуі де ешқандай нәтиже бермейді;
- қашықта отырып монитор экранынан ақпаратты қағып алу үшін өте қымбат құрылғы қажет. Бас жүйелік әкімшінің иығы арқылы қарағанның өзінде де, бәсекелес не алуы мүмкін?

Мүмкін, бұл ақпаратты бұдан да қарапайым жолмен алуға болатын шығар.

Әдетте бұл жағдай орташа кәсіпорын үшін сарапталатынын ескерген жөн. Егер мысалы, «мемлекеттік құпия» класындағы ақпарат электронды түрде сақталатын қорғаныс министрлігі жайында айтатын болсақ, онда әңгіме басқаша болмақ.

Ұйым құрылғыларына сенімді және қажетті деңгейде жұмыс істеп тұруына жағдай жасалды делік. Алайда, кәсіпорынның ақпарат кеңістігіне қызметкерлер мен қонақтар алып келетін бөгде құрылғының ену мүмкіндігі бар. Берілген жағдайда, қорғанысты екі сатымен эшелондау керек: ғимаратқа құрылғының енгізілуін қадағалау керек және ақпараттық желіге бөгде қосылулардың болуын тексеру.

Сыртқы тасушылар (құрылғы қатарына қосуға болатын), сондай-ақ сытрқы тасушыларға жазуға/оқуға арналған және осындай құрылғыларды

сыртқы қосылуларға арналған порттар ерекше назарға ие болу керек. Осы жағдайда сырқы тасушылар қауіпті ақпараттық объектілер/субъектілерді құпия ақпаратты ала отырып, ақпараттық кеңістікке енгізуші болуы мүмкін. Еркін порттарды (COM, LPT, USB инфрақызыл байланыс т.с.с.), оқу/жазу құралдарын өшіру/блоктау немесе физикалық түрде өшіру сенімді болмақ. Алайда, бір немесе бірнеше сыртқы тасушылармен жұмыс істеуге құзыры бар бөлек қызметті құрған жөн. Қызметтің міндеттеріне мыналар кіреді:

- алып келінген сыртқы тасушыда қауіпті элементтердің (вирустар, троян бағдарламалары, бөгде бағдарламалық қамтамасыз ету т.б.) барын тексеру;
- ақпарат бағытталған тұтынушыға, серверге, станцияға, сыртқы тасушыдан ақпаратты электронды түрде ғана жеткізу немесе көшірмесін беру;
- тұтынушыдан, ұйымнан сытрқы тасушыда шығаруға бағытталған ақпаратты алу;
- шығаруға арналған ақпарат құрамында құпия ақпарат болмауын тексеру және ақпаратты сыртқа тасушыға жазу.

Бұл қызмет үшін жалғыз рұқсат критикалық ақпаратты резервті көшірмесін алуға арналған жұмыс регламенті бөлек қызмет қана ерекшелік болуы мүмкін.

Ақпарат бағыты бойынша жеткізілгеннен кейін, сытрқы тасушылардан ақпаратты өшіру мәселесі маңызды болып отыр. Жойылған ақпаратты сыртқы тасушыдан қалпына келтіруге арналған шығын мәселесі қалпына келтіруге тиіс ақпараттың құнына байланысты. Қандай жағдай болса да, көп рет қайта жазу немесе корпустың физикалық бұзылуы ақпаратты қалпына келтіру кепілдігі бола алмайды. Егер ақпаратты кепілді түрде жою мәселесі маңызды болса, арнайы аппаратура сатып алу мәселесін сараптау керек.

Ақпараттық технологиялар құралғыларының басқа маңызды ерекшелігі ақпараттық қауіпсіздікке әсер ететін сипаттамалары бар: олар өзіндік құнды, яғни басқа құрылғыға қарағанда өзіндік құны бар, көптеген ұсақ бөлшектерінің болуы.

5 Тәуекелдерді басқару

5.1 Кәсіпорынның ақпараттық қауіпсіздігі мәселесі

Кәсіпорынның ақпараттық қауіпсіздігі мәселесін әкімшілік деңгейде, яғни ұйымның басшылығы атқаратын шараларды қарастырайық. Әкімшілік деңгейдегі барлық шаралардың негізінде, әдетте кәсіпорынның ақпараттық қауіпсіздігі саясаты деп аталатын құжат жатыр. Ақпараттық қауіпсіздік деп ақпараттық ресурстарды қорғауға бағытталған шаралар мен басқарушылық құжаттық шешімдер жиынтығы түсіндіріледі.

Ақпараттық қауіпсіздікті қамтамасыз етудің мұқият ойластырылуынан басқарудың басқа да деңгейлерінің: процедуралық, бағдарламалы-техникалық,

әсерлігі байланысты. Берілген құжатты құрастырғандағы басты қиындық – бөгделердің тәжірибесін қолданудың мәселелігі, себебі, қауіпсіздік саясаты өндіргіш қорлар мен берілген кәсіпорынның функционалды байланыстарымен тығыз байланысты. Сондай-ақ, Қазақстан мемлекет ретінде ондай типті құжат жоқ. Осы ойға ең жақын «ҚР ақпараттық қауіпсіздік доктринасын» алсақ болады, алайда ол өте жалпы сипатта.

Осыған байланысты ақпараттық қауіпсіздіктің саясатын құрастыруға шет елдер тәжірибесін қолданған жөн. Осы аспект егжей-тегжейлі 2.0 нұсқалы 22 мамыр 1998 ж. Британ BS779:1995 стандартының «Ақпараттық технологиялардың қауіпсіздігін бағалайтын жалпы талаптарында» құрастырылған. Онда ұйымның ақпараттық қауіпсіздігін сипаттайтын құжатқа келесі пункттерді қосу ұсынылады:

- бастапқы, жоғарғы басшылықтың ақпараттық қауіпсіздік мәселелеріне қызығуын растайтын;
- ұйымдастырушылық, ақпараттық қауіпсіздік саласындағы жұмыстарға жауапты бөлімшелердің, комиссиялардың, топтардың және т.б. сипаттамаларын қосатын;
- жіктелу, кәсіпорындағы материалды және ақпаратты ресурстар және олардың қажетті қорғаныс деңгейі;
- штатты, қызметкерлерге қолданылатын қауіпсіздік шараларын сипаттайтын (ақпараттық қауіпсіздік деңгейінде қарастырғандағы лауазымдар сипаты, оқудың жүргізілуі, режимнің бұзылуына әсер ету тәртібі және т.б.);
- ақпараттың физикалық қорғалуын мәлімдейтін бөлім;
- басқару бөлімі, деректерді беру желілері мен компьютерді басқару жолдарын сипаттайтын;
- өндірістік ақпарат шекаралары ережелерін айқындайтын бөлім;
- жүйелердің құралуы мен енгізілу тәртібін сипаттайтын бөлім;
- ұйымның үздіксіз жұмысын қамтамасыз етуге бағытталаған шаралар сипаты бөлімі;
- ақпараттық қауіпсіздік саясатының ағымдағы заңдарға сәйкестігін растайтын, заңгерлік бөлім.

Ақпараттық қауіпсіздік саясатын құрудың шетелдік құжаттардың негіз ретінде ұсынылуы түсініспеушіліктерге алып келуі мүмкін.

BS779:1995 стандарты нұсқаулығынан көрініп тұрғандай, олар жалпы сипатта және үй салудың барлық ережелері бірдей болатындығы сияқты тек ағымдағы заңдар мен ереже, нормалар және т.с.с сәйкес толықтырылады сондықтан, бұл нұсқаулықтар жердің кез келген нүктесіндегі кәсіпорындарға қолданыла алады. Сондай-ақ, нұсқаулықтың соңғы бөлімі ақпараттық қауіпсіздік саясаты соның негізінде құралатын елдің ағымдағы заңдарына қайшы келмейтіндігін растайды.

Сонымен, кәсіпорынның ақпараттық қауіпсіздік саясаты бұл соның негізінде қауіпсіздікті қамтамасыз етеу жүйесі құрылатын құжат. Өз кезегінде құжат тәуекелдерді сараптау негізінде құралады, сараптау түгел жүргізілген

сайын құжат та тиімді болады. Сараптау барлық негізгі ресурстарда, соның ішінде, материалдық базамен адам ресурстарында да жүргізіледі. Қауіпсіздік саясаты кәсіпорын ерекшеліктері мен мемлекеттің заңшығарушылық негізіне сәйкес құрылады.

5.2 Негізгі ұғымдар

Әр жүйенің немесе өнімнің артықшылықтары мен кемшіліктеріне тоқталмай-ақ, мынаны ескеру қажет – ақпараттық ресурстарды қорғау ойластырылу керек және оның эффективті болуы шарт. Себебі ол белгілі бір деңгейде ұйымның ресурстарын сақтауға бағытталған, соның ішінде финанстық ресурстарды. Осы мәселеде жақсы жарнамаланған қымбат ақпараттық қауіпсіздік құрылғысын сатып алу, ақпараттық қауіпсіздікке қатысты кәсіпорын мақсаттарына қайшы келуі мүмкін.

Әдетте компьютерді қорғауға кеткен қосынды сомма компьютердің операциялық жүйесімен қосқандағы өз бағасынан да асып түседі. (Құпия құжаттармен жұмыс істейтін оператордың қауіпсіздік қазметі сол құрылғыға жұмсаған соммасынан ондаған есе аз соммаға ақпарат беруге дайын екендігін ескерген жөн). Сонымен құпия деректерді таратуға байланысты шығын еш жерде айтылмайды.

Кейбір ақпараттық қауіпсіздікке байланысты басқарушы құжаттар қажетті қорғаныс деңгейінің анықталуының негізгі принциптерін жанама немесе формальды түрде ғана көрсетеді. Әдетте былай құрылады: «қорғауға кеткен шығындар соммасы шабуылдан тиген шығыннан аспауы керек». Басқа принцип сирек қолданылады: «Қорғанысты бұзуға кеткен қастандық ойлаушылардың шығындары, бұл шабуылдар нәтижесінің пайдасынан асуы керек». Бірінші қағида пайда табуға негізделген коммерциялық органдарға лайық, ал екіншісі мемлекеттік құпиялармен жұмыс істейтін ұйымдарға лайық.

Ақпаратты қорғауға бағытталған құрылғыларды сатып алуға кеткен шығындарды ескерсек, өндірістік шығындарды есептеу оңайырақ, ал қауіпсіздікті қамтамасыз етуге кететін шығындарды есептеу қиынырақ. Бәрімен қоса бұл жерде өзінің ерекшелігі бар. Егер, батыс саясаткерлерін әшкерелейтін ақпараттар олардың жұмыстан кетуіне алып келсе, ТМД елдерінде керісінше саясаткерге танымалдылық қосуы мүмкін.

Тәуекелділікті басқарумен тек қана ғаламдық модификацияны жоспарлау кезінде емес, сондай-ақ одан да кіші жағдайларда жасаған дұрыс. Мысалы, ұйым шет елдік ұсынушыдан автоматтық жүйені сатып алды, ал бірақ ол модификацияға ашық. Ақпараттық қауіпсіздікті қамтамасыз етудің элементтерінің бірі жүйенің тіркеу журналын тексеру болып табылады. Алайда жүйенің стандартты түсімі келесідей болады: журнал толық емес және қосымша ақпаратты подсистемалардан жинап, қосымша жұмыс істеуге тура келеді. Берілген мәселенің келесідей балама шешімдері мүмкін:

- қажетті жұмыстарды орындау үшін операторды жұмысқа алу;
- өндірушіден кең тіркеу журналы бар жүйенің жаңаруына тапсырыс беру;
- өз програмистеріне қосымша модуль құруды тапсыру.

Берілгеннен қажетті нұсқаны тек қана жүйені тіркеу журналының сараптауынынан кейін ғана таңдаған жөн. Себебі шабуыл кезіндегі жобалардың іске асырылуы шабуылдан кейін келетін шығындардан асуы мүмкін.

АҚ (ақпараттық қауіпсіздік) бағытының бөлігі ретінде тәуекелдер бағасы – тәуекелдікті басқару, қауіпсіздіктің құрылымындағы маңызды құрал болып саналады. Бірақ бұл құралды тиімді қолдану үшін бірнеше шарттар қатарын орындау керек. Мысалы, сапалықтан сандық түсініктерге өту. Егер «ақпаратқа рұқсат алу бірлестіктің күйреуіне әкеліп соғады» деген тұжырым жасасақ бұл сапалық түсінік, яғни сапалық сипат. Ал сандық сипаты мынадай бола алады «ақпараттың жариялануы n_1 тұтынушыдан төлем қажет, сот үрдістеріне мұнша шығын төленуі керек». Егер бірлестікте активтерді сұрыптау жүргізілсе, бұл процесс біршама жеңілдемек.

Тәуекелдікті басқару – дегеніміз бағаны сараптау, төмендету, жоюды анықтау процесі. Ол өз кезегінде келесі мәселелерді қамтиды немесе келесі сұрақтарға жауап береді:

а) егер бірдеңе болып қалса, онда шығын көлемі қандай болады;

б) ол қаншалықты жиі қайталанады;

в) осы сұрақтың жауабына қаншалықты сенімдіміз;

г) жиілігі мен ықтималдығын төмендету үшін не істеу қажет;

д) қолданатын шара қанша шығын әкеледі;

е) қабылданатын іс шара қаншалықты тиімді.

Тәуекел ықтималдыққа бағынады. Алғашқы үш сұрақ ықтимал болған сайын тәуекел көп, ал ықтималдықтар аз болған сайын тәуекел де аз болмақ. Ақпараттық актив – жұмыста қолданылатын және өзінен кіші жиындардан тұратын ақпараттар жиынтығы. Мүмкін болатын шығындар көлемі сан ретінде бағалануы керек.

- Ақпарат алмасу құны.
- Бағдарламалық қамтамасыздандыруды қостаудың алмасу құны.
- Мақсаттылық, рұқсаттылықтың күйреу құны.

Ақпаратты және бағдарламалық қамтамасыздандырудың бағасы бөлек, қарапайым жүргізіледі.

5.3 Тәуекелді басқарудың жалпы әдістемесі

Тәуекелдікті басқарумен айналысатын ұйымдардың стандартты әдістемелері:

- Тәуекелдікті басқарудың саясатын анықтау, оны ақшалай қамтамасыз ету. Еңбегіне төлеуден басқа оны оқыту, автоматты құралдармен қамтамасыз ету, жаңа әдістер мен тәсілдерді игеру керек болады.
- Тәуекелді бағалауды жүргізуге керекті құралдар мен әдістерді анықтау. Бұл жерде тәуекелді бағасын шығарғанда барлық керекті құралдарды іске қоспас бұын толық сенімді болу керек.
- Меншіктеу және тәуекелді өлшеу. Бірінші сатыда жұмысты қолдану аясын анықтап алу керек. Яғни туып тұрған қауіптерді, ақпараттық активтер мен олардың мағыналарын білу керек. Сапалы бағалау үшін кесте берілуі мүмкін. Бұл кестенің жолдарында активтер, ал бағаналарында жоғары, орта, төмен тәуекел деңгейлері көрсетіледі.
- Тәуекел тиімділігінің талаптарын орнату. Алынған мәліметтер негізінде мамандар басқарушылармен бірге тәуекел тиімділігін қабылданған тәсіл бойынша анықтау керек. Мысалы, 100000 АҚШ долларына тең тәуекелді тиімді емес деп қабылдау.
- Тәуекелді азайту және одан алыстау. Қабылданған талаптар бойынша тәуекелдіктің дәлсіздігін анықтау маңызды. Оны жою тәсілдерін анықтау. Бұған тәуекелдікті жоюдың құралдарын таңдап алу, құралдардың әрекеттілік бағасын анықтаудан тұрады.
- Тәуекелді басқару жұмыстарының мониторингісі. Мұнда қолданып отырған тәсілдердің тиімділігін, сыртқы және ішкі жағдайлардың ауысуына байланысты қайта бағалаулардан тұрады.

Тәуекелді басқарудың үш әдісі бар. Олар:
- Сапалы бағалау әдісі.
- Дәстүрлі әдіс, сандық модель деп те аталады.
- Атаулы әдіс «Миор нәтижесінің жалпы құндық әдісі».

5.4 Сапалы бағалау моделі

Сапалы бағалау көбіне кестені толтырумен түсіндіріледі. Мұнда ақ, қара, сұр түстер қолданылады.

3 кесте – Қауіп салдарының сапалы бағалануы

Шабуыл тәуекелі	Маңызды актив	Критикалық актив	Өмірлік актив
Төменгі			
Орташа			
Жоғары			

Кесте толтырушының интуициялық түсінігі, ұйымның білікті қызметкерлерінің анкеталары негізінде артық көру мәліметтерімен

толтырылады. Шешім объектіге арналған нақты ұйымдардың тәуелділігімен қабылданады.

Негізгі жолақ деп аталатын қысқартылған әдісті қолдануға да болады. Мұнда бірлестік қауіпсіздік жүйесінің қарастырылу жағдайын талдайды, оны өздері жасаған жүйемен салыстырады. Егер артта қалушылық байқалса, онда жағдайды қалпына келтіру жүргізіледі. Айталық барлық компаниялар электронды поштамен сандық сертификат үшін шығын шығарды. Онда нақты компания оны алудың қиын емес жолын іздеуі қажет емес. Алайда үлкен компания шабуылды анықтаған балса, онда кішірек компания үшін маңызды шығын жасауға негіз жоқ.

Тәуекелді бағалаудағы сапалы бағалау моделінің жағымды жақтары мынада:

- Есептеу жылдам әрі қысқа.
- Активке қаржы меншіктеудің маңыздылығы жоқ.
- Қауіптің пайда болу жиілігі мен оның нақты шығын көлемін есептеудің қажетсіздігі.
- Ұсынылатын шаралардың тиімділігін көрсетудің қажетсіздігі.

Жағымсыз жағы нақты қауіпсіздіктің шығынын көрсету керек болмаған соң, субъективті талдау қажеттігі.

5.5 Тәуекелдің сандық моделі

Тәуекелдің сандық моделі мынадай түсініктермен жұмыс жасайды.

- Істің жылдық жиілігі, былайша айтқанда шығынның пайда болу ықтималдығы (ARO).
- Күтілетін бірлік шығыны (SLE), яғни нәтижелі жорықтың құны.
- Күтілетін жылдық шығын (ALE), көлемі.

ALE= ARO· SLE.

ARO – оқиғаның болу жиілігі; егер оқиға 5 жылда 1 рет болса, онда ARO 1/5, ал 1 жылда 3 рет болса, онда 3-ке тең.

Мысал, егер бірлестікте 100 адамның 50-і ақпараттық жүйені пайдаланып, олардың 5-і жоғары мүмкіншіліктерге ие бола отырып, мамандануы төменгі деңгейде болғандықтан ай сайын күрделі қателер жіберетін болса, онда бұл жүйе үшін

ARO=5·12=60.

Мысалы, ғимарат 10000000 АҚШ долларынан тұрады. Өрт 30% шығын әкеледі. Өрттің болу ықтималдығы жылына 10 рет болуы мүмкін. Онда SLE=10000000·0,3=300000

ALE=300000·0,1=30000.

Осыған байланысты, егер бірлестік 30000 долларды өрт болмау үшін шығындалса онда бұл тиімді шешім болмақ.

5.5.1 Оқиғаның ықтималдығын анықтау.

Формулалардың қарапайымдылығына қарамастан жоғарыда көрсетілген әдісте қиындық бар. ARO да ықтималдықты қалай анықтау керектігі қиындыққа тап болады. Егер қауіптерді категорияларға сай бөлсек, онда біраз сұрақтарға жауап табылады. Климаттық шарттар туралы мәліметтерді мемлекеттік метеорологиялық бюроға жолығу керек. Өрт жағдайлары үшін өрт сақшылары мекемелеріне, жер сілкінісі туралы сейсмикалық орталыққа жүгініп, қажет мәліметтерге қанығу керек. Сонымен бірге компьютерлік қылмыстар да бар. Ол туралы көбіне ақпарат жабық, таратылмайды. Құрал жабдық пен компьютерлік бағдарламалық қамтамасыздандырушылар мен тәуелсіз сараптама қорытындыларын да алу керек.

5.5.2 Актив құнын анықтау.

Активтерді көрнекті және көрнексіз деп алайық. Көрнекті активтерге ақпараттық технологияға қызмет ететін тәсілдері – ақпаратты қамтамасыз ету, қосымша бөліктер, жүйенің қызмет етуіне арналған іс қағаздар және жалақы жатады. Бұл активтердің құндық сипаттамалары мәлім және оңай есептелінеді. Көрнексіз яғни көзге көрінбейтін активтердің құны екі түрлі шығынды құрайды: ауыстыру шығындары немесе бағдарламалық қамтамасыз ету шығындары, рұқсаттылық пен мақсаттылықтың жойылуымен келетін шығындар. Көрнексіз активтердің шығынын анықтау қиын мәселе.

Мысалы бір топ қандай да бір мәліметтер жиынтығын алу үшін зерттеу жүргізу кезіндегі көрнексіз шығындар құнын анықтау қажет. Егер де зерттеудің қандай да бір сатысында мәліметтер жиынтығы жоғалатын болса, онда келесі тәсілдерді қолдану керек:

- Егер МЖ интеллектуалды тауар күйінше сақталған болса, яғни оны жасушылардың ойында қалған жағдайда, шығындар тек қалпына келтіру үшін операторлар еңбегіне ғана жұмсалады. Мысалы, корректрлеу, сканерлеу және т.б.
- Ал егер МЖ жойылып, сонымен бірге ештеңе қалмаса, онда тағы да сондай шығын болады. Ал оның қалпына келтірушілер үшін шығын қарастырылмайды. Қандай да бір материал сақталып, оны қайта қолдануға жараса, онда оған кететін шығын жалпы шығыннан шегеріледі.

Егер зерттеу жайлы жарияланса, онда ол топтың мүддесіне ешқандай нұқсан келтірмейді.

Егер ақпараттың жариялануы компанияның күйреуіне соқса, онда бәсекелестер үшін мұндай зерттеу жүргізу компания секілді шығынға шығады. Ал егер де топтың зерттеу барысындағы жұмысы әрбір қадамда сақтандырылып қойылса, онда шығынды қысқартуға жағдай тумақ.

Бүтіндіктің жойылуын бағалау үшін жойылудың проект немесе жұмыс үшін қандай мағынасы бар екендігін анықтап алу керек. Ол үшін зерттеудің мағыналық қателерін анықтау, персоналдың мәліметтермен жұмысындағы қателерін анықтау, құралдың қателерін анықтау керек. Банк есепшотының бір санынан кеткен қатенің арты кітапханалық 100 тіркелуді 10000 тіркелуге дейін шатастырудан да күрделі жағдайларға соқтыруы мүмкін.

Егер мәліметтер өзгерісі материалдық шығыны тура есептелсе, онда мұндай мүмкін шығынның максимумы – бүтіннің бұзылу бағасы болады. Бірақ бұнда кейде максимал шығын жайдан жай шықпауын, дәл уақытта анықтау және тоқтатыла отырып, ал кейде осы шығынның бүтін немесе толық өлшемі кетірген құнның қайтару тәсілі мен компенсациялауға мүмкіндік бар екенін ескеріп отыру керек.

Осындағы өзгерістер үлкен немесе кіші шығындарды алып келетінін тек мамандар бағалай алады. Мысалы, химиялық формуладағы өзгерісті немесе химиялық қоспаның пропорциясы алапат катастрофаға әкеліп соғады.

Рұқсат етілудің бұзылуы бүтіндей уақытпен анықталады. Берілген уақытта екі негізгі түріне рұқсат етілмейді немесе ешқашан рұқсат етілмейді. Соңғы жағдай бір және екінші жағдайға ұқсас, ал үздікті рұқсат етілмеу уақыт аралығына жіктеу керек – егер МЖ минут, сағат, күн және т.б уақыт аралығында рұқсат етілмесе қандай шығын болады.

Осындай әртүрлі мүмкін нұсқаларды қарастырғаннан шығындарды алмасу үшін, белсенділікке қауіп және әсер арасындағы байланысты орнату керек.

5.6 Миордың құндық нәтижелерінің жалпы моделі

Миор моделі сандық тәуекелдердің моделі есептеудегі жеңілдіктер үшін ойлап жасалған. Алдыңғы моделдердің негізгі кемшіліктерінің бірі болып құраушылардың ықтималдылығын анықтау схемасы болып табылады. Шынында үлкен шығынмен орындалатын жиі жағдайлар және кішкене шығынмен орындалатын жағдайлар қорғау шараларының анықталуына әртүрлі мүмкіндіктерді талап етеді. Бірақ формуладан көріп отырғанымыздай есептеулерде олар бірдей көрінеді. Мұндай модель апаттық жағдайларды ескермейді, ол шығын мағынасын бөгеліп қалудан түсіндіреді. Ол жағдайдан кейінгі уақыттың функциясы ретінде қарайды. Әрбір ақпараттық немесе белсенділік белгілеріне ұқсас топтарды категориялар деп атаймыз. Олар бірлестікке әсер етудің бастапқы мерзіміне мүмкін шығындардың өлшемін анықтайды.

Мысалы, алғашқы күннен бастап бір күнде қарапайым негізгі өндіріс орнына 50000 доллар шығын алып келеді. Өнімдерді сату контрактілермен айналысатын қарапайым қызмет орындары күніне 10000 доллар, бесінші күн бөгеуліктің алғашқысынан орындалады.

Және ары қарай солай. Содан шығынның барлық категориялары қосылады.

Кейде шығынның өсу сұлбасын график түрінде көрсету ыңғайлы. Онда категориялар «күннің ішіндегі уақыт» екі осьтің функциясы – «ақшадағы шығындар». Нәтижелік графикте екі сызық көрсетіледі:

- сәтсіз жоспардың қорғаныс өткізілімінсіз қосынды шығынның бірлестігі;

- сәтсіз жоспармен орындалатын қосынды шығын.

Осындай графикте ақпараттың қорғалуын қамтамасыз ету қажеттігі және әсерлілігі байқалады.

Модель шығынның үш түрін анықтайды: тікелей көрнекті шығын, қосымша, көрнексіз шығын. Бірінші түрдің мысалы болып өндіріске пайда әкелуге қатысатын категориялар болады, яғни өндірістік белсенділер. Екінші түр сыртқы көздермен байланысты болатын белсенділер, негізінен қолдаудың функциялары және т.б. үшінші түрде атақтың шығыны, орындалмаған уәделер негативті қоғамдық ойлар. Осындай түрлердің категорияларын есептеу әдістемесі әдістеме авторының өзіндік иелігі және онымен келісімде ғана алынады.

Ақпараттық тәуекелділіктің сараптау негізінде қорғаныс қызметінің бірлестігінің стратегиясы және тактикасын анықтауға болады. Ақпараттық тәуелділіктердің технологиясының жалпы идеяларды пайдалану үшін практикада нақты бірлестіктің куәліктері толық болу керек. Әрбір бірлестіктің ерекшелігі мақұлданған принциптерді осы бірлестік үшін ақпараттық тәуеклділіктің сараптауын талап етеді.

Тәуекелділіктерді анықтаудың типтік проблемелары. Тәуекелдіктердің жіктелімі.

Тәуекелдіктердің жіктелімін келесідей мәселелер тұрғысынан қарастыру керек:

- тәуекелділікті өлшеуге болатын талаптар бойынша;
- жағдайлардың ықтималдылық бағасымен;
- өлшеу технологиясымен.

Талаптар

Әр түрлі ақпараттық куәліктерді салыстыру критерийлерін пайдаланған уақытта алдымен сандық бағалардың жоқтығымен соқтығысамыз және сарапшылардың бағасын пайдалануға тура келеді. Көбіне сарапшылар келесідей анықтамалардың бірін таңдауы керек болады:

- мұндай ақпараттық деректер мардымсыз құндылықты көрсетеді, фирманың маңызды мәселелерін шеше алмайды және олар тез уақытта қайта қалпына келтіріледі;
- мұндай ақпараттық куәліктер фирмаға орташа құндылықты көрсетеді, себебі маңызды мәселелерді шешуге қатысады, мәліметтер қайта қалпына келтіріледі, бірақ бағасы құптарлықтай;
- мұндай ақпараттық мәліметтер фирмаға жоғары құндылықты көрсетеді, себебі өте маңызды мәселелер шешіледі, қайта қалпына келтіру бағасы өте жоғары.

Мұндай дөрекі бағалардан басқа, қасиеттердің градациясы пайдаланылады. Әдетте градациялар бес деңгейге дейін құралады.

Жағдайлардың ықтималдығы.

Ықтималдылықтың екі түсінігі пайдаланылады: объективті және субъективті ықтималдылық. Субъективті ықтималдылықта алу процесі үш периодтан құралады: дайындықты, баға алу, сараптама периоды.

Дайындықты период зерттеу нысанның қалыптасуын құрайды және субъективті ықтималдылықты анықтауда ыңғайлы тәсілді таңдайды.

Баға алу периоды таңдалған әдіс негізінде сарапшылардан алынған санды теру құраушысын құрайды.

Сараптама периоды белгілі дәлелдемелері бар қайшылық және нәтижелердің ауытқуында сарапшылардың ойы нақтылынады.

Ақпараттық қауіпсіздік шығындарын бағалау мысалы.

Вирустардан қорғау жүйесін құру жобасын қарастырайық. Мұндай жүйенің даярлығының мүмкін болатын үш дәрежесін шартты түрде анықтаймыз: бастапқы, орташа және жоғары.

БАСТАПҚЫ. Жұмыстық стансаларда вирустардан жергілікті қорғау жүйелері бар. Антивирустық бағдарламалар үнемі жаңартылып тұрады. Ең қауіпті вирустарды автоматты түрде жоятын бағдарлама орнатылған. Бұл сатыдағы негізгі мақсат – аз шығын шығарып вирустардан минималдық қорғанысты ұйымдастыру.

ОРТАША. Вирустарды табу үшін желілік бағдарлама орнатылған. Жүйелік бақылау вирустар жайында құлағдар етіп, олардың ары қарай таралуына қарсы сәйкесінше шараларды ұсынады.

ЖОҒАРЫ. Антивирустық қорғаныс жүйесі фирманың кешендік қауіпсіздік жүйесіне енгізілген. Бұл кезде қауіпсіздіктің ұйымдастырушылық түрлері техникалық түрлерден басым түседі. Ақпаратты қорғау стратегиясы фирманың іскерлігінің даму стратегиясына тәуелді анықталады.

Рұқсатты басқару жүйесінің дайындығының үш дәрежесін көрсетуге болады: бастапқы, орташа, жоғары.

7 кесте – Әртүрлі қорғаныс деңгейінің сипаттамасы

Процесс	Мақсат	Бастапқы деңгей(0)	Жоғарғы деңгей (10)
Вирустардан қорғаныс	Антивирустық қорғанысты тарату	Ештеңе жасалмайды	Антивирустық қамсыздандыруды автоматты түрде жаңарту қолданылады
Вирустардан қорғаныс	Қорғаныстың қажет деңгейін қалыптастыру	Қорғаныс дәрежесі анықталмаған	Вирустардан қорғаныс деңгейі АЖ қызметімен фирмадан тыс жағдайға

Вирустардан қорғаныс	Клиенттік орындарды серверлік антивирустық қорғаныспен қолдау	0%	орнатылады 100%
Вирустардан қорғаныс	Вирустық шабуылдардың салдарын жою	Пайдаланушы өз бетімен зақымданған файлдардф жояды, жағдайлар хаттамасы жазылмайды	АЖ қызметкерлері болған жай туралы хабардар етіледі, жағдайлар хаттамасы негізінде зерттеулер жүргізіледі

БАСТАПҚЫ дайындық дәрежесі. Серверлер, жұмыстық стансалардың сериялық нөмірлеріне есеп жүргізіледі. Ақпараттық жүйе жабдықтарын орын ауыстыруға бақылау енгізілген.

ОРТАША дайындық дәрежесі. Электрондық, механикалық құлыптар, шлюздік бөлмелер және турникеттербар. Кірісте өту орындары ұйымдастырылған, нысанда бейнебақылау жұмыс жасайды, келеңсіз жағдайлар туындаған кезде әрекет ету нұсқаулықтары құрастырылған.

ЖОҒАРЫ дайындық дәрежесі. Ақпаратты қорғау шараларының кешені толығымен белсенді қолданылады.

Ақпаратты вирустардан қорғау жүйесін құру жобасы бастапқы деңгейден (0 деңгейі) жоғары (10 деңгейі) деңгейге өтуді және дамуды қарастырады. Кестеде фирманың ақпаратты қорғау жүйесінің дамуы процесінің негізгі сипаттамалары келтірілген.

5.7 Ақпараттық қауіпсіздік шығындары

Ақпараттық қауіпсіздік жүйесінің шығынсыз жұмыс жасауын толығымен қамтамасыз ету мүмкін емес. Бірақ жүйенің деңгейінен және ақпараттық қауіпсіздік саясатынан шығындардың бір бөлігін азайтуға немесе толығымен алып тастауға болады.

Ақпараттық қауіпсіздік жүйесінің дұрыс жұмыс жасауы кезінде келесі жұмыстарға шығатын шығындарды азайтуға болады:

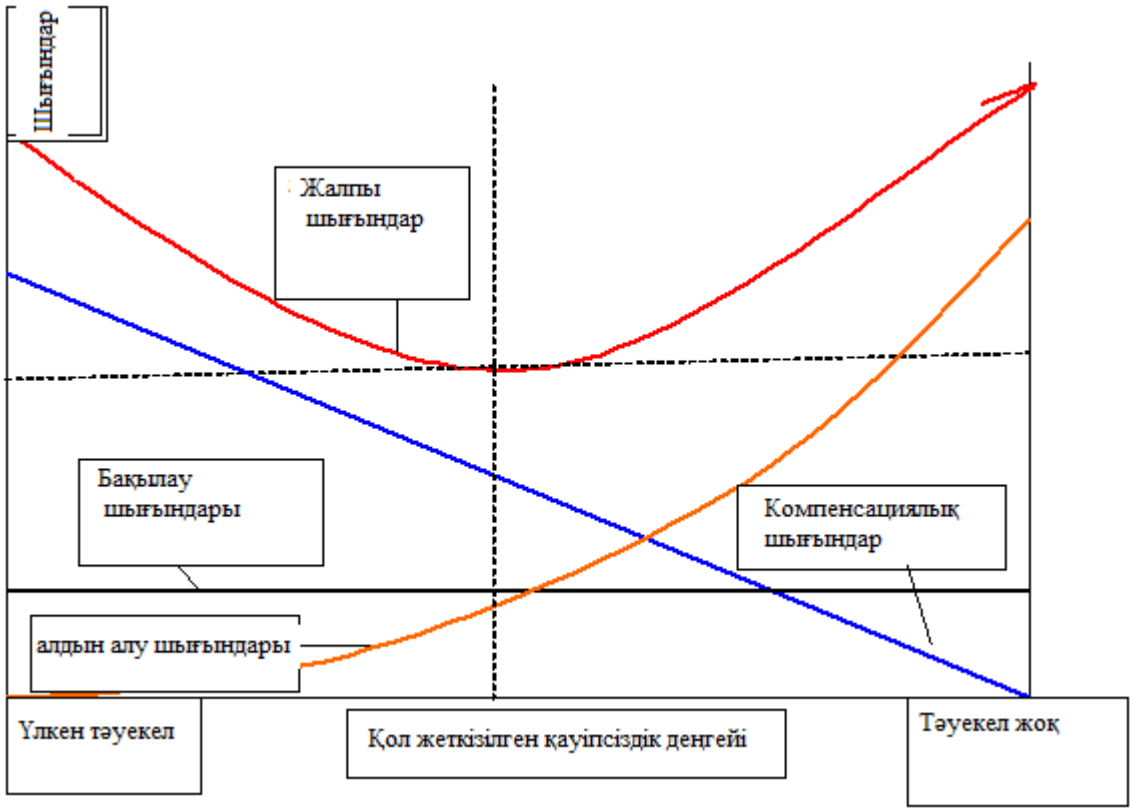
- қауіпсіздік жүйесін қажетті деңгейге дейін қалыпқа келтіру;
- АЖ қорларын қалыпқа келтіру;
- АҚ жүйесін қайта өңдеу;
- клиенттердің сенімін қалыпқа келтіру;
- заңды тартыстар және компенсацияларды төлеу;
- қауіпсіздік саясатын бұзу себептерін анықтау.

Шығындардың келесі түрлері қауіпсіздік жүйесін жаңарту кезінде қала береді:

- қорғаныстың техникалық құралдарына қызмет көрсету;
- құпия іс қағаздарды жүргізу;
- қауіпсіздік жүйесіне аудит жүргізу және жұмысын жасауын қамтамасыз ету;
- бөтен ұйымдардың қатысуымен жұмыс істей деңгейін талдау үшін тексерулер жүргізу;
- қызметкерлерді АҚ әдістеріне оқыту.

АҚ шығындары және қол жеткізілетін қорғаныс деңгейі.

Фирманың АҚ деңгейін жоғарлатуға шыққан шығындар қосындысы жалпы шығындарды құрайды. Қауіпсіздіктің жалпы шығындары мен фирманың ақпараттық ортасының қорғаныс деңгейі арасындағы байланыс 4 суретте келтірілген.



4 сурет – Шығындар және қол жеткізілген қорғаныс деңгейі арасындағы байланыс

Қауіпсіздікке жалпы шығындар ескертілген шараларға, сонымен бірге жоғалтуларды бақылау және толықтыруға шығындардан қалыптасады. Жүйесінің қорғаныштық деңгейінің өзгерісімен келтірілген құраушылар және шығынның ортақ деңгейі өзгереді. Суреттен қорғаныштықтың деңгейі «үлкен

тәуекел» және «тәуекел жоқ» мәндерімен шектелгенін көруге болады. Суреттің сол жақ бөлігінде жалпы шығындар үлкен және қауіпсіздіктің саясатты бұзылғанда өтемге кеткен шығындармен анықталады, ал жүйеге қызмет көрсетуге кеткен шығындар аз.

Егер қорғаныштықтың деңгейі үлкейсе, шығындар да көбейеді, бірақ үлкею қауіпсіздік жүйесінің күрделенуімен байланысты және сәйкесінше жабдық және шара шығындардың үлкеюімен байланысты. Өтемдерге шыққан шығындар төмендейді.

Экономикалық тепе-теңдік жағдайы уақыт бойынша өзгере алады. Экономикалық тепе-теңдік жағдайы шабуылдардың технологияларын жетілдіретін қаскүнемдердің жетістіктеріне тәуелді болады. Экономикалық тепе-теңдіктің тиісті деңгейі фирманың қауіпсіздік саясатына айтарлықтай тәуелді болады, және ол құпия кәсіпорындар үшін оң жақ аумаққа айтарлықтай ығысуы керек.

Егер АҚ бұзылса не істеу керек? Ол жоғары зерделі бұзу себебінен емес, желідегі жаңылу себебінен болды. Және бұл электр қызметкерлері және электрондық техника қызметкерлері немесе өрт сөндірушілердің міндеті ғана емес. Егер деректер жоғалса, яғни АҚ категориясы ретінде бүтіндік бұзылса, онда бұл мәселемен АҚ қызметі айналысуы қажет.

АҚ қауіптерінің ең жиі кездесетіндерін талдау бірінші орында апаттық сипаттағы (желінің жаңылуы, табиғи апаттар және тағы басқалар) себептер тұратынын көрсетті, содан кейін қызметкерлердің қатесінен болған жағдайлар, содан кейін барып қаскүнемдердің шабуылдары жүреді. Сондықтан, қаскүнемдердің шабуылдарымен сирек шұғылдануға тура келетіні ықтимал.

АҚ қаупінің пайда болуының зардаптарымен тиісті сабақтас шаралар арнайы құжатта болуы тиісті. Сондықтан ұйым осы уақытта көрсететін ахуал қызметшінің әсері суреттеген толық сипаттауы керек, сонымен бірге бұл қызметшіні табылған құжатқа оқиғалардан кейін сұрау керек. Алдын ала шаралардың қатары орындаған құжат едәуір қысқартқан залал болуы мүмкін. Бұл құжат барлық нұсқалардың, олардың ішінен ұтымды таңдауға байсалды жағдайда жасауы керек. Құжат нақты шарттарда, барлық қызметші тексеруі жағдайдағы апат ахуалын сезуі керек. Апат жоспары маңызды сұрақтардың жауабымен қызмет көрсетеді. Апаттың зардаптарын азайту үшін не болуы мүмкін? Апаттық жағдайлардың даму кезеңінде қандай шараларды орындау керек? Апаттық жағдайдан кейін не істеу керек? Қарапайым әрекетке қалай келу керек?

6 Апаттық жоспар және келеңсіз жағдайда жұмыс істеу

6.1 Апаттық жоспар қағидалары

Кәсіпорын үшін нақты апаттық жоспар - бұл ұйымның саласына, іскерлік ерекшеліктеріне және т.б., сондай-ақ орналасуының географиялық ерекшеліктеріне, жақын маңда орналасқан басқа ұйымдарға, апаттық топ қызметкерлерінің құрамы мен кәсіби сапасына тәуелді меншікті құжат. Мұндай жоспар құру үшін ұсынылатын өте көптеген үлгілір бар.

Авария жоспарды құруды апат дегеніміз не анықтамасынан бастаған жөн. Апат – жүйелі процедуралармен анықталатын күнделікті әрекеттерден өзгеше әрекеттерді талап ететін келеңсіз жағдай. Бұл әрекеттер арнайы жоспардың бөлшегін іске асыруды ескереді.

Оқиғалардың жіктелімі.

Табиғи апаттардың көпшілігін кейбір ақпараттық қамтамасыз етудің (жабдық, бағдарламалар, мәліметтер) уақытша немесе тұрақты қолжетпеушілік ретінде жіктеуге болады, ал бұл сынып ішінде ғимараттың (жабдықтың ұрлануы немесе қиратылуы) немесе бір бөлімшенің бөлігі немесе аумағының шегі ретінде жіктеуге болады.

Келесі қадам – ол жүйелер мен нысандарды қалыпқа келтіру басымдылықтарын анықтау. Мұндай жағдайда, үрдісті жеңілдету үшін жоғарғы деңгейден бастаған жөн, мысалы:

- кәсіпорынның түпкі мақсаты – клиенттерге қызмет көрсету;
- клиенттерге қызмет көрсетумен қызметкер шұғылданады;
- клиенттерге автоматтандырылған жүйе көмегімен қызмет көрсетіледі;
- автоматтандырылған жүйе қосымшалар мен мәліметтер талап етеді;
- қосымшалар және ДҚБЖ операциондық жүйе мен коммуникацияларды талап етеді.

Операциондық жүйе жабдықтық қамсыздандыруды және т.б. талап етеді. Ақпараттық жүйелер туралы сөз болғанда, апаттан соң кейбір жүйелер ғана іскерлігін бірден қалыпқа келтіруді талап етеді, яғни ақпараттық жүйелерді апаттық жоспар тұрғысынан жіктеу қажет.

Жүйелер келесідей болуы мүмкін:

- маңызды (кәсіпкерліктің жалғасы оларсыз мүмкін емес);
- екінші реттік және қосалқы есептер үшін;
- күнделікті жұмыс үшін қажеттік пайда болатын, бірақ апаттан кейінгі алғашқы сағ/күн емес;
- жүйенің дамуының болашағы үшін қажетті.

Резервтегі нысандар шәкілі (шкаласы).

Нысан қызметін қалпына келтіру үшін апаттық жағдайда керекті шарттардың тізімін анықтауға болады. Егер ғимарат және коммуникациялар аман сақталса, келесі кезең қажетті – жабдықтар және т.б. Бірақ та ең негативті нұсқаны ескеру керек – ол ұйым максималдық шығындарға

ұшырағанда. Мұндай жағдайда келтірілген тізім бойынша төменнен жоғарыға көтерілуге болады. Әрекеттер тізбегі мұндай жағдайда келесідей болуы керек:

- іскерлік әрекетті жалғастару үшін бөлмелер қажет. Жұмысты ашық аспан астында немесе шатырларда бастау да мүмкін, бірақ ондай жолдарға бағдар алған жөн емес;
- бөлмелер тиісті инфрақұрылыммен жабдықталуы керек (қоректену, су құбыры және тағы басқалар), немесе бұл инфрақұрылымды жуық арада жасау керек;
- егер бұл іскерлік үшін қажет болса, жергілікті желі орнатылып сыртқы ақпараттық кеңістікке шығулар ұйымдастырылуы керек. Апат кезінде желі толық немесе жартылай аман сақталуы мүмкін, бірақ желілік жабдықтың бөлігінің алмастыруын талап етеді;
- кәсіпорын жабдықтық қамсыздандыру қор қамын ойластыруы керек, немесе жабдықтаушымен жабдықтың жедел жеткізілуі туралы келісуі керек;
- кәсіпорындарда операциондық жүйелердің, қосымшалардың, ДҚБЖ тағы басқа бағдарламалардың орнату көшірмелері болу керек, немесе жедел түрде жабдықтаушыдан алу мүмкіндігі болу керек. Ұйым үшін маңызды мәселе программалық кешендердің кескінді күйге келтірулерінің көшірмелерінің бар болуы сұрақ болып қалады;
- кәсіпорындарда мәліметтердің резервтік көшірмесі болуы керек және де ол апаттың алдында барынша жақын уақыттағысы болғаны жөн;
- ақпараттық жүйелердің жұмысын қамтамасыз ету үшін қажетті және клиенттермен жұмыс жасайтын кәсіпорынның қызметкерлері (әкімдер тағы сол сияқтылар) өз функцияларынорындауға дайын болуы керек, немесе басқа фирманың қызмекерлерімен ауыстырылуы керек, немесе жедел сырттан жұмысқа алынуы қажет;
- ұйымның серверіне клиенттердің ену рұқсатын қамтамасыз ету керек. Егер ол қашықтағы сервер болса, онда тиісті коммуникациялардың (интернет, ерекшеленген каналдар) бар болуымен қамтамасыз ету керек.

6.2 Апаттық жоспардың құрылымы

Құрылымдалған апаттық жоспар бірнеше бөліктен тұруы және де төменде келтірілген құжаттар міндетті түрде болуы керек.

6.2.1 Жүйелердің нысандары бойынша апаттық жағдайды анықтауы және басымдылықтарды қою. Бұл құжатта сипатталған есептер жоғарыда қарастырылды. Басымдылықтарды анықтау және қою жоспар құрастырудың басталуына дейін орындалуы керек. Бұл жұмыстың нәтижелерін кәсіпорынның басқармасымен бекітілген жоспарда, апаттық жағдай туындағанда қосымша даулар пайда болмайтындай етіп бекіту керек.

6.2.2 Алдын алу шаралары. Алдын алу шаралары апаттық жағдай туындағанда мекеменің шығын көлемін азайту немесе жою үшін жүйелі өткізілетін шаралар мен әрекеттердің сипаттамасынан тұрады.

Қалыпқа келтіру негізі болып жұмыстың жаңа орнын құру табылады – қалыпқа келтірілген ақпараттық кеңістіктің бар болуы. Бұл жағдай үшін мүмкін болатын жолдар кәсіпорынның қаржы мүмкіндіктеріне тәуелді:

а) кәсіпорынға тиесілі жеке қордағы ғимараттың болуы. Қордың дайындығы әртүрлі кескіндерде болуы мүмкін:

- "ыстық" – орын толығымен жұмыс жағдайдың көшірмесі болып табылады, тек қана пайдаланушылар жаңа орындарына жайғасып, жұмыстық стансаларын қосса болғаны;
- "біртіндеп суу" дәрежелі – мысалы, жергілікті желі кәбілдер және жабдықтар түрінде бар, қосымша белсенді жабдықтардың орнатылуы қажет, электрлік қоректендіру бар, бірақ жалғанбаған және т.б.;
- "суық" – ғимарат, электрлік қоректену инфрақұрылымы және санитарлық - техникалық жабдықтар бар;

ә) апаттық жағдайда бір уақытта немесе кезекпен пайдалану үшін жеке ғимаратты басқа бір ұйыммен бірлесіп қорда ұстау;

б) күнделікті өмірде қойма ретінде немесе жұмыстық сервердің орналасқан орнын жартылай пайдаланып жүрген жеке ғимаратты қорда ұстау;

в) апаттық жағдайда кәсіпорынға қарасты мекемелердің біріне немесе әріптес ұйымға көшу.

Резервті қордағы ғимараттың болғаны жағдайда оның күзетін қамтамасыз етіп және жұмыс жүктемесін кез келген уақытта қабылдай алу дайындығын үнемі тексеру керек. Егер де ұйымның апаттық жағдайды күту тәртібінде тұрған компьютерлік жабдығы болмаса, онда мұндай жабдықтың қорын кәсіпорынның қоймасында қамтамасыз ету керек. Екінші жол – ол уақытша пайдалануға кейбір жабдықтарды беретін әріптес ұйыммен алдын ала келісімге отыру.

Келесі маңызды элемент – ақпараттық жүйелердің (жүйелік және қолданбалы бағдарламалық қамсыздандыру) инсталляциялық кешендерінің сақталуы. Қалпына келтіру асығыс түрде мүлде басқа мамандармен орындалуы мүмкін екенін ескеру керек, алайда аса маңызды бөлшектерді ескерген жөн. Ақпараттық кеңістікті қалыпқа келтіру кезінде оның қорғанысын қамтамасыз ету туралы да ұмытпаған жөн. Егер осы ақпараттық жүйе жеке реттеулерін файлдарда сақтауға мүмкіндік берсе, онда олардың көкейкестісінің көшірмесін резервтік көшірмелерімен бірге сақтау керек.

Сақтауға қажетті деректер апаттық жоспар тұрғысынан категорияларға жіктелуі керек. Деректер келесі түрдегідей бөлінуі мүмкін:

- алғашқы немесе жедел мәліметтер, яғни әрқашан қолжетімді болатын;
- екінші реттік немесе жартылай жедел мәліметтер, яғни қажеттілік туындағанда автоматты түрде қолжетімді болатын;
- үшінші реттік немесе автономды мәліметтер, яғни механикалық амалдардың қатарын орындаудан кейін қолжетімді болатын.

Берілген жіктелуді ескере отырып, мәліметтердің резервтік көшірмесі маңызды құраушы бола тұра апаттан құтқаратын жалғыз құрал емес екендігі

түсінікті. Мысалы, он-лайн қызметтерді көрсететін ұйымдар үшін деректері бар сервердің қирауы (резервтік көшірмелерден бірнеше сағаттар барысында қалыпқа келтіруді талап ететін) аса күрделі шығындарға әкеліп соғады.

Қазіргі заманауи технологиялардың ішінде территориялық таратылған қайталайтын түйіндерді қолданудың мүмкіндігі бар, сонымен бірге дисктік, процессорлық тағы басқа қорларды бөтен провайдерден жалдауға мүмкін. Резервтегі көшірмесін алу - бұл төменде толық қарап шығатын жеке үлкен сұрақ.

Алдын ала өкілеттік тұлғаларды анықтау қажет – апат туындаған жағдайда және қалыпқа келтіру жұмыстарында қызметкерлердің әрекеттерін басқаратын жұмыстық топ, комитет. Резервтік көшірмелерді қашықтан сыртта сақтау мүмкіндігі сұрағын қарастыра отырып олар да қауіпсіздік шараларын қолдану үшін зат болатынын ескеру керек. Маңызды қателердің бірі – резервтік көшірмелер қорғауының жоқтығы, оларда сол қолданушылар және әкімдердің құпия сөздерінің базасы секілді аса маңызды ақпарат болуы мүмкін.

Сыртқы тасушыларда деректерді қалыпты сақтау әдісі болып деректерді қорғаудың күшті криптографиялық механизмдерді қолдану табылады.

6.2.3 Апаттық жағдайлардағы шаралар. Апат болған кездегі және содан кейінгі жағдайда өнеркәсіп өндірістік процесті жалғастыруды бастағанда белсенді әрекет қолдану керек. Ең алдымен біз ақпараттық қауіпсіздік мәселелерін қарастыратынымызға қарамастан, адамдардың өмірі мен денсаулықтарының байбаламның жоқтығын қамтамасыз ету керек. Сонымен бірге бұл тармақ апатқа қатысты оқиғалардың шабуылы туралы ұйымның қызметкерлерінің жедел дерек беруі, шараның әсерінің және тағы басқа тұлғалардың клиенттері үшін қажетті шараларды түсіндіру керек.

Егер ақпараттық қорлардың сақталуы туралы адамдардың өмірінің байбаламдары жоқ болса, бірден тынышсыздану керек. Ол үшін әсерлі жүйелер үшін талап ететін жағдай талдау керек. Апат кезде тиісті әсерлерді анықтап формалау;

- авария оқиғасының шабуылында оқиғалардың түріне қажетті шараларды белгілеу;
- шараларда жұмыс істеген қызметкерлер оқиғаның осы түрін шабуыл туралы баяндап беру;
- әсерлер туралы қызметкерлердің хабарлы болуымен қамтамасыз ету және олардың орындауына дайындық тексере алу.

6.3 Апат жоспарының мысалы

Жоспар Массачусет технологиялық институтының жарияланған нұсқадан алынған апаттық жоспарды білдіреді.

6.3.1 Әкімшілік есептеудің регламенті бойынша комитет. Бұл комитет келесі қызметкерлер қоса алады:

- институттың үлкен вице-президенті – комитеттің төрағасы. Қалпына келтіру бойынша жұмыстармен басқарып басшылық етеді. Қалпына келтіргіш жұмыстардың орындауының жүрісі туралы есеп беру үшін ғылыми институттың жоғарғы басқаруымен өзара әрекеттесуді қамтамасыз етеді;

- қаржы операциялары бойынша вице-президент. Апат таңдандырылған кризистік бизнес-функцияларларды қолдау үшін комитетпен өзара әрекеттесуді қамтамасыз етеді;

- ақпараттық жүйелер бойынша вице-президент. Мәліметтердің барлық өңдеуі және телекоммуникациялық жүйелер, қалпына келтірілетін ғимараттар және ерекшеленген резервтегі орналастырылудағы операцияны қоса қалпына келтіру үйлестіреді;

- қорлардың дамытуы бойынша вице-президент. Апат таңдандырылған кризистік бизнес- функцияларларды қолдау үшін комитетпен өзара әрекеттесуді қамтамасыз етеді;

- зерттеулер бойынша вице-президент. Апат таңдандырылған кризистік бизнес-функцияларларды қолдау үшін комитетпен өзара әрекеттесуді қамтамасыз етеді;

- проректор. Апат таңдандырылған кризистік бизнес-функцияларларды қолдау үшін комитетпен өзара әрекеттесуді қамтамасыз етеді.

Бизнес- қызметтің жалғасын басқаратын команда:

- ақпараттық қауіпсіздік бойынша маман. Институттың апат таңдандырылған төңірегінде және сыртқы топтармен топтардың арасындағы өзара әрекеттесудің басқарулары қамтамасыз етеді. Сонымен бірге, авария жоспары бар жұмыстың дағдыларына авария жоспарының тұрақты сүйемелдеуі, үйренуге және авария жоспарының тестеуі. Бизнес- қызметті басқаратын топтарға қатысты сұрақтар бойынша жүйелердің институттық қолдау тобын үйлестіреді;

- операциялар және жүйелер бойынша директор. Бас мәліметтердің ортасындағы деректерді өңдеудің қорлары және уақытша орналастырылудың ерекшеленген орындары үшін қолдауды үйлестіреді;

- телекоммуникациялық жүйелер бойынша директор. Дауыстың берілуінің талғаулы каналдары және негізгі сызықтар апатпен шалдыққан жағдайдағы мәліметтерді қамтамасыз етеді. Ғылыми институттың желісінің сақтауы үшін тиісті құралдарды таңдайды және талаптарын бағалайды;

- студенттік қалашықтың полициялары. Таңдандырылған аудандар, ғимараттар және апатқа айналып кете алатын ахуалдарды хабарлау тетіктері үшін қосымша қолдауды, физикалық қауіпсіздікті қамтамасыз етеді. Апат таңдандырылған аудандар айналасындағы қауіпсіздік периметрін кеңейтеді;

- коммуналдық қызметтердің директоры. Су құбырының, электрдің және тағы басқа қолдау жүйелеріңің қалпына келтіруі сонымен қатар, құрылымдық бүтіндік үшін барлық қызметті үйлестіреді. Апатпен

зақымдалған болуы мүмкін құрылымдардың қолдануы үшін болжамды жүзеге асырады және бұзылуды бағалайды.

- сақтандыру және заң тұрғылары бойынша директор. Сақтандыруға және талаптар бойынша мамандардың өзара әрекеттесуін қамтамасыз етеді. Кәсіпкерліктің жалғасының жоспарлау бағдарламаларын сақтандыру бағдарламасымен үйлестіреді;
- жаңалықтар қызметінің директоры. Іске қосылмаған қалпына келтіргіш операцияның баспасөзбен, қызметшімен, қоғамдық ұйымдармен қарым-қатынасын қамтамасыз етеді;
- қызметші жұмысы бойынша департамент. Апат радиобайланысы арқылы қызметшінің хабарлауын және адам қорларымен байланысқан қалпына келтірулерінің элементтер қолдауын қамтамасыз етеді;
- таралған есептеуіш және желілік қызметтердің директоры. Әкімшілік, ғылыми жұмыстар және басқа таралған қызметтер мен желілер үшін желілік қолдауды қамтамасыз етеді;
- ақпараттық жүйелер бойынша вице-Президент көмекші. Сыртқы топтармен өзара әрекеттесуді қамтамасыз етеді және президент қызметін білдіреді.
- апаттық сезілу командасы. Бағдарлаушы инженерлік коммуналдық қызметтермен басшылық етеді және апаттық ахуалындағы бірінші кезеңнің сезілуін қамтамасыз етеді.

7 Зерттеу жүргізу

Зерттеуді жүргізу сезілу тобының функциясы болуы мүмкін немесе басқа мамандармен орындала алады - бұл кәсіпорынның саясаты және нақты соқтығыс түрінен тәуелді болады. Соқтығыс үшін уақыт бойынша таралғаны жеткілікті, зерттеуді шабуыл барысында өткізуге болады. Зерттеудің негізгі мақсаты – соғысқа қатысты көбірек ақпарат жинау, яғни кім, не, қашан, қайда, қалай және неге деген сұрақтарға жауап беру.

7.1 Алдын алу шаралары

Бірінші кезеңде зерттеу талап ететін соғыс болып не табылатынын анықтау қажет? Қандай оқиғалардың шабуылы зерттеуді жүргізуді талап ететінін құжаттамалы бекіту керек. Ең қарапайым мысал – кері нәтижесі бар қолданушы паролын енгізудің бірнеше рет талпыныстары дәлелінің табылуы. Зерттеу осы жағдайда керек болады әлде жоқ па?

Амалдар мемлекетаралық заңдар бойынша қылмыстар болып табыла алады деген себеппен қауіпсіздік мамандардан нақты назар талап ететін кейбір амалдар төменде көрсетілген, демек, кәсіпорын бұл мемлекеттің субьектісі ретінде мұндай оқиғаларға жауап қайтару керек:

- рұқсатталмаған мүмкіндік;

- рұқсатталған мүмкіндік құқығының асып кетуі;
- авторлық құқықтың немесе интеллектуалды меншігінің бұзушылығы;
- алынған мәліметтерді теріс пайдалану;
- порнографияларды қолдану, зорлыққа шақырулар, ұлттық және тағы басқа алауыздықты тұтандыру;
- қорларды рұқсат етілмей қолдануы (серверлер, қызметтер);
- мәліметтердің жалғаны, рұқсат етілмеген модификация;
- меншіктің ұрлығы (комплект жасайтын ақпараттық жабдық);
- ақпараттың құпиялылығы, жеке меншік құқығының бұзушылығы;
- сервистер жұмысындағы бөгет (қызмет көрсетуден бас тарту) немесе сала қорытындысы;
- компьютерлер арқылы алаяқтық;
- вирустарды тарату;
- жаман ойлы бұзу немесе берілген мәліметтерді жоюы;
- компьютер көмегімен қиянат жасау немесе бопсалау;
- жат дүниенің иемденуі;
- тыңшылық (соның ішінде өнеркәсіптік);
- терроризм (біздің жағдайымызда ақпараттық немесе компьютер көмегімен);
- ұйым қандай белгілер қылмысқа жатқызуға болған оқиға шабуылдың мүмкіндігінің идентификаторларымен немесе бірі болып табыла алғанын анықтауы керек.

Көңіл аударуды керек ететін басқа маңызды моменттің бірі кәсіпорын қызметтерінің жұмыс қызметі мүмкіндігі болатын зерттеу нәрсесімен хабардар болу болып табылады. Кері жағдайда, егер зерттеу барысында қажеттілік пайда болса, мысалы, өздік файлдарды және қызметкердің өз жұмыстарын станциясында немесе серверде сақталатын мәліметтерін талдау, бұл кәсіпорынға қызметкер жағынан талаптар себебімен қызмет ете алады.

Бұдан басқа, алдын алу шаралардың қосымша қатары қажет. Сот тәжірибесіндегі белгілі жағдайларды АҚ бұзылысының қатынасында талаптарды қарастыруда сот бас тартқан кездегі келесі себептер:

- бұзушы авторланбаған рұқсат тыйым салынғанына алдын ала хабардар болмаған;
- қызметші қауісіздік ұйымның ережелерімен таныспаған немесе оларды дұрыс түсінбеген;
- ұйым АҚ-ға көңіл бөлмеді және сайып келгенде, бұзушылықты арандатты.

7.2 Мақсаттар және зерттеу есептерін анықтау

Ұйымдар не үшін берілген зерттеу жүргізіледі, оның нәтижесі қандай болатынын анықтау керек. Зерттеуі нақты инцидентке байланысты негіз бола алады:

- қызметкердің қатынасында кәсіпорынның өзінің ішкі шешім үшін (айыппұл, жұмыстан шығару);
- сақтандыру компаниясына орнын толтыруға сұрау салу;
- әкімшілік жауапкершілік;
- қылмыстық қудалау.

Осыған тәуелді және зерттеу барысында оның нәтижелерінің рәсімдеуі ерекше және өзгешеленуі керек.

Іс заңның ерекшеліктерімен қосымша шиеленістіріп ала алады - қылмыстардың барлық түрлері заңмен бейнелене алмайды және де тексеретін тұлғалардың біліктілік талап ететін жоғарғы технологиялардың облысымен, сонымен бірге жұмыс ерекшелігімен қайтара алады. Олар соттағы дәлелдердің бөтен бағасы үшін келесі түрлердің біріне елестете алады:

- монитор бетіндегі сурет секілді;
- басып шығарылу секілді;
- бейне немесе фотосъемка секілді;
- ауызша немесе құжатты өтініш секілді.

Зерттеулер жүргізуде дәлелдер ұсынысының бұл әдістері есепке алыну керек. Мысалы, егер қылмыстар орында содан соң жоғалтқан мониторда суреттің түріндегі белгісіз айғақ жазып қойса, осылай, онда оның фотосурет немесе куәгерлердің құжатты сипаттамасының түрінде көрсетуге керек.

Бұдан басқа, бір ізге салған технологиялар үшін айғақтың түпнұсқасы әрдайым көрсету мүмкін емес. Көшірменің беруі үшін негізбен жағдайлар бола алатынын есепке алу керек:

- түпнұсқа табиғи құбылыспен немесе басқа кездейсоқ әсермен жойылған (қызметшінің қатесімен);
- кәдімгі өндірістік процесс жүрісіне түпнұсқа жойылған (бір берілгендер екіншісінің үстінене).

физикалық заттардың түрінде айғақтар жиынында олардың теңестіруін қамтамасыз ету керек (айғақтың берілген үлгісі, алып тастаудың мерзімі мен уақыты, алып тастау орны), сақталушылық (егер айғақта саусақ таңбасы бола алса, алып тастау қолғап арқылы өндіріп алу керек), өзгермейтіндік (сүргі салынған контейнерде сақталу).

7.3 Жедел әрекеттер

Соқтығыс болды ма немесе ол іске асырылу кезеңінде соқтығыс нәтижелерінен мүмкін болатын залалдың төмендеуі үшін қандай шаралар қолдану керек екендігін анықтау керек. Кәсіпорында соқтығыс білдірген бұдан әрі - қызметшіні немесе қолданылатын автоматтандырылған жүйені алып тастаған жөн. Қай кезеңде соқтығыс туралы басқару бірден немесе мәліметтің түсуінен кейін хабарлауын алдын ала келісу керек (осы жағдайда жалған қатынастардың үлкен саны болуы мүмкін) немесе егер осындай болса кейбір алдын ала тергеу, зардаптардың бағаларынан кейін.

Келесі кезеңде соқтығыс туралы мәлімет жариялаған болуы мүмкін бе екенін, мүмкін болса, онда қандай бөлігін және кімге екенін анықтау керек. Бір жағынан, мәліметтің ашылуы зиянды бола алады, яғни, біріншіден, қаскүнемдерге мәлімет беріле алады, екіншіден, серіктестікке кір келтіре алады. Басқа жағынан, ашылу соқтығыс белгілері туралы қолданушылар мағлұматтауға және соқтығыстың ары қарай дамытуы сақтап қала алады, сонымен қатар, әрбәр соқтығыс үшін куәгерлердің қосымша санын жақындату.

Қорытынды

Ақпараттық қауіпсіздік жаңа жүйелерге олардың жасалуы кезінде ендірілуі керек. АҚ стратегиясының негізіне оның барлық параметрлерін бақылау және келешекке әзірлеуді қою керек. АҚ тәуекелдер ақпарат алмасудың дамуымен байланысты болашақта өседі. АҚ жүйелерінің тиімді жұмысы үшін шешуші рөлді бұл процестің негізгі қатысушылары ойнайды, соның ішінде қызметкерлер, жабдықтаушылар және іскер әріптестер. АҚ технологияларының жаңғыртуына қатысты тенденциялар әзірше айтарлықтай емес. Биометриялық бақылаудың құралдарын тек қана ұйымдардың 5 % ендірді. АҚ технологиялардың жаңғыртуларына негізгі бөгет болатындар –ол технологиялардың құны, біліктіліктің жоқтығы, келешек технологияларды жеткілікті білмеу, техникалық сұрақтар болып табылады.

Компаниялар кезігіп қалатын тәуекелдерді, ақпараттық жүйелердің маңыздылығын негізге ала отырып, кәсіпорындардың оқиғаларға болғаннан кейін ғана әрекет етуі дұрыс емес.

А.1 қосымшасы

Қауіптер тізімі

А.1 форс-мажорлық жағдайлармен байланысты қауіптер
А1.1 Қызметкерлер шығындары.
А.1.2 Ақпараттық жүйенің ақауы.
А.1.3 Найзағай.
А.1.4 Өрт.
А.1.5 Су басу.
А.1.6 Кәбілдің жануы.
А.1.7 Қолайсыз температура және ылғалдылық.
А.1.8 Шаң, ластану.
А.1.9 Қарқынды магниттік өрістердің әсерінен деректердің шығыны.
А.1.10 Үлкен аумақтағы желінің ақауы.
А.1.11 Қоршаған ортадағы апаттар.
А.1.12 Ерекше қоғамдық оқиғалар.
А.1.13 Теңіз дауылы.

А.2 Ұйымдастыру деңгейіндегі қауіптер

А.2.1 Регламент белгілейтін құжаттардың жоқтығы немесе кемшіліктері.
А.2.2 Регламент белгілейтін құжаттардың талаптарын жеткіліксіз білу.
А.2.3 Жарамсыз немесе жеткіліксіз үйлесімді қорлар.
А.2.4 АТ –да қауіпсіздік деңгейін өлшеу және бақылау кемшіліктері.
А.2.5 Қызмет көрсетудегі кемшіліктер.
А.2.6 Қауіпсіздік саласындағыі талаптарға бөлмелердің сәйкессіздігі.
А.2.7 Өкілеттікті асыра қолдану.
А.2.8 Қорларды бейберекет қолдану.
А.2.9 Ақпараттық технологиядағы өзгерістерді бақылау процедураларындағы кемшіліктер.
А.2.10 Көрсетілетін талаптарға деректерді тарату ортасының сәйкессіздігі.
А.2.11 Жоспарлау көкжиегі жеткіліксіз.
А.2.12 Коммуникацияларды құжаттаудағы кемшіліктер.
А.2.13 Дистрибуторлардың әрекеттерінен жеткіліксіз қорғаныс.
А.2.14 Жұмыс орындарының қолайсыздығынан ақпараттық технологияларды қолданудың нашарлауы.
А.2.15 Құпия ақпараттық деректерге рұқсатсыз қол жеткізу мүмкіндігі.
А.2.16 Ықшам ЭЕМ-нің қолданушыларының рұқсат етілмеген (құжаттамалған) өзгерісі.
А.2.17 Криптографиялық кілттерді дұрыс емес басқару жүйесі.
А.2.18 Факстердің шығын материалдарымен лайық емес жабдықтау.

А.2.19 Қолданушыларды лайықсыз өзгерту жүйесі.

А.2.20 Мәліметтерді тексеру нәтижелерінің тиісті бағасының жоқтығы.

А.2.21 Желідегі құпия деректерге рұқсат етілмеген рұқсат.

А.2.22 Айырбас жылдамдығын кішірейту.

А.2.23 Бағдарламалық қамсыздандыруды жеткіліксіз тестілеу.

А.2.24 Теріс құжаттама.

А.2.25 Авторлық құқықтың бұзушылығы.

А.2.26 Бағдарламалық қамсыздандыруды эксплуатациялау сатысында бағдарламаларды рұқсатсыз тестілеу.

А.2.27 ОЖ басқаруымен жүйені дұрыс емес қорғау.

А.2.28 Телекоммуникациялық деректердің лайықсыз өткізу қабілеттілігі.

Әдебиеттер тізімі

1. Конеев И.Р., Беляев А.В. Информационная безопасность предприятия - М.: Мастер систем, 2003,-733 с.
2. Мельников В.В. Защита информации в компьютерных системах. - М.: Финансы и статистика; Электроинформ, 1997.-368 с.
3. Ярочкин В.И. Система безопасности фирмы. - М.: Ось-89, 1997-89, 106 с.
4. Петраков А.В., Дорошенко П.С., Савлуков Н.В. Охрана и защита современного предприятия. - М.:Энергоатомиздат,1999-568 с.
5. Управление информационными рисками. Экономически оправданная безопасность / Петренко С.А., Симонов С.В. – Компания АйТи; ДМК Пресс, 2004.- 384 с.: ил.
6. Рутгайзер О.З. Организация и управление службой защиты и безопасности информации – Учебное пособие, Алматы:АИЭС, 2006. – 77с. ISB 9965-708-28-2
7. Пшенин Е.С. Теоретические основы защиты информации: Учебное пособие, Алматы: КазНТУ, 2000-125с. ISB 9965-487-36-7
8. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты.-М., 2002-306 с.
9. Мельников В.П. Информационная безопасность и защита информации.-М., 2008.

Бахытжан Сергеевич Байкенов
Сандугаш Кудайбергеновна Оразалиева

Ақпарат қауіпсіздігі мен қорғаныс қызметін ұйымдастыру және басқару
Оқу құралы

Редакторы: Кегенбаева А.А.
2012 ж жин.тақ. жоспары, 49 реті

«__» ___ 2014ж. терілуге берілді

Пішіні 60х84 1/16
№ 2 типографиялық қағаз
Оқу-баспа таб. - 4.3. Таралымы 100 дана. Тапсырыс . Бағасы 2150 тенге.
Басуға _____ 2014ж. кол қойылды.

«Алматы энергетика және байланыс университеті»
Коммерциялық емес акционерлік қоғамының
көшірмелі – көбейткіш бюросы
050013, Алматы, Байтұрсынұлы көшесі, 126